AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ENHANCING PREPAREDNESS AND RESPONSE CAPABILITIES TO ADDRESS CYBER THREATS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

AND THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MAY 24, 2016

Serial No. 114–71

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

23–243 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON EMERGENCY PREPAREDNESS, RESPONSE, AND COMMUNICATIONS

DANIEL M. DONOVAN, JR., New York, *Chairman*

TOM MARINO, Pennsylvania
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
MICHAEL T. MCCAUL, Texas *(ex officio)*
DONALD M. PAYNE, JR., New Jersey
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*

KERRY A. KINIRONS, *Subcommittee Staff Director*
KRIS CARLSON, *Subcommittee Clerk*
MOIRA BERGIN, *Minority Subcommittee Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
KATIE RASHID, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

ENHANCING PREPAREDNESS AND RESPONSE CAPABILITIES TO ADDRESS CYBER THREATS

Tuesday, May 24, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON EMERGENCY PREPAREDNESS,
RESPONSE, AND COMMUNICATIONS, AND
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY TECHNOLOGIES,
WASHINGTON, DC.

The subcommittees met, pursuant to call, at 10:07 a.m., in Room 311, Cannon House Office Building, Hon. Daniel M. Donovan [Chairman of the Subcommittee on Emergency Preparedness, Response, and Communications] presiding.

Present: Representatives Donovan, Walker, McSally, Ratcliffe, Watson Coleman, Jackson Lee, Langevin, and Payne.

Mr. DONOVAN. The Subcommittees on Emergency Preparedness, Response, and Communications and Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittees are meeting today to receive testimony regarding efforts to enhance preparedness and response capabilities to address cyber threats.

I now recognize myself for an opening statement. First, I would like to thank Chairman Ratcliffe and Ranking Member Richmond for working with me and Ranking Member Payne on this issue. Also, I would like to thank all out of our witnesses today for coming to join us in this important discussion.

We are all aware the cyber threat is real, from both state and non-state actors. The countless cyber attacks against the United States and its citizens, including major attacks against Target, Home Depot, OPM, and Anthem are just the tip of the iceberg.

I believe that the number and magnitude of attacks will only increase, especially as more and more of our lives become connected to the internet. It is imperative that we ensure that our State and local officials, as well as our first responders, are prepared to protect against and respond to a cyber attack.

Furthermore, we are seeing an increase in the number of cyber attacks that, if successful, can cause widespread physical damages to a community and require a whole-of-community response. Already, state and non-state actors have attempted to interfere with 9–1–1 call centers, sent out inaccurate alerts and warnings, and tried to take over the controls of a dam. While we have taken numerous steps to enhance our capabilities, we have a long way to go in addressing these threats.

As a member of Chairman Ratcliffe's subcommittee, I have heard about the progress the Federal Government, States, and localities have made in enhancing our cybersecurity capabilities. But I am left scratching my head when I see that for the fourth year in a row, the National preparedness report released by FEMA indicates that States continue to report cybersecurity as the lowest core capability.

What is preventing us from reaching the appropriate level of cybersecurity? What obstacles are States facing, and what can we do to help? I am especially interested in learning more about what happens after a cyber attack that has physical consequences. Who is in charge of the response, and how are first responders coordinating with cyber officials who are trying to mitigate the attack? I know States like California have set up a task force to answer these exact questions.

Additionally, in 2012, the National-Level Exercise looked at the Nation's ability to respond to a large-scale cyber attack with physical consequences. One of the key recommendations from this exercise was to finalize a cyber response plan that clearly defines the roles and responsibilities of all of the potential response entities.

Four years since that exercise and 6 years since the interim draft of the National cyber incident response plan was released, we do not have a finalized and approved plan. Developing and finalizing this plan needs to be a priority of the Federal Government. I understand that the Department plans to finally begin stakeholder engagement on the development of the final plan in the coming weeks. I certainly hope that they will be engaging with all of today's witnesses to get their feedback.

Also, I have heard that while sharing cyber information is becoming more prevalent, there is still confusion on who States should talk to when an incident occurs. The sharing of cyber-related information with the emergency management and first response communities is, at best, ad hoc.

These people are going to be the first on the scene and should have insight into whether the incident they are responding to has been caused by a cyber attack. Can States utilize their fusion centers to be a force multiplier to disseminate critical cyber information? I know that my State is taking this approach, and I am interested to hear if it has been successful.

A few years ago, Secretary Johnson made a statement that I feel is still true today. He said, "Cybersecurity is a shared responsibility, and it boils down to this: In cybersecurity, the more systems we secure, the more secure we are. We are all connected on-line, and a vulnerability in one place can cause a problem in many other places. So everyone needs to work on this. Government officials and business leaders, security professionals and utility owners and operators." That is why we are here today.

I want to thank all the witnesses for testifying today, and I look forward to highlighting the good work that you are all doing to enhance your cybersecurity capabilities and learning about what areas are still a challenge and how the Federal Government can help in mitigating those gaps.

[The statement of Chairman Donovan follows:]

STATEMENT OF CHAIRMAN DANIEL M. DONOVAN, JR.

MAY 24, 2016

First, I'd like to thank Chairman Ratcliffe and Ranking Member Richmond for working with me and Ranking Member Payne on this issue. Also, I would like to thank all the witnesses for coming today to join in this important discussion.

As we are all aware, the cyber threat is real from both state and non-state actors. The countless cyber attacks against the United States and its citizens, including major attacks against Target, Home Depot, OPM, and Anthem, are just the tip of the iceberg. I believe that the number and magnitude of attacks will only increase, especially as more and more of our lives become connected to the internet. It is imperative that we ensure that our State and local officials as well as our first responders are prepared to protect against and respond to a cyber attack.

Furthermore, we are seeing an increase in the number of cyber attacks that if successful can cause wide-spread physical damages to a community and require a whole-of-community response. Already, state and non-state actors have attempted to interfere with 9–1–1 call centers, send out inaccurate alerts and warnings, and tried to take over the controls of a dam. While we have taken numerous steps to enhance our capabilities, we have a long way to go in addressing these threats.

As a Member of Chairman Ratcliffe's subcommittee, I have heard about the progress the Federal Government, States, and localities have made in enhancing our cybersecurity capabilities, but I'm left scratching my head when I see for the fourth year in a row, the National Preparedness Report, released by FEMA, indicates that States continue to report cybersecurity as the lowest core capability. What is preventing us for reaching the appropriate level of cybersecurity? What obstacles are States facing and what can we do to help?

I'm especially interested in learning more about what happens after a cyber attack that has physical consequences. Who is in charge of the response and how are first responders coordinating with cyber officials who are trying to mitigate the attack? I know States like California have set up task forces to answer these exact questions.

Additionally, in 2012, the National Level Exercise looked at the Nation's ability to respond to a large-scale cyber attack with physical consequences. One of the key recommendations from this exercise was to finalize a cyber response plan that clearly defines the roles and responsibilities of the all the potential response entities.

Four years since the exercise and 6 years since the interim draft of the National Cyber Incident Response Plan (NCIRP) was released, we still do not have a finalized and approved NCIRP. Developing and finalizing this plan needs to be a priority of the Federal Government. I understand that the Department plans to finally begin stakeholder engagement on the development of the final plan in the coming weeks. I certainly hope they will be engaging with all of the witnesses at today's hearing to get their feedback.

Also, I have heard that while sharing cyber information is becoming more prevalent, there is still confusion on who States should talk to when an incident occurs and the sharing of cyber-related information with the emergency management and first responder communities is ad hoc at best.

These people are going to be the first on the scene and should have insight into whether the incident they are responding to has been caused by a cyber attack. Can States utilize their fusion centers to be a force multiplier to disseminate critical cyber information? I know my State is taking this approach and I'm interested to hear if it has been successful.

A few years ago, Secretary Johnson made a statement that I feel is still true today. He said "[c]byersecurity is a shared responsibility, and it boils down to this: In cybersecurity, the more systems we secure, the more secure we are. We are all connected on-line and a vulnerability in one place can cause a problem in many other places. So everyone needs to work on this: Government officials and business leaders, security professionals and utility owners and operators." And that is why we are here today.

I want to thank all the witnesses for testifying today and I look forward to highlighting the good work you all are doing to enhance your cybersecurity capabilities and learning about what areas are still a challenge and how the Federal Government can help in mitigating those gaps.

Mr. DONOVAN. The Chair now recognizes the gentleman from New Jersey, Mr. Payne, for an opening statement he may have.

Mr. PAYNE. Good morning. I would like to thank Chairmen Donovan and Ratcliffe for holding today's hearings to assess our ability

to respond to cyber threats. The last time our subcommittee held a joint hearing on the subject was in the 113th Congress, about 3 years ago. What we have learned is that cyber threats are the new frontier of disaster response.

Our legacy response doctrine from the National Response Framework to the Stafford Act are rooted in the era that predates reliance on cyber networks and growing threats posed by sophisticated actors. Despite our best efforts to ensure that our National preparedness doctrine is responsive to evolving threats, it has not kept pace with cyber threats.

My district is rich with critical infrastructure, all of which rely on cyber networks. Within 2 miles, we have major transit systems, chemical facilities, and refineries mixed among homes, schools, and hospitals. A hack of any one of these targets could have devastating, cascading effects and could risk overwhelming our brave first responders. We know that the threat is real.

Earlier this year, Iranian hackers breached the Bowman Avenue's Dam network in Rye, New York. Fortunately, the dam was off-line for repair when the authorities discovered this breach. But I am worried that it is only a matter of time before the hackers are successful, and we need to be prepared when they are.

I applaud efforts at the State level to confront cyber threats head on. Some States, like California and my home State of New Jersey, have established State-level cyber information-sharing centers modeled after the National Cybersecurity and Communications Integration Center, or NCCIC. I would be interested to learn whether these centers facilitate improved information sharing and encourage better relationships among non-traditional partners who would play an important role in cyber response.

At the same time, I would be remiss if I did not note that while States annually indicate that they lack the confidence in their cybersecurity capabilities in the National preparedness report, very few invest homeland security grant funding to address the capability gap. I would be interested in understanding why. Is it because the Federal Government has not provided adequate guidance on how to address the threat or whether the amount of grant funds available after cuts to grant programs in the recent years prevent States from investing in cyber capability?

The witnesses at that hearing made two points that stuck with me: First, the witnesses emphasized that the response to cyber attacks will require people from chief information officers to emergency managers to private-sector partners to break out of their silos and coordinate with non-traditional partners; second, they said that the existing disaster response guidance does not adequately address the complexities of responding to cyber events these days.

I look forward to hearing our witnesses' opinions on how the National Incident Management System, the National Response Framework, and other disaster management doctrine should be updated to reflect the unique qualities of a cyber event. I appreciate the witnesses for being here today, and I look forward to their testimony.

With that, Mr. Chair, I yield back.

[The statement of Ranking Member Payne follows:]

STATEMENT OF RANKING MEMBER DONALD M. PAYNE, JR.

MAY 24, 2016

The last time our subcommittees held a joint hearing on this subject was during the 113th Congress—about 3 years ago. What we learned is that cyber threats are the new frontier of disaster response.

Our legacy response doctrine—from the National Response Framework to the Stafford Act—are rooted in an era that predates reliance on cyber networks and growing threats posed by sophisticated hackers. Despite our best efforts to ensure that our National preparedness doctrine is responsive to evolving threats, it has not kept pace with cyber threats.

My district is rich with critical infrastructure, all of which rely on cyber networks. Within 2 miles, we have major transit systems, chemical facilities, and refineries mixed among homes, schools, and hospitals. A hack of any one of these targets could have devastating cascading effects and could risk overwhelming our brave first responders.

And we know the threat is real. Earlier this year, Iranian hackers breached the Bowman Avenue Dam network in Rye, New York. Fortunately, the dam was off-line for repair when the authorities discovered the breach. But I am worried it is only a matter of time before the hackers are successful—and we need to be prepared when they are.

I applaud efforts at the State level to confront the cyber threat head on. Some States—like California and my home State of New Jersey—have established State-level cyber information-sharing centers modeled after the National Cybersecurity and Communications Integration Center. I will be interested to learn whether these centers facilitate improved information sharing and encourage better relationships among non-traditional partners who would play important roles in a cyber response.

At the same time, I would be remiss if I did not note that while States annually indicate that they lack confidence in their cybersecurity capabilities in the National Preparedness Report, very few invest Homeland Security Grant funding to address that capability gap.

I will be interested in understanding why—is it because the Federal Government has not provided adequate guidance on how to address the threat or whether the amount of grant funds available after cuts to grant programs in recent years prevents States from investing in cyber capabilities?

While I am on the subject of grant funds, I have been outspoken about my opposition to the proposed cuts to the Homeland Security Grant Program as well as the Port and Transit Security Grants. I have serious concerns that the proposed cuts would only further jeopardize whatever progress States and other grantees are making to address cyber threats, and I will be interested in the witness' thoughts on that point.

Finally, as I indicated, our subcommittees held a joint hearing on responding to a cyber attack about 3 years ago. The witnesses at that hearing made 2 points that stuck with me.

First, the witnesses emphasized that a response to a cyber attack will require people—from chief information officers to emergency manager to private-sector partners—to break out of their silos and coordinate with non-traditional partners. Second, they said that existing disaster response guidance does not adequately address the complexities of responding to a cyber event.

I look forward to hearing our witness' opinions on how the National Incident Management System, the National Response Framework, and other disaster management doctrine should be updated to reflect the unique qualities of a cyber event.

Mr. DONOVAN. The gentleman yields.

The Chair now recognizes the Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, the gentleman from Texas, Mr. Ratcliffe, for an opening statement he may have.

Mr. RATCLIFFE. Good morning, everyone. I want to thank Chairman Donovan, Ranking Member Payne, for working with me and with Ranking Member Richmond on putting this issue together today.

I also want to thank the witnesses for being here today. I am looking forward to hearing your testimony.

On the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, we talk a lot about the variety and high number of growing cyber threats that are out there. But today, we are going to hear about the other part of the equation, which includes the people, the hours, the programs designed and dedicated to preparing for and responding to the dangers that these cyber threats pose.

Hopefully, having this discussion at a National level, will help bring to light some of the best practices and most evident areas for improvement at every level of government, whether it be the Federal, State, or local level. Because the truth is, every level of government is constantly having to face and respond to these threats, so we all need to be working together to understand the tactics and techniques and procedures that hackers are using so that we are better equipped to face the threats of tomorrow.

It is important that we spend as much time and energy thinking about the solutions that secure Americans as we do examining the dangers. The purpose of today's hearing is to focus on seeking those solutions to make Americans safer. In that spirit, we are constantly seeking to improve upon and expand the programs and partnerships in both the private sector and State and local governments that function to help keep Americans safe. These partnerships are the nuts and bolts to secure Americans against the havoc that is possible if a bad actor were to successfully disrupt or damage one of the many systems that we rely upon for everyday life, like our water and our power.

What we are hoping to gain from today's hearing is what more we can be doing to further these partnerships and programs. The importance of the flow of information can't be stressed enough, as information is the currency with which security and insecurity is established in today's digital age.

As fast as the bad actors are moving in cyber space, we have to be constantly moving faster to stay ahead of them, and right now we are not. While they have to only be right one time to cause damage, we have to always be resilient and stand perpetually ready with a plan and with answers. I am glad to be having this joint hearing to highlight the interconnectedness of the response plans that are in place in case of a devastating cyber event, and the first responders who carry them out.

At the Federal level, we have the ability to push out and develop plans beyond the capability currently available to the 50 States. But it is the responders already in those areas who will be the first people that those most directly affected will see if a catastrophic cyber attack occurs.

As Chairman Donovan mentioned, the draft National incident response plan, or NCIRP, was delivered to the White House in fall 2009, and in March 2010, an interim draft was released but not approved, subject to on-going review by the administration. It has now been 6 years since the release of the interim draft with stakeholder engagement just now starting. Six years is entirely too long for any type of response plan to sit on a shelf in the White House, but it is especially dangerous in the case of cyber.

In 2014, Congress passed a law to require this cyber incident response plan to be finalized. Clearly, the administration, by not fi-

nalizing this plan doesn't seem to be taking cyber incident response planning seriously. It begs the very obvious questions: What if there is a significant cyber attack in the United States? Does every level of government know their role? And how cyber response will be coordinated?

We are neither too ignorant nor too proud to think that a major cyber event is outside the realm of possibility right now. So I would like to take this moment to convey that we are watching the development of this document very closely.

Look, it is very apparent that we have a lot more work to do. Securing our States from cyber threats now includes entirely new roles and responsibilities that didn't exist 50 years ago. Discussing, examining, and encouraging the programs and partnerships that Americans rely upon is absolutely critical to being able to preserve and guarantee the American way of life.

I look forward to hearing from our witnesses today to learn what more we can and what we should be doing to advance the security of the American people.

Thank you. I yield back.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

MAY 24, 2016

Good morning, I want to thank Chairman Donovan and Ranking Member Payne for working with myself and Ranking Member Richmond on this issue. I also want to thank the witnesses for coming today to speak on this important topic. On the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technology, which I chair, we often discuss the wide variety and high number of cyber threats that are out there and growing. Today, we are going to hear about the other part of the equation, which is the people, the hours, and programs designed and dedicated to preparing for and responding to the dangers that these cyber threats pose.

Hopefully having this discussion at a National level will help bring to light some of the best practices and most evident areas for improvement that will be applicable to every level of government whether it be at the Federal, State, or local level. Because the truth is, every level of government is constantly having to face and respond to these threats. We all need to work together to understand the tactics, techniques, and procedures of hackers in order to better equip ourselves and face the threats of tomorrow.

It is important that we spend as much time and energy thinking about the solutions that secure Americans as we do on the examination of the dangers. The purpose of today's hearing is to focus on seeking those solutions to make America safer. In that spirit, we are constantly seeking to improve upon and expand the programs and partnerships with both the private sector and State and local governments that function to make Americans safe. These partnerships are the nuts and bolts to secure Americans against the havoc that is possible should a bad actor successfully disrupt or damage one of the many systems that we rely on for everyday life such as our water and our power.

What we are hoping to gain from today's hearing is what more we can be doing to further these partnerships and programs. The importance of the flow of information cannot be stressed enough as information is the currency with which security and insecurity is established in today's age. As fast as the bad actors are moving in cyber space, we have to be constantly moving faster to stay ahead of them. While they only have to be right once to do damage, we must be resilient and stand perpetually ready with a plan and with answers.

I'm glad to be having this joint hearing to highlight the interconnectedness of the response plans that are in place in the case of a devastating cyber event, and the first responders who carry them out. At the Federal level we have the ability to push out and develop plans beyond the capability currently available to States, but it is the responders already in the area who will be the first people that those most directly affected will see when a catastrophic cyber attack occurs.

As Mr. Donovan mentioned, the draft National Incident Response Plan or NCIRP was delivered to the White House in the fall of 2009. In March 2010, a draft interim was released but not approved, subject to on-going review by the administration. It has now been 6 years since the release of the interim draft, with stakeholder engagement just now starting. While 6 years is entirely too long for any type of response plan to sit on a shelf in the White House, it is especially dangerous in the case of cyber. In 2014, Congress passed a law to require this cyber incident response plan to be finalized. Clearly, this administration, by not finalizing this plan, does not take cyber incident response planning seriously. It begs the very obvious question "What if there is a significant cyber attack in the United States? Does every level of government know their role and how cyber response will be coordinated?" We are neither too ignorant nor too proud to think that a major cyber incident is outside of the realm of possibility so I would like to take this moment to convey that we are watching the development of this document very closely.

It is very apparent that we have a lot more work to do. Securing our States from cyber threats now includes entirely new roles and responsibilities that didn't exist 50 years ago. Discussing, examining, and encouraging the programs and partnerships that Americans rely on is absolutely crucial in guaranteeing the solvency of our ways of life. I look forward to hearing from the witnesses to learn what more can and should be done to advance the security of the American people.

Mr. DONOVAN. The gentleman yields back.

The Chair recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Mr. Chairman, I ask unanimous consent to submit the gentleman from Louisiana, the Ranking Member, Mr. Richmond's statement into the record.

Mr. DONOVAN. Without objection, so ordered.

[The statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

MAY 24, 2016

In developing policy and budgeting for cyber preparedness and response, it is crucial we know what needs protecting, how badly protection is needed, and what kinds of redundancies can be made available.

For critical infrastructure entities, after knowing what machines are operating on a network, what applications they are running, and what privileges have been established, the posture of cybersecurity for each of these entities and systems networks is key.

Also, for critical infrastructure enterprises and supply chains, the advent of, "bring your own devices", along with the growing sophistication of smart phones and tablets involved in day-to-day infrastructure operations, compounds cybersecurity efforts and increases our resiliency challenges.

Knowing where to devote efforts to protect our information security in critical infrastructure organizations is a core choice, particularly in determining how much defense to commit to the perimeter, and how much to commit to internal threats.

Consider the potential for adversaries to employ countermeasures . . . as defenses are installed on our systems, we must acknowledge that we are dealing with a thinking and competitive opponent in the cyber world . . . and that as we install measures to thwart hackers that very act tends to induce countermeasures from our foes, as hackers probe for ways around or through our new defenses.

As new versions of cyber attacks emerge affecting critical infrastructure, it will be important to have the DHS Industrial Control Systems Computer Emergency Response Teams, or ICS–CERT, and the Joint Interagency Task Force consisting of the National Institute of Standards and Technology, or NIST, the Department of Defense, and the intelligence community, clearly delineate and prioritize their roles in protecting critical infrastructure, and to have that as well-defined as possible.

A good place to start is to build a body of cyber knowledge on how various critical infrastructure cyber systems are likely to fail, which is a necessary prerequisite to preventing failure, and then share that information among all sectors.

Most experts tell us this is a daunting proposition, in light of the fast pace and range of cyber threat vectors that present themselves daily, but we must try.

In closing, any critical infrastructure sector that is prepared to share what went wrong and what could be done better next time, will create the most likely scenario

to produce higher levels of cybersecurity and resiliency for future regional and National cyber emergency situations.

Mr. DONOVAN. Other Members of the subcommittees are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MAY 24, 2016

Over the past 15 years, the Nation has experienced man-made and natural disasters that caused damage beyond our expectations and overwhelmed the response capabilities of the impacted communities. After each disaster—from the 9/11 attacks and Hurricane Katrina to the Boston Marathon bombings and Hurricane Sandy—we take the lessons learned and adjust the response plans so that we are better prepared for the next version of the same event.

Preparing to respond to those kinds of events has become almost routine. We assess terror threats and the potential for various natural disasters. We conduct vulnerability assessments of our communities, and we hone, train, and exercise our disaster response plans. The doctrine guiding how we prevent, protect against, mitigate, respond to, and recover from more conventional disasters is well-established and incorporates important lessons learned from past events.

Unfortunately, National guidance of a similar caliber is lacking for a response to a cyber attack. When I am home in Mississippi, local emergency managers tell me that roles and responsibilities are not clearly defined for a cyber response and that the statutory authority for the Federal Government to render aid to affected States is murky at best.

We need to do better. The frequency of cyber attacks is increasing and the attacks are becoming more sophisticated. I fear a cyber Katrina if we do not establish a "whole community approach" to prevent, respond to, and recover from cyber attacks soon, before hackers disable part of the electric grid, gain control of one of our transit systems, or infiltrate our water treatment facilities.

Addressing the growing cyber threat and equipping emergency managers with the tools they need to effectively respond to disasters triggered by hackers will require at least 3 changes.

First, we have to improve information sharing. Second, we have to improve communication among the emergency response community and non-traditional response partners, including private-sector infrastructure owners and chief information officers. Third, we have to do a better job defining roles, responsibilities, and authorities related to a cyber response.

Late last year, the House of Representatives took an important step advancing those objectives by passing H.R. 3878, the Strengthening Cybersecurity Information Sharing and Coordination in Our Ports Act.

Introduced by Congresswoman Torres, H.R. 3878 would improve information sharing and cooperation in addressing cybersecurity risks at our Nation's ports by directing DHS to establish voluntary guidelines for reporting of cybersecurity risks, implement a maritime cybersecurity risk model, and make recommendations on enhancing the sharing of cyber information.

The legislation also directs the Coast Guard to ensure area maritime security and facility security plans address cybersecurity risks. H.R. 3878, along with several other important pieces of cybersecurity legislation from this committee, has passed the House is currently pending in the Senate. I urge our Senate colleagues to act on these bills before the summer recess.

In the mean time, I am eager to learn from our witnesses about existing challenges in developing response plans for cyber events and what the Federal Government can do to help.

Mr. DONOVAN. We are pleased to have a distinguished panel before us today on this important topic. Mark Ghilarducci serves as the director of the California Governors Office of Emergency Services, a position he has held since July 1, 2013. As a member of the cabinet, Director Ghilarducci serves as the Governor's Homeland Security Adviser, and oversees State-wide public safety, emergency management, emergency communications, counterterrorism efforts, and a State threat assessment system. Mr. Ghilarducci previously

served as the secretary of the California Emergency Management Agency. Welcome, sir.

Lieutenant Colonel Daniel J. Cooney currently serves in the Office of Counterterrorism of the New York State Police. He serves as adviser to the director of the New York State Office of Homeland Security and oversees the staff of the New York State Intelligence Center, New York's fusion center. He has been a New York State police officer for 23 years, and has been awarded a master's degree in security studies from the Naval Postgraduate School. Welcome, Colonel.

Brigadier General Steven J. Spano is president and chief information officer of the Center for Internet Security. Most recently, he served as the general manager for defense and national security for Amazon Web Services Worldwide Public Sector. Prior to Amazon Web Services, General Spano served over 28 years in United States Air Force in a variety of leadership roles. He retired in 2011 from Air Force combat command where he served as the director of communications. Welcome, General, and thank you for your service to our country.

Mr. Mark Raymond began serving as the chief information officer for the State of Connecticut Department of Administrative Services, Bureau of Enterprise Systems and Technology on June 2, 2011. He has over 2 decades of technology and business experience consulting in New York, Connecticut, and Massachusetts; that includes working in the areas of finance, payroll, human services, budgeting, procurement, human services revenue, and transportation. As a consultant, he has worked with Federal agencies, including the United States Treasury, Federal Highway Administration, National Highway Traffic Safety Administration, and the U.S. Department of Transportation. Welcome, sir.

Mr. Robert Galvin serves as the chief technology officer for the Port Authority of New York and New Jersey, a position he has held since December 2013. In this capability, he provides oversight, direction, and management for all of the agency's technology, information systems, and technology service delivery. Prior to joining the Port Authority, Mr. Galvin served as the chief technology officer at the New York City School Construction Authority.

The witnesses' full written statements will appear in the record. The Chair now recognizes Mr. Ghilarducci for 5 minutes.

STATEMENT OF MARK GHILARDUCCI, DIRECTOR, EMERGENCY SERVICES, OFFICE OF THE GOVERNOR OF CALIFORNIA

Mr. GHILARDUCCI. Okay. Well, good morning, Chairman and distinguished Members of the subcommittee. Mark Ghilarducci, and I am the director of OES in California. I am here today on behalf of the National Emergency Management Association, which represents State emergency management directors of the 50 States, territories in the District of Columbia.

I appreciate the opportunity to come before you today to discuss concerns related to the consequences of a cyber attack and the role of emergency management community in responding to this unique and evolving threat. As our lives, our systems, our critical infrastructure, as well as our emergency management coordination and

communication platforms become more and more integrated with and dependent upon the Internet of Things, so does the proliferation of threats and complexities from cyber attacks, and, of course, the need to continue to evolve capabilities and countermeasures.

These emerging threats, ushered in by advancements in technology, are a challenge for emergency management at a time when the adversary is unpredictable, asymmetrical, and very active. The range of threat actors, the methods of attack, targeted systems, and victims are ever-expanding. Because information systems are now the backbone of critical infrastructure in the United States, we are at an age of transitioning into next generation public safety due to its significance to National and economic security.

Of concern to the emergency management community is the threat and potential cascading impacts of a cyber attack to our critical infrastructure systems. Lifelines and assets, whether physical or virtual, by actors with malicious intent to exploit vulnerabilities, disrupt or destroy control systems, or incapacitate the delivery of essential services, all which places the security and safety of our communities, our citizens, and the economy at great jeopardy.

Like the consequences of other asymmetrical terrorist threats, consequence management of cyber attacks is challenging due to its unpredictable and ubiquitous nature. It requires a considered and coordinated effort of collaborative planning, risk identification and management, communications, information sharing, interdiction, response and mitigation.

As information technology becomes increasingly integrated with physical infrastructure operations, emergency management must plan and prepare for the increased risk for large-scale or high-impact events and that cascading impacts that could harm or disrupt services, or worse, cause fatalities or destruction in our communities. Widespread and long-term power outages, loss of water telecommunications systems, disruption of public health or public safety systems, destruction of control systems, interruption of food production and distribution, and/or the movement of commodities or people are just a few potential consequences of a successful cyber attack on our critical infrastructure; all consequences emergency management must consider, plan, and prepare for.

There is no doubt that the potential aftermath of a significant cyber attack resulting in physical consequences will challenge existing hierarchies, dependencies, reporting structures, and planning assumptions. Emergency managers will need to leverage all necessary local, State, and private-sector resources; implement redundant capabilities for continuity of operations, and possible continuity of Government; and will require Federal support for both technical and Stafford Act assistance. But it remains unclear today how the consequences of an attack will be defined and meet requirements for Stafford Act assistance.

Another challenge facing State emergency management and homeland security organizations is the ability to effectively manage cyber risk as it is not possible to eliminate it. Like many other hazards, both natural and human-caused, State leaders must build cybersecurity systems, communication, and information capabilities, and procedures designed to not only preempt attacks through adequate cyber defense systems, but enable an organization to with-

stand attacks when they succeed, or, in other words, to build cyber resilience.

A logical approach to cybersecurity preparedness and incident response begins at all levels of government and in partnership with the private sector. As the Federal Government continues to build its capabilities, policies, and strategies, it has left States to build cybersecurity capacities with limited resources, trained personnel, and guidance or a specific blueprint to follow, all while facing threat actors who are advanced, nimble, quick to adapt, and overcome defenses in intending to do harm to private citizens and government services.

Dedicated cybersecurity grants for planning and operational capabilities, developing, training, and supporting the blueprint of a workforce of cyber warriors, as well as identified post-event, remediation funding streams that do not currently exist, but are absolutely necessary to ensure States are prepared to adequately build cyber capabilities and defenses, this needs to be a priority.

For example, in California, one key cybersecurity capability we recently stood up is the California Cybersecurity Integration Center as a way to measure our whole-of-Government and public/private sector integration approach. The Cal–CSIC, as it is called, integrates critical cybersecurity functions directly impacting my ability to manage both the homeland security and emergency management portfolios in California.

It is co-located with the California State Threat Assessment Center, our State's primary fusion center, which maximizes information sharing and allows for communications to be properly vetted and classified, ensuring conductivity and information sharing between the intelligence community, law enforcement, and California's other 5 regional fusion centers, and it expands upon our current capabilities focused specifically on protecting California.

It resides within our homeland security division, aligned with DHS's organizational structure, and integrates both the academic and private sectors. It provides a State-wide nexus for cyber threat information sharing for the State of California, our critical infrastructure sector partners that provide essential services, our 9–1–1 system, the intelligence community, and law enforcement.

It promotes proactive situational awareness of the cyber threat, cyber hygiene, and best cybersecurity practices, and it augments the State Emergency Operation Center during activations for emergency incidents through systems analysis and resilient communication. Most importantly, it provides support to our State's emergency support Function 18, the component of the State emergency plan that focuses on the impacts and countermeasures related to a major cyber attack.

A key element for success of this capability, but, nonetheless, a challenge we are working with, is establishing a blueprint for integrating desperate agency sector efforts and mission sets into a unified, coordinated, and streamlined operation that reflects the full intelligence cycle from collection analysis to dissemination that supports situational awareness and the complete emergency management cycle.

The Cal–CSIC design forces collaboration between all of the major State agencies and sector representatives that have a role in

cybersecurity through protocols and the integration of respective cybersecurity staff. This partnership forces down the silos and stovepipes and generates a level of collaboration on the cyber front not seen before in our State government, which helps to define the roles and responsibilities of each organization during cyber events at a State-wide significance.

As well, through partnerships with the National Cybersecurity Communications Integration Center and a multi-State information-sharing analysis center, the Cal–CSIC addresses prevention, protection, response, and recovery while providing detail on cyber threats and trends specifically to California. The Cal–CSIC can use this analysis to notify residents of current threats and how to prevent and mitigate those threats.

The consolidation of National, State, and local cyber threat data will provide a more strategic picture benefiting prevention and response. To further our resiliency platform, we are also moving to implement the DHS and CCIC cyber hygiene campaign across California's State agencies and departments.

In closing, collaboration, coordination, training, planning, clear protocols, real-time information sharing, and processing of indicators of attack are essential elements of a robust cybersecurity and emergency management posture for all governments. Linking up critical infrastructure assessors and analysis, and analysts with cybersecurity personnel and emergency planners also needs to be approached holistically and sustainably.

At all levels, Government must be prepared to deal with an ever-changing and increasingly complex set of challenges that test our traditional approaches to emergency preparedness and response to disasters. Changing demographics, emerging technologies, and the interdependencies of our infrastructure and systems create vulnerabilities that defer from those of the past.

The cyber threats facing our Nation are not subsiding, but, in fact, are evolving in such a way that these threats demand purposeful, proactive action, adequate funding support, and a more forward-thinking and collaborative approach at all government levels and critical infrastructure sectors. This has to be one team, one fight.

Thank you.

[The prepared statement of Mr. Ghilarducci follows:]

PREPARED STATEMENT OF MARK GHILARDUCCI

MAY 24, 2016

INTRODUCTION

Thank you Mr. Chairman, Ranking Member, and distinguished Members of the committee. My name is Mark Ghilarducci, and I am the director of the Governor's Office of Emergency Services as well as the Homeland Security Advisor to Governor Jerry Brown for the State of California.

I am here on behalf of the National Emergency Management Association (NEMA), which represents the emergency management directors of the 50 States, territories, and District of Columbia. NEMA's members, many of whom, like me, also serve as Homeland Security Advisors, are prepared to deal with an ever-changing and increasingly complex set of challenges that test traditional approaches to natural and man-made disasters. I appreciate the chance to come before you today to discuss the current concerns related to consequences of cyber attacks and the role of the emergency management community in responding to these unique events.

WHERE ARE WE NOW?

We are witnessing a more diverse array of threats than at any other time in history. The skill, speed, and adaptability of these threats are challenging our defense in ways we have not seen before. The emerging threat landscape for the Nation is characterized both by standing threats, as well as dynamic and fluid ones ushered in by advancements in technology. As we witness our society make unprecedented advancements in innovation, we become more and more reliant on information technology and increasingly vulnerable to devices that are developed and distributed with minimal security requirements. The ranges of threat actors, methods of attack, targeted systems, and victims are also expanding.

We are transitioning into Next Generation Public Safety, and information systems are now the backbone of National and economic security in the United States. Our success as a Nation depends upon critical infrastructure functioning reliably at all times. The threat to this infrastructure by those with malicious intent to exploit vulnerabilities, steal information and money, and disrupt, destroy, or threaten the delivery of essential services are unlike any other. Cybersecurity threats exploit the risks associated with the increased complexity and connectivity of these systems, which places our Nation's security, economy, and public safety at greater risk.

This risk affects both the private and public sectors. We have seen "Ransomware" in the public and private sector in California and across the United States designed to prevent public and private institutions from accessing their own data. Criminal tools and malware are increasingly being discovered on State and local government networks.

As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide-scale or high-impact events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. Long-term power outages, loss of water, and disruption in the movement of goods, services, and people as a result of disrupted transportation systems are a few of the potential consequences of a successful cyber attack on our critical infrastructure.

The aftermath of a cyber event with physical consequences will challenge existing hierarchies, reporting structures, and planning assumptions. In the event of an incident, most emergency managers will turn to the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Pub. L. 92–288) for Federal assistance, but unless the consequences of a cyber attack have large-scale physical consequences, funds from the Stafford Act will be limited.

Many of the fixes, whether administrative or legislatively initiated, throughout the last few years seem to only address the prevention and preparedness side of cybersecurity. While the pre-event aspects of cybersecurity maintain a high level of importance, so too will the post-event considerations especially when considering the potential disastrous physical consequences of a cyber attack.

CURRENT CHALLENGES FACING STATE EMERGENCY MANAGEMENT/HOMELAND SECURITY

While cybersecurity and cyber response capabilities continually rate very low in FEMA's annual National Preparedness Report, identifying the capability gaps and needs is often a difficult task for State and local government and has limited measurable improvement toward the National Preparedness Goal.

- Cyber risk must be managed as it is not possible to eliminate; the diverse possibilities of malicious actors penetrating, intruding, and circumventing from the inside continue to grow and will hold every internet communication technology system at risk for years to come.
- The risk calculus employed by some State and local organizations does not adequately address the top cyber threats or systemic interdependencies across critical infrastructure sectors.
- State leaders must accept the predictability of cyber attacks, and build security systems and procedures that can not only preempt attacks through cyber defense, but enable organizations to withstand attacks when they succeed, or in other words build cyber resilience.
- A coordinated approach to cybersecurity preparedness and incident response is in its nascent stages, even at the Federal level. As the Federal Government is still working to build Federal institutions, policy, and strategy, it has left States to build cybersecurity capacities with limited resources and trained personnel, and a lack of guidance or successful blueprint to follow—all while facing threat actors who are advanced, nimble, quick to adapt and overcome defenses and who intend to harm private citizens and Government services.

- A dedicated cybersecurity grant funding stream would also ensure States were prepared to adequately build their cyber capabilities and defenses. Currently there is no funding dedicated specifically to this priority.
- States are still playing catch-up in developing a "whole-of-Government," Statewide approach to cybersecurity.

BEST PRACTICES AT THE STATE LEVEL/ON-GOING EFFORTS TO IMPROVE RESILIENCE

I am excited to discuss some California examples of best practices we are implementing to ensure the Golden State is safe and secure and cyber resilient.

- *Cyber Hygiene Partnership with DHS's National Cybersecurity Communications Integration Center (NCCIC).*—We are moving to embrace and implement the DHS's National Cybersecurity Communications Integration Center's Cyber Hygiene campaign across California State Agencies. Working with NCCIC staff, we are working to push this program to all of California's State executive agencies as a start. This program is voluntary, but it will allow us to baseline State agencies' vulnerabilities and provide an overall State profile for a majority of public-facing assets. This is a good metric for performance and will help our team develop a long-term State strategy. To date, only 13 organizations across all of California are taking advantage of this Federal program.
- *Integrating and Automating Data Feeds.*—One of the things we are spearheading in California is a Cal OES-supported project at our California fusion centers that supports automating cyber threat intelligence, as we believe that is a fundamental facet to cyber resilience on all levels of Government. We must get past the manual human-to-human transactions that continue to dominate State and local cyber information sharing and move towards an automated cyber threat intelligence design, which we believe should anchor States' resilience and inform cyber response efforts. We are also working, in conjunction with DHS/NCCIC, on a program called Automated Indicator Sharing Initiative, which shares observable cyber "indicators" to also help bolster the State's defense through a machine indicator exchange.
- *California Cybersecurity Integration Center (Cal–CSIC).*—We recently stood up our California Cybersecurity Integration Center (Cal–CSIC) (pronounced Cal–SICK) as a way to mature this approach, but one of the biggest challenges we face is establishing a blueprint for integrating disparate efforts and mission sets into a unified, coordinated, and streamlined operation that reflects the full intelligence cycle from collection, analysis, to dissemination, and that supports a robust cyber response.

The Cal–CSIC does the following critical cybersecurity functions, directly impacting my ability to manage both the homeland security and emergency management portfolios in California:

- Expands upon current capabilities in our State's primary fusion center to build out a cybersecurity center focused specifically on protecting California.
- Resides within the Cal OES Homeland Security Division, aligning with DHS's organizational structure.
- Its co-location with the California State Threat Assessment Center (STAC) allows for communications to be properly vetted and classified, ensuring connectivity between the intelligence community, law enforcement, and fusion centers.
- Provides a State-wide nexus for cyber threat information sharing for the State of California, intelligence community, and law enforcement.
- Promotes situational awareness of cyber threats, cyber hygiene, and best cybersecurity practices for all California organizations.
- Augments the State Operations Center activities during emergency incidents through media analysis and resilient communications.
- Marries our critical infrastructure analysts and assessors to our cybersecurity professionals to create a novel holistic security assessments capability.

The National Cybersecurity Communications Integration Center (NCICC) and Multi-State Information Sharing Analysis Center (MS–ISAC) operate as focal points for cyber and physical protection of Federal, State, local, Tribal, territorial government (FSLTT) and Critical Infrastructure/Key Resources (CI/KR) network, storage, and communications systems and seeks to address prevention, protection, response, and recovery.

The Cal–CSIC will address prevention, protection, response, and recovery while providing detail on cyber threats and trends specifically to California. The Cal–CSIC can use this analysis to notify residents of current threats and how to prevent and mitigate those threats. The consolidation of National and State cyber threat data will provide a more strategic picture benefitting prevention and response. The

NCCIC will also be a partner in the Cal–CSIC as will other Federal agencies to ensure for real-time collaboration and coordination that is needed.

The Cal–CSIC design forces collaboration between all of the major State agencies that have a role in cybersecurity because those agencies have, or are going to, embed their cybersecurity staff there. This partnership will force down the siloes and stove pipes, and generate a level of collaboration on the cyber front not seen before in State government, which helps to define the roles and responsibilities of each agency during cyber events of State-wide significance.

- *Governor's Cybersecurity Task Force*.—This task force facilitates cybersecurity outreach to private industry, academic, law enforcement, and Government partners both inside and outside of California. The Governor's Cybersecurity Task Force is a public-private partnership that serves as the advisory body to the Cal–CSIC to raise awareness of new threats and mitigation techniques.

Sometimes, simply assembling the right players to have the tough conversations is half the battle. In this case, educating cybersecurity professionals about emergency management, and vice versa, remains a significant challenge. This is why the State of California created the Governor's Cybersecurity Task Force to be wide-reaching, pairing up local emergency management experts with cybersecurity professionals to collaborate on the bigger strategic questions. It has made a tremendous impact, but more work needs to be done to align State and local defense with Federal efforts.

RECOMMENDATIONS FOR THE FUTURE

As a Nation we must map out a comprehensive collaborative strategy that delivers timely, cost-effective, and actionable responses. This will strengthen our National security by better preparing us to respond to potential disruptions that would have cascading consequences on the country. Collaboration, employee cybersecurity training, enterprise defense-in-depth, and real-time information sharing and processing of indicators of attacks are essential elements of a robust cybersecurity posture for all governments. Marrying critical infrastructure assessors and analysts with cybersecurity personnel also will breed unique and nuanced synergies by approaching the problem holistically. This would include:

- Review current statutory authorities for emergency management personnel and ensure resources can and will be available to respond to a cyber attack.
- Encourage information sharing between intelligence and operational officials to ensure stovepipes do not unnecessarily hinder collaboration and integrated planning.
- Coordinate with State and local officials to ensure their priorities are included in legislative reforms and changes within the administration's cybersecurity policies.
- Avoid mandating State and local governments without also providing Federal funding.
- Provide adequate and sustainable funding to ensure for the development of robust cybersecurity interdiction, response and preparedness/education systems at the State and local levels, to better inform and empower communities, where the consequences of cyber attacks are most impactful.
- Ensure that we communicate to American citizens our commitment to protecting their privacy, when incorporating emerging technology—specifically, the Internet of Things or "smart devices."

While these devices maximize efficiency and carry the allure of convenience, we must incorporate the benefits of innovative technology into State and local government with the utmost appreciation for their potential to threaten data privacy, data integrity, or continuation of services. This also opens vulnerabilities by allowing threat actors to not only steal data, but also, manipulate it. Threat actors almost certainly will adapt and introduce new tactics that will challenge our defenses so we must seize the opportunities to implant past intelligence from cybersecurity investigations back into the intelligence cycle for further analysis and dissemination.

CONCLUSION

At all levels, Government must be prepared to deal with an ever-changing and increasingly complex set of challenges that test our traditional approaches to emergency preparedness and responses to disaster. Capability, experience, and flexibility are critical in dealing with emerging issues and the unknown. Changing demographics, emerging technologies, and the interdependencies of our infrastructure and systems create vulnerabilities that differ from those of the past. The cyber threats facing our Nation are evolving in such a way that demands purposeful action and a more forward-thinking approach in our National preparedness efforts.

I appreciate the opportunity to testify before you today and stand ready to answer any questions the committee may have.

Mr. DONOVAN. Thank you, Mr. Ghilarducci.

The Chair now recognizes Lieutenant Colonel Cooney for 5 minutes.

STATEMENT OF DANIEL J. COONEY, ASSISTANT DEPUTY SUPERINTENDENT, OFFICE OF COUNTER TERRORISM, NEW YORK STATE POLICE

Mr. COONEY. Good morning, Chairman Donovan, Ranking Member Payne, Chairman Ratcliffe, and Members of the subcommittees. Thank you for inviting me to testify today.

My name is Dan Cooney. I am a lieutenant colonel with the New York State Police responsible for overseeing the New York State Intelligence Center or NYSIC, the State's designated fusion center, which is staffed by approximately 90 individuals, drawn from nearly 20 law enforcement and homeland security agencies at the local, State, and Federal levels.

Since we opened our doors in 2003 as one of the Nation's first fusion centers, NYSIC has maintained an all-crimes approach with the ultimate goal of preventing criminal and terrorist activity in our State, and supporting our partners' on-going law enforcement investigations.

The New York State Police has long had a computer crimes unit. NYSIC incorporated cyber threat intelligence into its mission in 2014 by creating a cyber analysis unit when the NYSIC had just moved to co-locate with the Center for Internet Security and the Multi-state Information Sharing and Analysis Center.

Our approach is based on partnerships, intelligence production, and outreach. To further our outreach, NYSIC spearheaded creation of the New York State cyber partners working group, which meets monthly and is comprised of State and Federal Government law enforcement, homeland security, and information technology personnel, and a National Guard.

As the intelligence center, our role is to take the lead in developing cyber intelligence products for both the technical and nontechnical audiences, and we leverage the partnerships formed through this group to accomplish this mission.

The NYSIC also relies on National cyber information-sharing networks. Routinely, we access the National Fusion Center Association's cyber intelligence network through which over 250 Federal, State, and local law enforcement members act as a virtual fusion center, utilizing a cloud service provided by the homeland security information network to share cyber threat intelligence in real time at the "For Official Use Only," or FOUO level.

Within the State, our distribution lists are separated by sector and between technical and nontechnical audiences to ensure recipients receive exactly the information they need: Actionable intelligence for IT staff, so they can deploy appropriate prevention or mitigation controls; and more strategic information on trends in cyber actors' tactics, techniques, and procedures for executives and policy makers to better inform policy decisions and resource allocation.

NYSIC's intelligence liaison officer network maintains points of contact in fire, EMS, and emergency management agencies in each county with whom we engage in 2-way threat information sharing. Additionally, nearly all of the 500-plus law enforcement agencies in New York State have a designated field intelligence officer that regularly communicates with the NYSIC. More technical products are shared directly with county chief information security officers.

At both the fusion center and across State agencies, New York State is sharing more information more effectively than ever before. Despite a constantly changing environment, we have made excellent progress. But I want to highlight two specific areas for continued growth from the full statement I submitted on the record.

First, the information-sharing lessons of the last 13 years in the counterterrorism space must be applied to cybersecurity today. At the State level, the fusion center is DHS's single point of contact for terrorism-related information, and we know from where within DHS this information is coming. This is not yet the case with cyber threat information, and more often than not, the fusion centers do not receive cybersecurity intelligence information in a timely manner. The more information that fusion centers receive, the more we can share with agencies and businesses within our State, allowing us to close the current intelligence gaps, and push information to smaller entities that direct Federal sharing currently does not reach.

Second, we observe a large amount of cyber threat information is Classified. While fusion centers have the capability to receive Classified documents, we cannot share useful contents with many of our customers unless the classification is downgraded.

On behalf of New York's fusion center and as part of the larger National network of fusion centers, thank you for this opportunity to speak before your subcommittees, and I welcome any questions.

[The prepared statement of Mr. Cooney follows:]

PREPARED STATEMENT OF DANIEL J. COONEY

MAY 24, 2016

Good morning Chairman Donovan, Ranking Member Payne, Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittees: My name is Dan Cooney and I am an assistant deputy superintendent with the New York State Police, responsible for overseeing the New York State Intelligence Center, the State's designated fusion center. Thank you for inviting me to speak today about our cyber threat information and intelligence-sharing efforts.

The New York State Intelligence Center, or "NYSIC", is managed by the New York State Police and staffed by approximately 90 people representing nearly 20 law enforcement, homeland security agencies at the local, State, and Federal levels. Since we opened our doors in 2003 as one of the first fusion centers in the Nation we have maintained an "all-crimes" approach, with the ultimate goal of preventing criminal and terrorist activity in our State and supporting our partners' on-going law enforcement investigations. We are primarily responsible for supporting the 57 counties outside New York City, but we work closely with our New York City Police Department colleagues on New York City-based issues.

NYSIC incorporated cyber threat intelligence into its mission in 2014 by creating a Cyber Analysis Unit. The catalyst was two-fold: We recognized the need to dedicate resources to the growing threat of cyber attacks, and we had just co-located with the Center for Internet Security and the Multi-State Information Sharing and Analysis Center (MS–ISAC), which the U.S. Department of Homeland Security has designated as the cybersecurity information sharing and analysis center for State, local, Tribal, and territorial governments. This provided a timely opportunity for us to learn best practices from top cybersecurity experts. Over time, we were able to

staff the unit with an Investigator and 4 intelligence analysts who possess a mix of specialized technical knowledge or intelligence and analysis experience, a hiring model that has worked well. Our approach is based on partnerships, intelligence production, and outreach, and I will highlight a few examples of the benefits to the State's cybersecurity efforts.

BEST PRACTICES IN INFORMATION-SHARING EFFORTS

The New York State Police has long had a Computer Crimes Unit, and other agencies in New York have worked on cyber threats for some time. We have worked to bolster our relationships with other agencies, not only to learn from them, but to ensure proper information sharing, identify collaborative opportunities, and avoid duplication of effort. To that end, the NYSIC spearheaded the creation of the New York State Cyber Partners Working Group. This group of State and Federal Government agencies—including law enforcement, homeland security, information technology and the National Guard, to name a few—formally meets on a monthly basis to review cyber threat intelligence and discuss training, exercise and joint project opportunities. As the intelligence center, our role is to take the lead in developing cyber intelligence products for both technical and non-technical audiences, and we leverage the partnerships formed through this group to develop and share intelligence. The Cyber Partners Working Group also joins together for training and exercises. NYSIC, along with its working group partners, has participated in table-top and National-level full-scale cyber-related exercises, as both observers and participants. Examples include GridEx III, Cyberstorm V, and New York agency-specific tabletops.

Effective State and Federal collaboration is also vital to confronting these challenges. For example, recently NYSIC and its State and Federal partners collaborated on the production and dissemination of a joint cyber intelligence bulletin detailing the analyses of detected malware. During the analysis, which determined the malware was a well-documented downloader and credential stealing Trojan, an encrypted file was discovered. Encryption often prevents further investigation; however in this case the team obtained a tool from a partner agency that allowed us to decrypt the file. The file revealed specific and actionable data that could protect IT assets. The NYSIC published these findings as a joint cyber intelligence bulletin and received positive feedback from recipients.

The NYSIC also relies on National cyber information-sharing networks. Routinely, we access the National Fusion Center Association's Cyber Intelligence Network (CIN), which is a relatively new network of fusion center cyber analysts, to ascertain whether the intelligence we are developing in New York may be part of a broader trend. The CIN is comprised of over 250 Federal, State, and local law enforcement members who focus on cyber crimes. These members come together and act as a Virtual Fusion Center utilizing a cloud service provided by the Homeland Security Information Network (HSIN) to share real-time cyber threat intelligence in support of an incident, event, or mission. This level of cyber threat information sharing was impossible only a few years ago, yet now is becoming routine.

There are several instances in which the CIN collaborated during high-profile events to great effect. For example, the CIN launched the HSIN's secure, web-conferencing platform, called CINAWARE, in response to Distributed Denial of Service (DDoS) attacks launched by cyber hacktivists against several State and local government networks which included law enforcement and emergency medical service entities that were responding to an incident. The CIN immediately began sharing real-time intelligence on the attacks with the relevant local agencies. The National Fusion Center Association reports that more than 350 individuals from fusion centers and other Federal, State, and local agencies around the country participated in the CINAWARE room over a period of several weeks, with an average of 50 to 90 users in the room at any given time. The room was supported 24/7, which included overnight support from the MS–ISAC. During that period, more than 250 queries were submitted and answered via the CINAWARWE room, enabling rapid sharing of information with decision makers. Leaders in State, local, and Federal agencies were consistently briefed on the information from the CINAWARE room.

Since that event, the CINAWARE room on HSIN has been opened to support the response to the Vikingdom DDoS attacks against State and local networks across the country, the sharing of cyber-specific information related to the Paris Bombings, and to support the law enforcement and homeland security mission for Super Bowl 50. The CIN also facilitates daily sharing throughout the country of indicators of system-compromise identified in discrete geographic regions, issues and responds to Requests for Information, and acts as a team of subject-matter experts to support

local operations. All of this sharing occurs between fusion centers utilizing the Federal platform, HSIN, and occurs at the For Official Use Only (FOUO) level.

Similarly, the NYSIC's co-location with the Center for Internet Security and the MS–ISAC allows our staff to walk downstairs and talk with their intelligence or operations analysts about Nation-wide reporting and how it may impact New York State. Any relevant, sharable information these networks provide NYSIC ultimately benefits our Cyber Partners Working Group and the State's broader cybersecurity prevention efforts.

This intelligence is of limited use, however, if we cannot provide it to consumers and decision makers. Equally as important is communication with those outside of NYSIC. The NYSIC team is constantly meeting and briefing local governments and private critical infrastructure sectors on cybersecurity concerns. Participants leave with contact information needed to build distribution lists for intelligence products. Our distribution lists are separated by sector, and between technical and non-technical audiences, to ensure recipients receive exactly the information they need. We provide IT staff with actionable intelligence that can be cross-referenced with traffic on their networks, so they can deploy appropriate prevention or mitigation controls. Other partners, such as executives, appreciate more strategic information on trends in cyber actors' tactics, techniques, and procedures relevant to their sectors that can help inform better policy decisions. We listen to their feedback and tailor our intelligence products appropriately.

The NYSIC Cyber Analysis Unit may receive or develop intelligence that is particularly relevant to the first responder community, or a subset thereof. For the Fire/EMS/Emergency Management agencies in New York, our team leverages NYSIC's Intelligence Liaison Officer (ILO) network—points of contact in each county from those 3 disciplines that participate in two-way sharing of threat information with our center. We educate them on cyber threat reporting and the types of technical and analytical support NYSIC can provide. For example, we crafted a cyber bulletin distributed specifically to 9–1–1 call centers with an "E–911" capability based on our receipt of threat and vulnerability information relevant to technology that is employed.

Information specific to law enforcement is pushed to agencies in the field using another outreach program called the Field Intelligence Officer (FIO) program. In support of this program, nearly all of the more than 500 law enforcement agencies in New York has a designated FIO that regularly communicates with the NYSIC to advance the homeland security and counter-terrorism mission. We utilize these members to share cyber information in their jurisdictions as well. More technical products, which may include vulnerability and consequence information, are shared directly with county Chief Information Security Officers (CISOs).

New York State is currently working to expand its information sharing with the health care sector—both public- and privately-owned facilities. The NYSIC is finding that this sector is willing to partner with the State to discuss intelligence requirements, information sharing, training opportunities, and best practices in mitigating cyber threats.

RECOMMENDATIONS FOR CONTINUED GROWTH IN INFORMATION SHARING

New York State has made significant strides in building its cybersecurity capabilities, both at the fusion center and across State agencies. We are sharing more information more effectively than ever before. Policies and best practices have been developed by consensus through multilateral and interagency policy bodies and professional associations. They are reinforced through daily engagements between Federal, State, local, and private-sector partners. Despite a constantly-changing environment we have made excellent progress.

In order to build upon our successful efforts, we have identified 4 areas for continued growth.

First, information-sharing regarding cyber threats between the Federal Government and the States should be further streamlined. The information-sharing lessons of the last 13 years in the counter-terrorism space must be applied in the cybersecurity today. In 2003, as the first New York State fusion center director, I remember working through information-sharing issues with DHS, FBI, and others. Ultimately, an agreed-upon vertical information-sharing pathway was developed between Federal partners and the fusion centers. At the State level, the fusion center is DHS's single point of contact for terrorism-related information, and we know from which subset of DHS to expect information. This is not yet the case with cyber threat information. There are many entities within DHS that gather, analyze, and disseminate various types of cyber threat intelligence, whether it's tactical indicators of compromise, strategic intelligence assessments, or organizing outreach campaigns

with private-sector entities in our jurisdiction. Given this information—whether it is raw information or finished intelligence—does not come together in one place at the Federal level with a designated unit to ensure rapid communication with the fusion centers, more often than not the centers do not receive information in a timely manner. This problem is exacerbated by the fact that other Federal agencies also have a cyber mission, and many have not yet built relationships with the fusion centers like DHS or FBI have over the last 13 years. This includes sector-specific agencies like Energy, Treasury, and Health and Human Services that play an important role in protecting key sectors of the Nation's critical infrastructure and economy, and who conduct outreach and information dissemination campaigns with private-sector entities under their jurisdiction. Any steps that DHS can take to streamline the overall Federal cyber intelligence-sharing processes with the fusion centers will help States and our local partners better understand the current threat landscape and more efficiently align our own cyber information sharing with the private sector. Working together will better enable us to protect against and respond to inevitable cyber attacks. The more cyber threat intelligence that fusion centers receive, the more we can share with agencies and businesses in our jurisdictions. This will close intelligence gaps and help us communicate threats to smaller entities that Federal information-sharing currently does not reach.

Second, we must also continue to evaluate how we share Classified cyber-threat intelligence from the Federal Government to the fusion centers. There is no central Federal system that stores indicators of compromise against which fusion center cyber analysts can run comparisons and lookups. The National Network of Fusion Centers does not have a space on the National Cybersecurity and Communications Integration Center (NCCIC) floor, and therefore lacks access to that critical data source which is available to other Federal information-sharing partners. The network has interactions at the DHS Office of Intelligence and Analysis' Cyber Intelligence and Analysis Division (CIAD), but that interaction primarily occurs at the FOUO level and involves information being shared up to the Federal level, but not necessarily back down. Additionally, we observe that a large amount of cyber threat information is Classified. While the NYSIC understands why that might be the case, the Federal community needs to continue to focus on creating Unclassified tear lines of actionable intelligence. The fusion centers may have the capability to receive Classified documents, but cannot share useful contents with many of its customers unless the classification is downgraded. We would be pleased to work with authors of Classified documents to develop Unclassified actionable information for our non-cleared partners. I believe there has been some effort to share more Unclassified indicators based on recent production efforts by one Federal agency, and I hope that effort continues across the Federal community.

Third, we need to continue our efforts to share information with local and county governments and private sector. We need to make sure there is consistency, and not confusion, regarding "who to call" when a local government or private entity experiences a cyber incident. We successfully worked through similar issues in the counter-terrorism area and I believe collective development of clear guidance would better serve our customers.

Finally, the parallels between counter-terrorism and cyber extend beyond information sharing. Adequate cyber preparedness requires wide-spread implementation of best practices and mitigation efforts, which invariably can exceed the capacity of local and county governments facing a growing myriad of threats. In our ever-more connected world, your network is only as strong as its weakest interconnection, yet implementing strong cybersecurity solutions is often costly. As we continue the hard work of policy development and adoption of best practices, the need for Federal Government support of State and local cybersecurity preparedness should not be overlooked. Much the same way the DHS Homeland Security Grant Program provides essential Federal support for counter-terrorism initiatives, similar support for cybersecurity would further enhance the capacity of States, fusion centers, and local governments to prevent and respond to cyber incidents that threaten our Nation's critical infrastructure and economy.

Thank you for this opportunity to speak before your subcommittees. On behalf of New York's fusion center, and as part of the larger National Network of Fusion Centers, I appreciate the invitation to participate in this discussion and I welcome any questions you may have.

Mr. DONOVAN. Thank you, Lieutenant Colonel.

The Chair now recognizes General Spano for 5 minutes.

STATEMENT OF BRIGADIER GENERAL STEVEN SPANO, (RETIRED, USAF), PRESIDENT AND CHIEF OPERATING OFFICER, CENTER FOR INTERNET SECURITY

Mr. SPANO. Mr. Chairman, Ranking Members, Members of the committee, I am Steve Spano, the president and chief operating officer for the Center for Internet Security, or CIS. I appreciate the opportunity to share our thoughts on the state of National cybersecurity, and offer a number of suggestions and address some of the challenges that lie ahead.

I would like to talk a little bit about our organization, what we do, our primary ambition, and how that feeds into our assessment of the current state of cybersecurity in the area that we know best, which is State, local, Tribal, and territorial governments. Then I will talk a little bit about how we service and are enhancing that mission, working with our partners, like the fusion center, and State and local governments, and then offer some ideas moving forward strategically that perhaps this committee can begin to address as the challenges we face continue to grow.

About CIS, it began in 2000 out of the passion and the belief that everybody deserves a secure on-line experience. The 100-plus professionals work collaboratively to enhance the cybersecurity mission, readiness, and response, and we do that in 3 core areas: Beginning from the foundation, we believe that it is inherently practical and important to establish a secure framework to build your cyber strategy on and evolving to.

We call that security framework the critical security controls, or the CIS controls. They are a set of prioritized actions that organizations of any size can take in a priority order to deal with the current threats that exist in today's environment. That security framework serves as a foundation for some of the products and services that we offer, one such being the security benchmarks, which are automated configurations that lock down devices, operating systems, and software. So these security benchmarks help execute and implement the CIS controls, along with many of the services and products that our partners out in industry also support and provide.

The controls, the benchmarks, the products, and services are put into execution in our primary mission, and that is running the Multistate Information Sharing and Analysis Center, or the MS–ISAC. The ISAC was established in a partnership with DHS in 2010, and we began the journey of beginning to monitor all 56 SLTTs, where we are approximately more than two-thirds of the way through bringing the States and these local governments and Tribal networks onto our network.

We currently have 41 that we actively monitor that we provide network intrusions, that we provide intelligence analysis to, that we provide forensics capability and response as part of a computer emergency response team. That mission continues to grow and strengthen.

What I would like to talk about now is how that mission feeds our assessment of where we believe the current state of National cybersecurity is within the SLTTs. We inform it through the day-to-day mission and the operation over the last several years, our experience, and global situational awareness and engagement. We

are also responsible for producing the National cybersecurity in this report to DHS, which every 2 years is provided to Congress. We are working to finalize this year's report.

The NCSR is a self-assessment by the States in 13 key categories, and we measure those categories in a number of ways through the self-assessment amongst these entities. We find that in each of the 13 categories, while year to year, there has been improvements among the States, there are still challenges that reside in all 13 categories to meet the self-prescribed benchmarks metrics that they want to achieve.

Progress is being made. I characterize in my written testimony that the current state within the SLTTs is improving, but there are still a number of challenges that are facing the States, to include under-resource budgets, a workforce that I would characterize as high-demand, low-density in its assets and that is insufficient to address on many of the challenges, and a number of other areas of dealing with basic hygiene in terms of executing some of their strategies. But progress is being made, and I would characterize it as improving.

I look forward to the dialogue and the questions and to diving into some of the specific details on how we can improve moving forward in two key areas: One is establishing a basic hygiene campaign, whether that is a built upon the critical security controls or other frameworks; and the other areas I mentioned that I believe is a strategic challenge for us Nationally is how to inspire and generate a cybersecurity workforce that can grow and meet the challenges. Because as I mentioned, they are high-demand, low-density asset across, and the trends we are seeing within K through 12 and interest in STEM, colleges and universities are offering programs but it is insufficient to get to scale. We are seeing that just the basic capabilities to keep up with the growing threats and the expertise and the training of existing professionals is a challenge for a lot of the SLTTs.

Thank you very much for the opportunity to address you. I look forward to your questions.

[The prepared statement of Mr. Spano follows:]

PREPARED STATEMENT OF STEVEN SPANO

MAY 24, 2016

Chairmen Donovan and Ratcliffe, Ranking Members Payne and Richmond, and Members of the committee, thank you for inviting me today to this hearing. My name is Steve Spano, and I serve as the president and chief operating officer of the Center for Internet Security—or "CIS." I appreciate the opportunity today to share our thoughts on the current state of National cybersecurity, focusing in the area we know best: State, local, Tribal, and territorial (SLTT) government entities. As the Nation addresses the complicated issue of cybersecurity, your efforts to assess the current state of National cyber preparedness and response capabilities and determine how best to improve our National cybersecurity posture is noteworthy. I look forward to offering our ideas on how we can collectively build on the progress being made in this important area of critical National security.

Established in 2000 as a not-for-profit organization, CIS's primary mission is to advance cybersecurity readiness and response. CIS was instrumental in establishing the first guidelines for systems hardening at a time when there was little on-line security leadership. In 2010, the U.S. Department of Homeland Security (DHS), under the National Protection and Programs Directorate (NPPD), partnered with CIS to host the Multi-State Information Sharing and Analysis Center, or MS–ISAC. Under a cooperative agreement with DHS, the MS–ISAC was established as a 24x7

cybersecurity operations center that provides real-time network monitoring, threat analysis, and early warning notifications to SLTTs. MS–ISAC also consolidates and shares threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC), where we have 2 employees serving as liaisons for MS–ISAC. In 2015, we became the home of the CIS Critical Security Controls, previously known as the SANS Top 20. With this expanded operational mission, CIS has evolved as a trusted resource to help public and private organizations start secure and stay secure.

Today, CIS collaborates with the global security community to lead Government and private-sector entities to on-line security solutions and resources. While I will elaborate more fully below, the 100-plus professionals at CIS provide cyber expertise in three main program areas:

1. As I just mentioned, the MS–ISAC operates a 24x7 Secure Ops Center to support SLTTs.
2. The CIS Critical Security Controls (CIS Controls), a consensus-driven, prioritized set of cyber best practices created to stop today's most pervasive and dangerous cyber attacks. The CIS Controls are referenced in several policy and security frameworks such as the NIST 800.43; and
3. The Security Benchmarks, a program that provides well-defined configuration best practices to help organizations world-wide assess and improve their cybersecurity. Over 100 consensus-based Security Benchmarks have been developed to date, and Security Benchmarks members can access tools and automated content for both traditional hardware and software as well as cloud-based services.

More information about CIS is included at Attachment A and incorporated herein by reference.

THE CURRENT STATE OF CYBERSECURITY PREPAREDNESS

CIS's assessment of the current state of cybersecurity preparedness and response capabilities is based on our collective daily experience with the MS–ISAC, represented by over 1,000 SLTT members (including all 50 States), as well as our dealings with those using the CIS Security Benchmarks and the CIS Controls, all of which provide us unique and wide-ranging insight into the cybersecurity posture of those we serve.

Today, thanks to Congressional and DHS support and SLTT participation, the MS–ISAC is actively monitoring the networks of 41 States and territories. In 2016, our goal is to have all 50 States and all 6 territories being monitored by the MS–ISAC. Our members represent local governments, public universities, critical infrastructure entities, and public authorities that own and operate critical infrastructures. In 2015, our monitoring program analyzed over 3 trillion records, which generated over 56,000 actionable alerts to our SLTT partners. In 2015, our CERT team managed 161 incidents for our partners, largely focused on computer forensics. Their efforts actively identify types of threats, origins of attack, and root causes of the attack. Our intelligence team has produced a large number of analytical reports that both DHS and the FBI have cited as key resources to help in their investigations and high-level threat detection. Our cyber support for SLTTs also includes a computer emergency response capability, and the issuance of real-time cyber alerts, advisories, and intelligence products.

Based on this work, we can state that since 2004, when the MS–ISAC partnership with DHS began, we have seen progress in the state of cybersecurity of our SLTT partners that can be characterized as improving, with many positive trends. There are, however, significant challenges that we are collectively working to improve. These challenges include under-resourced cybersecurity budgets, poorly crafted and vulnerable software provided by vendors, misconfigured networks, and insufficient numbers of qualified professional staff.

Our assessment of SLTT cybersecurity preparedness and response capability is supported in the findings of the DHS-funded Nation-wide Cyber Security Review (NCSR). This annual review, tasked to the MS–ISAC by DHS, is produced in conjunction with the National Association of Counties and the National Association of State Chief Information Officers, and is reported to Congress by DHS every 2 years. It is a voluntary, self-assessment survey designed to evaluate cybersecurity management within, and the cybersecurity posture of, SLTT governments. To gauge the Nation-wide level of cybersecurity readiness, the NCSR measures maturity of cybersecurity programs within the SLTT community by assessing how SLTTs are performing in 13 key cybersecurity areas. The 2013 and 2014 NCSRs found SLTT respondents continuing to improve towards the highest level of maturity, "risk aware", in all 13 of these measured functions, but they have not yet reached that maturity level in any of the 13 categories. Further support for our assessment is found in

the DHS 2015 National Preparedness Report (the "Preparedness Report"), which acknowledges both that SLTTs place significant emphasis on the importance of cybersecurity, but have been challenged to find sufficient financial resources and staffing to meet growing cybersecurity demands.

The MS–ISAC, the NCSR and the Preparedness Report all recognize that steady progress is being made in many areas of SLTT cybersecurity, in the face of cyber threats that continue to increase in scope, sophistication, and number, but that challenges remain for SLTTs to reach full cybersecurity preparedness. This reality will not change any time soon. The strategy and execution of defensive responses must evolve at a faster pace. This will require continued investment, strong leadership, and collaboration at all levels of government.

Outside of the SLTT space, our experience with our Security Benchmarks customers and those using the CIS Controls also show increased efforts to improve organizations' cybersecurity posture. In the last 3 years, the number of organizations purchasing Security Benchmarks memberships has almost tripled, and the growth in the use of automated machine image versions of the Benchmarks has grown tenfold since they were first released a year ago. This shows us that there is increasing emphasis on ensuring that organizational networks and devices are securely configured.

In October 2015, we released Version 6 of the CIS Controls. In the period of time since the release, the CIS Controls have been downloaded over 32,000 times. This data, coupled with on-going requests for information and assistance in learning more about the Controls, shows us that companies and organizations are seeking guidance in how to start secure and stay secure, and are looking for the roadmap to tell them how to get there.

HOW CIS IS WORKING TO INCREASE CYBERSECURITY PREPAREDNESS

Since its inception, CIS's mission has been focused on increasing cybersecurity preparedness, both for SLTT governments through the MS–ISAC and for the private sector as well with the CIS Controls and Security Benchmarks programs. I appreciate the opportunity to highlight our work in these 3 areas, and why we believe our work is making a difference.

MS–ISAC

The on-going work of the MS–ISAC has and will continue to improve the cybersecurity posture of SLTT governments. Our continuous monitoring of SLTT networks across the country provides us with the ability to see and analyze the scope of potential malicious activity and identify when there are multiple incidents of the same nature and source. As noted above, in 2015 alone, MS–ISAC detected and analyzed malicious activity events that generated over 56,000 incident reports. We provide response assistance if needed, including CERT team assistance. Equally importantly, we provide timely issue alerts to all our SLTT members, which include steps to take to avoid or mitigate the risk of the identified malicious activity event. We also share SLTT event information with Federal agencies and other trusted partners through our liaisons on the NCCIC floor, so our work also informs the cybersecurity posture of the Federal Government and the Nation as a whole.

In addition to our monitoring and response services, we produce a monthly situational awareness report that shares timely cybersecurity information with our over 1,000 members. We distribute weekly reports of cyber threat indicators and support an automated indicator sharing platform (STIX/TAXII). We hold monthly webcasts focusing on particular cybersecurity issues. We also offer group purchasing opportunities for cybersecurity training and products, with substantially discounted pricing for SLTTs, educational and not-for-profit entities. Since starting the purchasing alliance in 2012, we have been able to save SLTT governments almost $30 million in their purchase of essential cybersecurity training and products. Our work with the NCSR is providing SLTTs with a tool to monitor and track their progress, both internally and against other SLTT entities.

More information on MS–ISAC services is included in Attachment B and incorporated herein; further information is available here: *https://msisac.cisecurity.org/*.

CIS Critical Security Controls

CIS is the home of the Critical Security Controls, the set of internationally recognized prioritized actions that form the foundation of basic cyber hygiene, demonstrated to prevent 80–90% of all known pervasive and dangerous cyber attacks. The CIS Controls were initially created, and are regularly updated, by a global network of cyber experts based on actual attack data derived from a variety of public

and private threat sources, so they are informed by both professional expertise and real-world threat information.

The CIS Controls act as a blueprint for network operators to improve cybersecurity by suggesting specific actions to be done in a priority order. In this regard, we strongly believe that the CIS Controls can help all organizations, especially the small- and mid-sized entities, many of which need help in identifying exactly what to do and when.

The CIS Controls are recognized by a number of cybersecurity frameworks and reports as an effective and practical tool for improving an organization's cybersecurity preparedness. The CIS Controls are specifically called out in the NIST Cybersecurity Framework as one of a handful of cybersecurity tools that help organizations implement the Framework. Just recently, the California Attorney General released the California Data Breach Report (2016), which specifically points to the Controls as a tool that if followed, would meet the requirement of "reasonable security" under California law. (The full report can be accessed here: *https://oag.ca.gov/breachreport2016*).

Additionally, the Controls are included in the following foundational frameworks, reports, and documents:

- NIST Framework
- Symantec 2016 Internet Security Threat Report, *https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf*, pages 75–77
- Verizon DBIR 2015, page 55
- Tripwire, "The Executive's Guide to the Top 20 Critical Security Controls," *http://www.tripwire.com/state-of-security/featured/20-csc-list-post/*
- Zurich Insurance/Atlantic Council "Risk Nexus: Overcome by Cyber risks? Economic Benefits and Costs of Alternate Cyber Futures"—page 28
- NGA "National Governors Association Call to Action on Cybersecurity", page 4
- UK CPNI (the British infrastructure protection directorate—entire web page references the Controls)
- Conference of State Bank Supervisors, "Cybersecurity 101: A Resource Guide for Bank Executives, pages 8, 12, 24, *https://www.csbs.org/CyberSecurity/Documents/CSBS%20Cybersecurity%20101%20Resource%20Guide%20-FINAL.pdf*

We make the CIS Controls available for download at no cost to the general public, as well as free companion guides that provide more detailed information and support for the implementation of the CIS Controls. Find out more information about the Controls and download them for free at: *https://www.cisecurity.org/critical-controls.cfm*. Additional information about the CIS Controls is also included at Attachment C and incorporated herein by reference.

CIS Security Benchmarks

CIS is also the world's largest producer of authoritative, community-supported, and automatable security configuration benchmarks and guidance. The CIS Security Benchmarks (also known as "configuration guides" or "security checklists") provide highly technical, detailed security recommendations for specific components of information technology, such as operating systems and devices, and are vital for any credible security program. The Security Benchmarks are developed though a collaborative effort of public and private-sector security experts. CIS has developed over 100 consensus-based Security Benchmarks have been developed today and are available in PDF format free to the general public, or in an automated format through the purchase of a membership. We have also created a number of Amazon Machine Images® (AMIs) for the most utilized Security Benchmarks, which are available for purchase in the AWS Marketplace® and in Amazon GovCloud®, and we are discussing similar arrangements with other cloud providers. CIS Security Benchmarks are used world-wide by organizations ranging from small, nonprofit businesses to Fortune 500 companies.

The CIS Security Benchmarks are referenced in a number of recognized security standards and control frameworks, including:

- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)?
- NIST Guide for Security-Focused Configuration Management of Information System;
- Federal Risk and Authorization Management Program (FedRAMP) System Security Plan;
- DHS Continuous Diagnostic Mitigation Program; and
- CIS Critical Security Controls, Version 6©

More information about CIS Security Benchmarks is included at Attachment D and incorporated herein by reference.

WHAT MORE CAN BE DONE?

The current cyber threat is clear, unmistakable, and unlikely to abate anytime soon. Fortunately, much is currently being done to improve cybersecurity—but more needs to be done. We would like to focus our comments on 2 areas that we believe are of significant importance to both SLTT and non-SLTT organizations: (1) Improving cyber hygiene; and (2) creating a comprehensive approach to both increasing and improving the cybersecurity workforce.

Improving Cyber Hygiene

Probably the single most important effort that we can undertake to dramatically make our networks more secure is to adopt basic cyber hygiene. Like personal hygiene, it involves basic, regular routines and actions that are needed to maintain basic safety and security.

Despite a growing understanding of the threats and vulnerabilities in the technical community, wide-spread adoption of safe cyber behavior in cyber space is the exception, not the norm. It is our experience that the vast majority of cyber incidents result from either the failure to patch known vulnerabilities in software and web applications or failure to adopt proper security configurations on network operating systems or devices.

We believe that part of the difficulty in getting more traction for cyber hygiene is the existence of a plethora of defensive tools, security frameworks, and guidelines, combined with the complexity of our networks, which have simply overwhelmed and confused consumers, private-sector companies and governments. For example, while the NIST Framework lays out a process for beginning a dialogue on cybersecurity measures, it is by design not a framework listing prioritized actions based on effectiveness.

As we have discussed above, we believe that the CIS Controls provide the specific, actionable controls in priority order that will thwart the most pervasive attacks. This is supported in a study by the Australian government Department of Defense, which revealed that 85% of known cybersecurity vulnerabilities can be mitigated by deploying the Top 5 CIS Controls. Whether by using the CIS Controls or some other framework, increased efforts by the Federal Government to promote a roadmap for basic cyber hygiene will yield proven results in mitigating the most prevalent and pervasive cyber attacks.

Creating a Comprehensive Approach to Improving Our Cybersecurity Workforce

One of the major reasons that organizations have struggled in achieving basic cyber hygiene is the lack of available and qualified cybersecurity professionals to undertake the necessary cyber protection actions, particularly on an on-going basis. There are simply too few qualified cyber professionals in the workforce. This is the result of several factors:

- too few students in the K–12 level of education are interested in pursuing further education in computer science and cybersecurity;
- too few universities and colleges are offering cybersecurity degree or certificate programs that offer the practical training needed to meet the qualifications of cybersecurity professional roles;
- there is a need for more continuing cyber education of staff in the current cybersecurity workforce to keep up with the ever-changing technical landscape of cyber threats; and
- for SLTTs and smaller organizations, the ability to hire from the limited existing cybersecurity workforce is hampered by the inability to compete with private-sector salary levels.

We believe that there are several areas in which the Federal Government can assist with increasing and improving the cybersecurity workforce:

1. Help to increase awareness and promote STEM education at the K–12 level;
2. Because of our DHS support, CIS is able to recruit students from the National Science Foundation's Scholarship for Services Program (SFS) for certain MS–ISAC positions. This program has been a great tool in helping us recruit and maintain entry-level cyber professionals. We would recommend considering additional funding for the SFS program to open the program up to more students. This would assist in growing the number of students entering cybersecurity studies at the college level. We would also suggest considering broadening the organizations that qualify to hire SFS students to include non-governmental critical infrastructure organizations and not-for-profits, all of whom share the same challenges that Federal and SLTT governments face in recruiting and retaining cyber talent.
3. Providing more opportunities for cyber exercises and simulations and expand participation by SLTT entities. In addition to allowing SLTTs more opportuni-

ties to assess their cyber readiness and response capabilities, these exercises and simulations provide on-going training for the SLTT cybersecurity workforce.

The threat to our Nation is real and extends down to every individual. As such, improving our cybersecurity defense of this country demands the combined efforts of us all. We will continue our efforts at CIS to help SLTTs protect citizen data at every level of Government. We will also continue our excellent partnership with the Federal Government as we work to extend monitoring services to all 56 States and territories as the foundation of best practice in cybersecurity information sharing.

I want to thank the committee for the opportunity to participate in this important hearing, and look forward to addressing any questions you might have.

Find out more information about CIS here: *https://www.cisecurity.org/*.

Attachment A.—The Center for Internet Security
Attachment B.—MS–ISAC
Attachment C.—CIS Critical Security Controls
Attachment D.—CIS Security Benchmarks

Mr. DONOVAN. Thank you, General Spano.

The Chair now recognizes Mr. Raymond for 5 minutes.

STATEMENT OF MARK RAYMOND, VICE PRESIDENT, NATIONAL ASSOCIATION OF STATE CHIEF INFORMATION OFFICERS

Mr. RAYMOND. Thank you, Chairman Donovan, Chairman Ratcliffe, and Ranking Members Payne and Richmond for inviting me to testify for you today.

My name is Mark Raymond, and I serve as the chief information officer for the State of Connecticut and the vice president of the National Association of State Chief Information Officers. NASCIO is a nonprofit association that represents State CIOs and IT executives and managers from States, territories, and the District of Columbia.

Today, I would like to provide the committee with an overview of cybersecurity preparedness in the States, what States are doing to improve our resilience, and opportunities to enhance the security profile of our Nation.

State CIOs are Executive branch officials who serve as business leaders, advisers of IT policy, and implementation at the State level. The most critical role for the CIO today includes the security of State networks, protection of State data, and helping formulate the response for cyber incident or disruption. These responsibilities are shared with the chief information security officer, or CISO, a position that exists among all 50 States and for whom are becoming increasingly standardized in their roles.

State CIOs and CISOs operate in an increasingly challenging environment. In the 2014 Deloitte-NASCIO Cybersecurity Study, we found that the top barriers for States addressing cybersecurity were insufficient budgets, increased sophistication of threats, and the inadequate availability of security professionals.

Regarding insufficient funding, the majority of the States spend in the range of 1 to 2 percent of their overall IT budget on cybersecurity. The Federal Government spends around 14 to 16 percent. Combined with recent events, this disparity shows that there is no one correct amount or percentage. States must assess their cybersecurity risk and spend commensurate with that risk.

The lack of qualified IT security professionals are also a challenge for States. People with IT security skills are the most difficult to recruit and retain for States, and the State government

salary rates and pay structures are the biggest challenge in bringing on IT talent.

Another obstacle for CIO and CISOs is the increasing sophistication of threats. The top 3 are malicious code, hacktivism, and zero-day attacks. State CIOs are playing defense, but we have been able to better prepare for known threats through information sharing.

Despite these challenges, States are progressing towards a more secure cyber environment. NASCIO has long called for States to adopt a cybersecurity framework, and quickly endorsed the NIST framework upon its release. From 2015 data, we know that 80 percent of the States have adopted a cybersecurity framework based on National standards and guidelines.

States are utilizing public and private resources to enhance their cybersecurity posture in both times of relative rest and in times of emergency. To better identify and detect cyber threats, States are increasingly sharing threat information through fusion centers and MS–ISAC. Eighty percent of States have established trusted partnerships for information sharing and response. Eighty percent of the States have also acquired and implemented continuous vulnerability monitoring capabilities to better identify and detect malicious cyber activity.

Many States also participate in ALBERT, a joint program between MS–ISAC and DHS, which brings an EINSTEIN-based, cyber-traffic monitoring system to the States. Knowing that the ability to identify and detect is our first line of defense, Connecticut is the first State to take advantage of DHS's threat intelligence offering provided by iSight partners.

In the realm of response and recoveries, States are also showing maturity. In a disaster, State officials expect the State CIO to maintain reliable and secure infrastructure, coordinate with other State officials, and restore communications services. I am responsible for these duties in my State as outlined in our disaster response framework.

Recognizing that States could face a catastrophic disaster that coincides with or is caused by a cyber event, NASCIO has called on States to develop a cyber disruption plan that contemplates massive disruptions to the business of State government. States like Michigan have taken the whole-community approach and have developed disruption plans that outline roles and responsibilities during a disaster.

A key partner to the States has been DHS. States are heavy utilizers of DHS State and local cyber programs like ICS–CERT and FedVTE. Also Federal programs like CyberCorps helps shore the IT security workforce gap that all States are facing.

Another way the Federal Government could aid in enhancing State's ability to identify, protect, detect, respond, and recover is by harmonizing Federal security requirements. CIOs must comply with IRS publication 1075, FBI–CJIS, HIPAA, FERPA, CMS's MARS–E, amongst others. Regulation harmonization could lessen the burden on States, enabling us to focus on providing security services rather than checking off boxes.

Thank you for holding this important hearing and for the opportunity to testify today on this truly critical issue.

[The prepared statement of Mr. Raymond follows:]

PREPARED STATEMENT OF MARK RAYMOND

MAY 24, 2016

Thank you Chairmen Ratcliffe and Donovan and Ranking Members Payne and Richmond for inviting me to testify before you today.

My name is Mark Raymond and I serve as the chief information officer (CIO) for the State of Connecticut and also as the vice president of the National Association of State Chief Information Officers (NASCIO). At NASCIO, I also co-chair the cybersecurity committee. NASCIO is a nonprofit, 501(c)(3) association representing State chief information officers and information technology executives and managers from the States, territories, and the District of Columbia.

Today, I would like to provide the committee an overview of the status of cybersecurity preparedness in the States, what States are doing to improve and enhance resilience to cyber attacks, and opportunities to enhance the security profile of our Nation.

State chief information officers are State 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 within the executive branch of State government. The office of the State CIO takes many forms, some are cabinet officials and others are executive directors; regardless of the title, all State CIOs share a common function of setting and implementing a State's IT policy.

State CIOs are also responsible for providing IT services to State executive branch agencies. This not only includes the more typical business of provisioning enterprise data or phone services but also securing the digital business of State government. The most critical role today for the CIO includes the security of State networks, protection of State data, and helping formulate the response for a cyber incident or disruption. These responsibilities are shared with the chief information security officer (CISO), a position that exists among all 50 States and duties for whom are becoming increasingly standardized.

State CIOs and CISOs operate in an increasingly challenging environment.—In the *2014 Deloitte-NASCIO Cybersecurity Study, State governments at risk: Time to move forward*, (2014 Deloitte-NASCIO Study) [*http://www.nascio.org/Portals/0/Publications/Documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf*], we studied the current cybersecurity environment in the States, common challenges, and barriers to a strong State cybersecurity posture. The 2014 Deloitte-NASCIO Study showed that the top barriers to States addressing cybersecurity were insufficient budgets, increased sophistication of threats, and the inadequate availability of security professionals. These challenges remained the same in 2015.

Insufficient budgets for cybersecurity have been cited as a top barrier since the inception of the Deloitte-NASCIO Cybersecurity Study in 2010. The majority of States spend in the range of 1–2 percent of their overall IT budget on cybersecurity. The Federal Government spends around 14–16 percent of their IT budget on cybersecurity. Combined with recent events, this disparity shows that there is no one correct amount or percentage; States must assess their cybersecurity risk and spend commensurate with that risk.

Funding challenges also affect the ability of States to hire and retain skilled IT security personnel. NASCIO's *State IT Workforce: Facing Reality with Innovation [http://www.nascio.org/Portals/0/Publications/Documents/NASCIO_StateIT-WorkforceSurvey2015_WEB.pdf*] survey shows that a shortage in the State IT workforce has been predicted for some time and States are finding that those with IT security skills are the most difficult to recruit and retain (67.3%) followed by application development, programming, and support (57.1%); and architecture (55.1%). Ninetey-two percent of respondents reported that salary rates and pay structures are a challenge in bringing on top IT talent. States are responding to the dearth of qualified IT security personnel by getting innovative.

In Maine, State CIO Jim Smith confronted the reality that 24 percent of his 480 State IT workers would be eligible to retire in the next 2 years thus highlighting the need to recruit and retain new IT talent. He has addressed 1 aspect of the workforce issue by updating the application process, moving it on-line, and making it mobile friendly. He has also created an IT intern program and over 70 percent of those interns have become full-time employees. High school students are also welcome to visit Maine's Office of Information Technology for its annual "Technight," [*http://www.maine.gov/oit/technight/index.shtml*] where students participate in a variety of tech-related activities, which introduces them to exciting IT careers.

While insufficient budgets and workforce shortages continue to be obstacles for State CISOs, 3 out of 5 also reported that the increasing sophistication of threats

was also a major barrier to addressing cybersecurity. In the *2014 Deloitte-NASCIO Study*, CISOs reported their top 3 cyber concerns: Malicious code (74.5%), hacktivism (53.2 %), and zero-day attacks (42.6%). Malicious cyber activity happens daily in State government, but State CIOs have been able to better prepare for known threats through information sharing, a concept with which emergency managers are acutely aware.

Despite these challenges, States are progressing toward a more secure cyber environment. NASCIO has long called for States to adopt a cybersecurity framework and quickly endorsed [*http://nascio.org/Newsroom/ArtMID/484/ArticleID/34/NASCIO-Supports-Adoption-of-the-NIST-Cybersecurity-Framework*] the National Institute of Science and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Cybersecurity Framework) upon its release in February, 2014. In the 2014 Deloitte-NASCIO Study, we found that 88 percent of States were reviewing or planning to leverage the *NIST Cybersecurity Framework* within the year. In the NASCIO, Grant Thornton, CompTIA *2015 State CIO Survey, The Value Equation: Agility in Sourcing, Software and Services*, [*http://www.nascio.org/Portals/0/Publications/Documents/2015/NASCIO_2015_State_CIO_Survey.pdf*] we found that 80 percent of States had adopted a cybersecurity framework based on National standards and guidelines.

States are adapting to shared cybersecurity challenges and utilizing public and private resources to enhance their cybersecurity posture both in times of relative rest and in times of emergency. The NIST *Cybersecurity Framework* identifies 5 basic functions: Identify, protect, detect, respond, and recover. States are making progress in each of these areas.

To better identify and detect cyber threats to protect a wealth of State digital assets, States are increasingly sharing threat information through established forums like fusion centers and the Multi-State Information Sharing and Analysis Center (MS–ISAC). From the *2015 State CIO Survey*, we know that 80 percent of States have established trusted partnerships for information sharing and response. Additionally, 80 percent of States have also acquired and implemented continuous vulnerability monitoring capabilities in order to better identify and detect malicious cyber activity. Knowing that the ability to identify and detect are our first line of defense, NASCIO has called on States to invest in advanced cyber analytics as a part of the practice of business intelligence and recently published, *Advanced Cyber Analytics: Risk Intelligence for State Government*. [*http://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_AdvancedCyberAnalytics_FINAL_4.18.16.pdf*] To that end, Connecticut is the first State to take advantage of DHS's threat intelligence offering provided via iSight Partners. Many States also participate in ALBERT, a joint program between MS–ISAC and DHS which brings an EINSTEIN-based, cyber-traffic monitoring system to the States.

In my State, in addition to participating in the information sharing through MS–ISAC and utilizing ALBERT, Emergency Management Deputy Commissioner and State Homeland Security Advisor, William Shea, and I co-chair a cybersecurity task force whose membership includes a diverse mix of stakeholders including higher education, law enforcement, public utilities, private businesses, and others. We meet regularly to discuss the latest threat and vulnerability information because we know that information sharing is key to cultivating a culture of information security and is a best practice to which States should conform.

In the realm of response and recovery, States are also showing maturity.—State CIOs are expected to play a role in helping State governments respond to and recover from natural and man-made disasters. According to the *2015 State CIO Survey*, the top 3 functions for which State CIOs were responsible are maintaining a robust, reliable, and secure infrastructure; coordinating with other State officials; and restoring communications services.

When riots broke out in and Baltimore, Maryland, Governor Larry Hogan declared a state of emergency. Maryland's CIO organization, led by Secretary of Information Technology David Garcia, assisted with the swift deployment of "Maryland First Responders Interoperable Radio System Team (FIRST)," the State-wide radio communications equipment for first responders and stood up a website, "Maryland Unites" to which State and local leaders could direct members of the affected community. They also worked with public and private partners to reverse engineer Anonymous' attack on State networks. Information sharing was also helpful; officials in Missouri shared their experience with Maryland as they had faced a similar crisis. In ways like these, State CIOs are showing maturity in response in both the cybersecurity and emergency management fronts and especially when those two worlds collide.

Recognizing that States could face a catastrophic emergency event that coincides with or is caused by a cybersecurity event, NASCIO has called on States to develop

a cyber disruption plan and recently released the "*Cyber Disruption Response Planning Guide*." [*http://www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_040616.pdf*] A cybersecurity disruption is defined as: "an event or effects from events that are likely to cause, or are causing, harm to critical functions and series across the public and private sectors by impairing the confidentiality, integrity, or availability, of electronic information, information systems, services, or networks that provide direct information technology services or enabling and support capabilities for other services; and/or threaten public safety, undermine public confidence, have a negative effect on the state economy, or diminish the security posture of the state." A cybersecurity disruption differs from a cybersecurity incident which is limited in scope and impact.

Examples of a cybersecurity disruption include: A cyber attack on the power grid which leads to a loss of power for a significant population; a cyber attack on water treatment and delivery leading to a loss of water supply to a significant population; a cyber attack on network capabilities leading to loss of communications which then hampers, interrupts, or prevents the operation of government and requires implementation of a continuity of operations plan; or a hurricane, flood, or other natural disaster that impairs or destroys key infrastructure assets that then precipitates the loss of connectivity over the internet or internal network.

With these scenarios in mind, States like Michigan, taking the "whole community" approach, convened State and local government representatives and private-sector critical infrastructure owners and operators to develop the Michigan Cyber Disruption Response Strategy, initially completed in 2013. Michigan's Cyber Disruption Response Strategy [*https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf*] provides a common framework to encourage a State-wide effort among public and private partners to defend Michigan's critical networks. Specifically the plan prompts critical infrastructure owners and operators to address: Data backup, disaster recovery/business continuity, halt key processes, equipment shutdown, log file, communications, and how to activate the cyber disruption response plan.

States like the Commonwealth of Massachusetts, New Hampshire, and Rhode Island have taken a regional approach to cyber disruption planning, an effort supported by FEMA's Regional Catastrophic Preparedness Grant Program and Urban Areas Security Initiative (UASI) funding. In 2012, as part of the New England Regional Catastrophic Preparedness Imitative (NERCPI), these 3 States along with the city of Boston and Providence completed regional cyber disruption planning and created a Cyber Disruption Response Annex which outlines how cyber responders will support industrial control system (ICS) structure in each jurisdiction, how critical cyber incident information will be shared, and how IT organizations can support public safety and each other. NERCPI also created cyber disruption teams in each State and the city of Boston; these teams are comprised of experts from IT, emergency management and public safety and are responsible for coordinating resources and information during catastrophic events.

As these previous examples exhibit, *protection from cybersecurity attacks requires a "team" or "whole community" approach and a key partner to the States has been the U.S. Department of Homeland Security (DHS)*. States are heavy utilizers of DHS's cybersecurity-focused State and local programs including: ICS–CERT, FedVTE (virtual training environment), and cybersecurity advisors (CSA). Also, Federal programs like "CyberCorps: Scholarship for Service" allow qualifying students to serve in an IT assurance role with a Federal, State, or local government after graduation; this helps shore the IT security workforce gap that all States are facing.

The Federal Government, principally through DHS, has and hopefully will continue to provide support for successful cybersecurity programs. There is, however, another way the Federal Government could aid in enhancing States' ability to identify, protect, detect, respond, and recover—by harmonizing Federal security requirements.

When States receive Federal funds, they are required to certify that certain security measures are in place; this is mandated by the Federal Information Security Management Act (FISMA). CIOs and CISOs must also comply with a variety of Federal regulations, typically promulgated in a silo-ed fashion. Some of the Federal regulations with which our community must comply include: IRS Publication 1075, FBI-Criminal Justice Information Services (FBI–CJIS), the Health Insurance Portability and Accountability Act (HIPAA), social security administration security standards, Family Educational Rights and Privacy Act (FERPA), Office of Child Support Enforcement (OCSE) security requirements, the Center for Medicare and Medicaid Services' Minimum Acceptable Risk Standards for Exchanges (MARS–E), among others.

The overarching goal of these regulations is data/information security. Knowing that the vast majority of States are utilizing National standards like those issued by NIST, the Federal Government could lessen the regulatory burden on States by harmonizing Federal requirements especially since most if not all of these regulations share a common security goal.

Cybersecurity is an issue that will only become more complex as we enter an age where the Internet of Things will become more prominent and technology like unmanned aerial systems (UAS), body-worn cameras, and cloud adoption are a norm. New technologies will require State governments to constantly assess security vulnerabilities as citizens demand consumer-level technology services to be deployed on a whole-of-Government or enterprise basis. Given this background, the Congress and Federal agencies should continue to partner with State CIOs and CISOs when reviewing or promulgating new data security laws or regulations to ensure that the goal of security is achieved without undue burden or redundancy.

Thank you for opportunity to testify today on this critical issue.

Mr. DONOVAN. Thank you, Mr. Raymond.

The Chair now recognizes Mr. Galvin for 5 minutes.

STATEMENT OF ROBERT GALVIN, CHIEF TECHNOLOGY OFFICER, PORT AUTHORITY OF NEW YORK AND NEW JERSEY

Mr. GALVIN. Good morning, Chairman Ratcliffe, Chairman Donovan, Ranking Member Payne, and Members of the subcommittees. Thank you for this opportunity to discuss strategies for strengthening our Nation's cybersecurity.

Since December 2013, it has been my privilege to serve the Port Authority of New York and New Jersey as its chief technology officer. The Port Authority builds, operates, and maintains infrastructure critical to New York and New Jersey transportation and regional trade. These facilities include America's busiest airport system, including JFK, LaGuardia, and Newark Liberty International Airports, the World Trade Center, the PATH rail transit system, 6 tunnels and bridges between New York and New Jersey, the Port Authority Bus Terminal, Hudson River ferries, and marine terminals.

For more than 90 years, the Port Authority has worked to improve the quality of life for more than 18 million people who live, work, and visit New York and New Jersey metropolitan region.

Safety is the No. 1 priority across all of the authority's locations. Technology touches virtually all of our operations so the secure and reliable functioning of our computing assets is vital to public safety.

In our limited time, I would like to briefly discuss 3 areas in which I believe the Federal Government can assist technology professionals in addressing cyber threats. These areas are communication, readiness, and public education. In the realm of communication, events like today's public hearing play a valuable role. Government and technology leaders need to work together to create safe forums to discuss prevention strategies and deconstruct cybersecurity incidents. Through the avenues of improved communication, best practices can be shared across many organizations to the benefit of the whole.

Turning now to readiness. When I joined the Port Authority, the organization was in the planning stages of designing a comprehensive cybersecurity program. We adopted a framework, the NIST 800–53, which was developed by a joint task force of people from the National Institute of Standards and Technology, DOD, Department of Homeland Security, intelligence community, and Com-

mittee on National Security Systems. This was an invaluable tool saving us time and money as we put our cybersecurity program in place.

I believe the Federal Government has a similar opportunity to assist organizations by coordinating regular drills, simulating large-scale cybersecurity events. Facilitating these exercises would allow those involved to understand whether they have the right procedures in place to respond effectively and to identify any deficiencies. At the Port Authority, our Office of Emergency Management conducts regular readiness drills simulating such things as active-shooter scenarios and aircraft emergencies. From these exercises, teams learn how to improve their response. Cybersecurity professionals can benefit from the same rigorous testing of our readiness.

Like many organizations, the Port Authority invests resources to detect, prioritize, and examine suspicious activity on our computer networks. We also use strong, complex passwords across all mission-critical systems, restrict administrator access to only essential personnel, and staff a 24×7 operations center to respond to alarms generated by our cybersecurity tools and alerts received from other agencies.

But probably the single most important thing we do to improve our cybersecurity posture is to require all staff who access Port Authority computers to participate in mandatory cybersecurity training programs. Themes such as "Think Before You Click on Email Links" and "Be Aware Before You Share on Social Media" encourage people to contact our help desks and the operations center before they open questionable links and attachments.

Education is essential. I believe the Federal Government can play a significant role in strengthening America's cybersecurity by sponsoring a National public education campaign to promote safe computing practices. In my experience, people are more likely to exercise good cyber hygiene if they understand the important role their individual actions play in keeping our computer network secure.

In the physical world, we rely on the American public to see something and say something. We need to develop Nation-wide awareness and training programs to empower people to do the same in the realm of cybersecurity. I thank the committee and look forward to your questions.

[The prepared statement of Mr. Galvin follows:]

PREPARED STATEMENT OF ROBERT GALVIN

MAY 24, 2016

ABOUT THE PA

The Port Authority of New York & New Jersey conceives, builds, operates, and maintains infrastructure critical to the New York/New Jersey region's trade and transportation network. These facilities include America's busiest airport system, including: John F. Kennedy International, LaGuardia, and Newark Liberty International airports, marine terminals and ports, the PATH rail transit system, 6 tunnels and bridges between New York and New Jersey, the Port Authority Bus Terminal in Manhattan, and the World Trade Center. For more than 90 years, the Port Authority has worked to improve the quality of life for the more than 18 million people who live and work in New York and New Jersey metropolitan region.

I. It is important to keep the Authority up and running

The Authority operates a diverse groups of facilities that can have both logistic and economic impacts that can reach across the globe if the facilities were to be shut down by a cyber attack. These facilities have implemented many different internet-based technologies to add efficiencies to how they operate. However, it is these technologies that make these facilities more vulnerable to cyber attacks.

II. The Authority relies of its supply chain to operate

The Authority relies on its supply chain in 2 States (New York and New Jersey) in order to operate its facilities. Required resources are provided by multiple suppliers. If fuel cannot be provided, or if electricity is impacted in either State, the Authority cannot operate at full capacity. It is critical that these supply chains are resilient to cyber attacks and have resilient business continuity plans.

III. The Port Authority takes cybersecurity seriously and has an evolving program

The Port Authority takes cybersecurity very seriously. In 2012, the Authority conducted an audit of its cybersecurity posture, and as a result, immediately started to build a cybersecurity program. Working with a consultant to identify the requirements of our cybersecurity program, the authority decided to use the NIST SP 800–53 guidelines as a standard for organizing teams, and developing and implementing the program. Leveraging this existing standard created by a joint task force of NIST (National Institute of Standards and Technology), the Department of Defense, Department of Homeland Security, the intelligence community and the Committee on National Security systems saved The Port Authority time and effort we otherwise would have had to develop a framework implementing cybersecurity.

The first step the Authority took to advance the cybersecurity program was to implement services from MS–ISAC (Multi-State Information Sharing and Analysis Center). MS–ISAC analyzes all the logs generated by our perimeter security tools and provides the authority visibility into potential indicators of compromise.

The Authority built and staffs a 24x7 Cybersecurity Operations Center (CSOC) that responds to all of the alarms generated by our cybersecurity tools, and to alerts received from the agency partners and cybersecurity services.

We created and manage a mandatory cybersecurity awareness and training program for all staff who access the authority's computing resources.

Through this process, Port Authority developed and maintains strong partnerships with DHS, FBI, NYPD, NJSP, MS–ISAC (multi-State information sharing and analysis centers), US–CERT, and ICS–CERT. We continue to engage these agencies to perform vulnerability assessments and to assist with incident response. We also strengthened internal partnerships within the Port Authority between the Chief Security Office, Office of Emergency Management, Office of Inspector General and the Technology departments. Early on we recognized that no one team or group would have the total solution.

From these efforts, the Port Authority has seen positive results, but much work remains to protect critical assets. The technology we put in place provides visibility into emerging threats and have shown results, such as the ability to detect and automatically block 90% of critical incidents. We continue to make improvements in our cybersecurity operations. Last year, we reduced our critical incident response time by one-third over the previous year.

However, just as the technology sector continuously innovates, criminal organizations, nation-states, and hacktivists are also innovating their methods for exploiting vulnerabilities presented by new technologies, "apps", and new attack surfaces like the Internet of Things.

IV. The Port Authority's Biggest Cybersecurity Concerns

- Like many organizations, The Port Authority uses a large number of ICS (Industrial Control Systems) to operate its facilities, for example: tunnel ventilation systems, PATH Train Control Systems and Airport Airfield Lighting Systems. Some of these systems, if compromised, could cause loss of life. This year, the Authority initiated a program to better understand our vulnerabilities and properly patch and mitigate these systems. But, it is an enormous task.
- In order to properly respond to a massive cyber attack or the breach of a partner organization, the PA must be in communication with partner organizations in real time and have specific remediation actions or practices to follow. Today's ISACs while useful, do not provide such real-time breach notification. According to Verizon's 2015 Data Breach Investigations Report, 75% of attacks spread from the first victim to the second victim within 24 hours, and 40% spread from the first victim to the second in 1 hour.

- In order to operate all these diverse facilities and business functions, the Agency hires thousands of contractors. These individuals have access to some of our most critical systems. The Authority has recognized that insider threat is potential attack vector.
- The Authority invests in resources and money to implement cybersecurity tools. We have learned from telecommunications carriers and cybersecurity service providers that it is possible for aggressive nation-states to obtain these tools through third parties and to reverse engineer them to determine how these detection and prevention tools may be circumvented.

V. How can the Federal Government help?

- *Education*.—I think there is a clear role for the Federal Government to play by launching a massive public education campaign to practice "Safe Computing". The weakest link in our cybersecurity chain is the end-user. Phishing scams, e-mails with links to malevolent sites are often the first step toward a breach. Two-thirds of cybersecurity incidents that fit a pattern of cyber-espionage feature phishing scams. (DBIR, 2015). Raising our internal education & awareness level was a crucial step in improving the security posture at the Port Authority. I think PSAs (public service announcements) to inform the public about how technology works, responsible measures such as good passwords, "Think before your click" and other safe computing practices should be taught to the American public, beginning in school.
- *Communication*.—Events such as today's, not built around an incident or a breach, but a conversation between technology and policy makers to reach understanding go a long way to help both technologists and our Government make better decisions. Government and technology leaders need to work together to create safe forums to discuss prevention strategies and de-construct cybersecurity incidents. The Federal Government can conduct in-depth reviews following an organizational breach, similar to the investigations conducted following plane crashes or what hospitals do after a medical mistake. These non-punitive approaches have been very successful improving airline safety and in reducing medical mistakes in the hospitals and emergency rooms—I would think it could have a significant impact improving cybersecurity. The name of the breached organization could be withheld, and the Federal Government can inform agencies of findings and recommendations after completing the review. Case studies provide more than technical remediation requirements; they inform industry how to prevent problems over the long term.
- *Simulations*.—The Federal Government can assist the PA and related agencies by coordinating an exercise or drill simulating a large-scale cybersecurity event. This drill would allow the agencies to understand where our deficiencies lie, and whether we have the right procedures and external relationships in place to respond correctly. For example, the operations of the Port Authority rely on several Federal Agencies: The CBP (Customs & Border Protection), TSA, FAA. If their systems were compromised, the impact on the Port Authority would be substantial. if the TSA cannot perform pre-screening, we cannot board passengers, if the CBP cannot review manifests, we cannot transport cargo, if the FAA air traffic controllers are impacted, our regional airports can be shut down. The operational stability of these Federal entities has a direct impact on the Port Authority's ability to provide services to the region. Post-drill, the Fed can assist the agencies to ensure that their comprehensive cybersecurity programs and resilient business continuity plans are complete and coordinate with related agencies.
- Consider oversight of cybersecurity tool developers to ensure their intellectual property is not compromised. The Authority, like many public and private-sector organizations, invests resources and money into their cybersecurity tools. If aggressive nation-states obtained these same tools through third parties and reverse-engineered them to determine how they can be circumvented, the protection we seek from cybersecurity tools would be lost. The tech industry and Federal Government must work together to protect the intellectual capital that represents the vanguard of our security apparatus for it to operate effectively. The Federal Government may be able to provide oversight of the developers of cybersecurity tools to ensure that they are not sold to malicious third parties.
- Consider stopping the Federal Government's participation in "bug bounty" programs which encourage grey hat hackers to sell zero-day vulnerabilities to the highest bidder. The amount governments are willing to pay for some vulnerabilities inflates their value and creates a potentially lucrative secondary market for trading vulnerabilities and may even encourage programmers to 'build in' vulnerabilities they can later sell.

VI. Challenges related to planning for, and responding to, cybersecurity

The first challenge of planning for cybersecurity is the wide variety of threat scenarios an organization must plan for: Viruses, ransomware, hacktivists, nation-states, simple human error, Point-of-Sale intrusion, payment card skimmers, web app attacks, denial-of-service attacks, and cyber espionage.

The second challenge is the size, configuration, and expanding nature of the attack surface: Internet presence (websites), internal network, desktops and servers, cloud-based software systems & file storage, public WiFi infrastructure, portable storage devices, VOIP systems, and the looming Internet of Things. This list includes the traditional boundary of the organization. However, we are seeing a common entry point into an organization being the subcontractors and consultants who bring equipment onsite or connect their organization's networks to provide services. The computing networks and infrastructure of suppliers who provide critical support services to an organization should be considered part of any organization's 'attack surface' that could be exploited by a malevolent entity.

Another challenge is the speed with which threats evolve and time required to detect a breach before damage can be done. This is often referred to the "volume, velocity, and variation" of malware. At a high level, there are approximately 5 malware events globally every second (170 million in 2015). Most of this is filtered out by an organization's firewalls and other cybersecurity technology, but half of all organizations discover malware during 35 or fewer days per year. This seems to align with 'releases' of malware during specific periods, rather than all year long. As for variation, 70–90% of malware samples in 2015 were unique to the organizations in which they were found. This combination shows that adversaries are getting more sophisticated to overcome defenses and more targeted in their approaches.

Mr. DONOVAN. Thank you, Mr. Galvin.

I now recognize myself for 5 minutes for questions. Since each of us only has 5 minutes, I would like to give each of you an opportunity to answer. I think I would like to just ask the entire panel just one question and ask each of you to spend a minute on a response.

States have constantly ranked their cyber capabilities the lowest among their core capabilities, and it makes sense that States would look towards the Federal Government for assistance. Each of you, in 1 minute, can you tell me—and some of you hit on it—declassification of information, training as we do it, active-shooter demonstrations we should do with cyber attacks. Could each of you just tell me what you think the No. 1 priority of the Federal Government should be for each of the States to help them in securing their cyber terrorist capabilities?

Mr. GHILARDUCCI. Mark Ghilarducci. Really, 2 areas: No. 1, information sharing is really critical here so that we are all on the same page with regards to the threat streams; and dedicated funding to implement that collective footprint or blueprint as we move forward working together to minimize the threat. There is no dedicated funding for cybersecurity. It needs to be raised on the priority scale.

Mr. DONOVAN. Lieutenant Colonel.

Mr. COONEY. In the post-9/11 environment, there was a tremendous amount of effort and time put together to create a structure and a network for counterterrorism, and that is, you know, the National network of fusion centers. I compare the cyber environment now to that environment then where, you know, we should leverage this structure that took so long to build, you know, to share this threat, this cyber threat information. I think, as I mentioned in my testimony, I think that is something that is there, we just need to take it a little further, and I think—if I had to name one thing, that would be my one topic.

Mr. DONOVAN. Thank you, sir.

General.

Mr. SPANO. Yeah, I would probably say the workforce is probably the biggest challenge and where the Federal Government can help. In that area, the States are really struggling, both to compete with industry, and so when they do hire cyber professionals, because, again, they are in such demand, it is hard to compete with industry who also is requiring and demanding and hiring of those cyber professionals.

So looking at the catalyst of how to start in K through 12 to get more interest in STEM, to look at the scholarship for service and how perhaps we can broaden that into other areas of not-for-profits and other businesses that surround critical security controls and critical infrastructures would be a clear role for the Federal Government to sort-of serve as a catalyst.

I would say very closely to that would be tighten in the command and control in the apparatuses that link the State governments through the fusion centers, through the ISAC, to continue to strengthen the situational awareness that we present from the ISAC to DHS, which informs many National and international threats and actions and fusing that together and presenting it for National action. So they would be my 2 areas.

Mr. DONOVAN. General, I suspect that one of your frustrations is that all of you train people who then eventually go onto industry.

Mr. SPANO. Yeah.

Mr. DONOVAN. Yes. Mr. Raymond.

Mr. RAYMOND. Thank you. Two areas: No. 1 is, I think, continuing to raise the recognition of cyber risks as equally as critical as physical infrastructure risk to our critical infrastructure. I think the second is to leverage—broader leveraging of funding that is available to the States for a variety of different directed programs; that if we could leverage that more broadly to address the cyber risk across the State, that would be tremendously beneficial to the States.

Mr. DONOVAN. Thank you, sir.

Mr. Galvin.

Mr. GALVIN. Chairman, thank you. So I outlined 3 in my opening remarks. If I had to narrow it down to—I could narrow it down to 2, which I think is in the area of readiness. I talked a little bit about coordinating cybersecurity simulation incidents. My intent there is really not so much to exercise the cybersecurity plans of each organization or agency, but to look at the coordination between agencies and organizations. For example, the Port Authority relies heavily on Customs and Border Protection and the FAA. But there is no one organization that is responsible for overseeing a coordinated response to a coordinated attack, which is a very high concern for me.

The other I talked about is public education. So as a technology practitioner professional who has been working in the technical areas for 30 years, frankly, I don't know how most normal individuals who have training in other areas deal with the onslaught of technology that comes at them every day. We have all been trained as technology professionals in information access and security and control mechanisms and so on and so forth.

Today, people buy WiFi devices, they come home, and they set them up. They buy televisions that interconnect with their WiFi networks and their cable systems. There are protections that you can use and leverage, but without some kind of a training plan, I don't know how people deal with it. I assume that what happens is most of them, if they don't have someone in their life that works in the technology sphere to come and help them set up, I think they take it out of the box, they plug it in, and if it works, they declare victory and they leave it until it breaks and they buy another one.

So I think public education has a huge role in protecting individuals' information as well as the information at risk in organizations, because what we are seeing is social media being leveraged by people who are posing a threat in order to gain access to corporate and agency systems.

Mr. DONOVAN. Thank you, sir. I thank you, all, for your testimony and sharing your expertise with us.

The Chair now recognizes the gentleman from New Jersey, Mr. Payne, for questions.

Mr. PAYNE. Thank you, Mr. Chairman.

Just on Mr. Galvin's last question, I resemble some of those remarks. I was the relative back in the 1980s that hooked everyone's VCR up. So I went around to all my aunts and uncles and that was my job for a while, so I understand what you are saying in terms of that.

I will stay with you, Mr. Galvin. You know, like California, we in New Jersey have established a State cybersecurity and communications integration cell with the goal of bringing together diverse stakeholders, promote State-wide awareness and local cyber threats and wide-spread adoption of cybersecurity best practices.

In your opinion, is New Jersey cybersecurity cell carrying out its mission effectively? What is it doing well and what should it be doing better?

Mr. GALVIN. Great. Thank you.

One thing I want to make clear is that, you know, the work of securing our information assets and ensuring the reliable function of our systems is performed by a, in my organization, a hard-working staff of technology and security professionals, and also in our partners' agencies. I am truly fortunate to work with such a talented and dedicated set of public servants. I assume that other members of the panel have a similar experience.

This is a team effort. You know, we recognized early on putting our cybersecurity program together that there was no one group or individual that was going to have the total solution. So we have developed strong partnerships with New Jersey CISC, New York CIG, New Jersey State Police, NYPD, FBI, DHS, the MS–ISAC, US–CERT, and ICS–CERT, and we continue to engage with those agencies to perform vulnerability assessments and to assist with incident response.

Likewise, we also, in this process of putting our cybersecurity program together, strengthen internal partnerships between the chief security office, which the Port Authority is responsible for the PAPD, the Office of Emergency Management, the Office of Inspector General, and the technology departments. So it's definitely a co-

ordinated team approach that—I think you said it very well, Mr. Ghilarducci, that it is a team solution.

Mr. PAYNE. So you feel that you are breaking through the silos of these different entities and working together to better assess these threats?

Mr. GALVIN. We do. We spent time—I assume this will probably be a question—breaking down the NIST 853 framework, and we did a RACI diagram—responsible, accountable, consulted, and informed—to identify who was in the lead for each of the different tasks. It was a very lengthy exercise, but it was extremely valuable to us in helping put our plan together.

Mr. PAYNE. Thank you.

Mr. Ghilarducci, every year the National Preparedness Report reveals that of the 32 core capabilities, States are least confident in cybersecurity. At the same time, States invest very little of their homeland security grant funds into improving that cybersecurity capability. Why do you think that is?

Mr. GHILARDUCCI. Well, I think that part of it is because really the emphasis from DHS to States, to the State administrative agents or to the HSAs that are doing the investment justifications, are not necessarily clear.

The whole concern about cyber, as has been stated here, really isn't fully yet understood. This is an evolving threat. It is getting more complex. It is getting worse as the days go on. I think that we, as DHS and the States, really we need to catch up with the fact that this threat is not going away.

So once the DHS—and of course Congress—allocate funding specifically targeted towards the cyber threat, I think that then you will start to see States start to implement more of that capability.

Now, I would say that just this year, I, as the SSA, went into our investment justification and broadened the investment justification to include cybersecurity and countering violent extremism to be able to push down to local grant recipients at other State agencies and local governments so that they could utilize what funds they do have and repurpose those funds. But, as you know, funds are pretty limited as they are, and it is hard to sort-of move one thing to start working on the other. So it is a constant prioritization and reprioritization issue.

Mr. PAYNE. Thank you.

Mr. Chair, I will yield back.

Mr. DONOVAN. The gentleman yields.

The Chair now recognizes the gentleman from Texas, Mr. Ratcliffe, for questions.

Mr. RATCLIFFE. Thank you, Mr. Chairman.

Earlier, I guess the end of last year, we passed an information-sharing bill in this Congress aimed at improving our ability to timely share cyber threat indicators.

I want to start with you, General Spano. How would you characterize the quality of the information flow that the MS–ISAC has with the NCCIC?

Mr. SPANO. I would say that the quality, I believe, as representative and testified by FBI and other DHS of information that we provided from monitoring State networks, is very high quality, and it is fused. We have representatives from the MS–ISAC that sit on

the NCCIC floor as liaison, so they are very integrated into that mission.

Mr. RATCLIFFE. So is that how you give feedback in terms of what information you are getting that is valuable?

Mr. SPANO. The feedback of what we provide comes from our analysis within the MS–ISAC from our monitoring mission. So, for instance, 2015, we analyzed 3 trillion records and provided 56,000 alerts, sifting through all of those that were actionable for the States, but we also fed into the NCCIC for further analysis and fusing with other sources of intelligence.

We have supported FBI investigations with some of our analysis of what we have seen at the State level. So the conduit and the function and the command and control has been working extremely well based upon the maturity of the ISAC mission and its capabilities year over year.

Mr. RATCLIFFE. Okay. So I am pleased to hear that the sharing is going extremely well.

Can you offer, would you offer anything to improve the efficiency or effectiveness?

Mr. SPANO. Again, what we provide is, I think, moving up in its intelligence. The processes are lean and getting better as we continue to strengthen that relationship. The challenges, I think, are more downward into the State levels, as I talked about with respect to some of the resources.

Mr. RATCLIFFE. Yes. You talked about the workforce being a challenge.

Mr. SPANO. Right.

Mr. RATCLIFFE. I think you characterized it as high-demand, low-density.

So what can DHS do to create a workforce that is well-trained and fully-equipped to respond to cyber threats?

Mr. SPANO. I don't know that it is any one responsibility or one responsibility of any single agency. I believe it is a collaborative effort at all levels—public, private, facilitated, encouraged by DHS. They have a number of programs that the ISAC implements to try to encourage younger students. We do a poster contest, and the CIS offers some summer camps to try to encourage it. There is a scholarship for service under the National Science Foundation, which is really important. We believe that looking at that and examining whether we can continue to do that.

It is not any silver bullet that is going to solve this problem. It is a generational problem where if the pipeline at the K through 12 is not satisfying the growing demand, you are sort-of always chasing. Looking at it from a comprehensive perspective of how to ignite that STEM capability at all levels and then balancing the differences between the public and private partnerships, I think will help create a stop-gap with programs that are specific to workforce exercises, joint exercises, to raise awareness.

Mr. RATCLIFFE. All right. Thank you.

Let me turn to you, Mr. Raymond. Last month I held a field hearing in my district where I got perspectives from fire chiefs and local law enforcement officials on how they are responding to cyber incidents. I want your perspective from the State, the NASCIO perspective.

What is the greatest limitation out there right now for States in terms of defending their cyber networks? I guess part 2 of that is, are there shared best practices that NASCIO is using to coordinate between State CIOs and local first responders and law enforcement?

Mr. RAYMOND. Thank you for that question.

I would say that the biggest challenge is the velocity of the threat and the changing threat. So continued improvement on providing information and actionable information as efficiently as it can be provided almost to machine-to-machine level to allow us to react will continue to allow the States to be able to defend as best we can. It does help with the workforce issue in many ways where we can have our machines responding on our behalf.

In terms of working out with the field, NASCIO has put out over 31 different publications that are responsible or intending to work with both the education aspects, so making sure that our leaders understand how important cyber, is all the way to practitioners. We have over a 100-page cyber guide and a set of information for State information security officers on best practices that we have assembled across the States to help them as they are new to these rules. We do have turnover, that they can pick it up quickly and understand the very diverse environment that we have across all States.

Mr. RATCLIFFE. Terrific. Thanks very much.

I appreciate you all being here and your testimony.

My time has expired, so I will yield back.

Mr. DONOVAN. The gentleman yields back.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our panel here today. Your testimony was excellent, and I appreciate your work that you are doing in this field.

Let me start, if I could, with Mr. Raymond and Mr. Galvin. Let's say that the State of Connecticut or the Port Authority has experienced what you, Mr. Raymond, in your testimony term a cyber disruption event. Whom do you call first?

Mr. RAYMOND. For Connecticut, we actually have a cyber working group. So the homeland security adviser, Deputy Commissioner Bill Shea, and I work closely with this. Our first call is to the fusion center and then to MS–ISAC in terms of coordinating our events. We pull together a cyber response team that includes both homeland security and my office in terms of dealing with the response.

Mr. LANGEVIN. Okay.

Mr. GALVIN. For our organization, we have a cybersecurity operations center that would likely be the initial point of contact or the discovery point for a potential incident. We would assess as much as possible the depth of the breach before reaching out. But we would certainly contact MS–ISAC. Usually they find out the same time we do. If we identify that the breach involves personally identifiable information or something of that sort, we would initiate a call to the FBI.

Mr. LANGEVIN. Okay. Thank you.

As a follow-up, Colonel Cooney and Mr. Ghilarducci, as individuals with emergency management roles, whom do you recommend New Yorkers or Californians call in the event of a disruption event?

Mr. COONEY. For us it depends on the nature, but, of course, I would say the NCCIC, the fusion center being collocated with the MS–ISAC, and then we would take it from there depending on the nature of it.

Mr. GHILARDUCCI. As well, it depends on the nature. With this new integration center we built, this will be the central point where all information and reporting will flow into. If there is a criminal predicate associated with the intrusion, our State police that has a cyber crime investigation unit will sort-of take the lead and be supported by the rest of the entities that have come together in a collaborative way.

But that is the process. Because the center also includes connections with DHS and FBI, they are right there with us, and then we can move on as rapidly as possible.

Mr. LANGEVIN. Do you all feel comfortable with knowing who in particular who to call at the Federal level and who would respond to you in the event of a cyber disruption event? I have found that that is something that is unclear to many, whether it is big businesses or even Government agencies. Are you all clear on that, and who would you call?

Mr. GHILARDUCCI. Well, this is a question, I mean, we typically would turn to the FBI, DHS as information sharing. But the FBI would be working with us on the actual analysis of the intrusion. But the Secret Service also plays a role in it. So there is a little bit of a conflict there. But, typically, our next step is to go to the FBI.

Mr. LANGEVIN. Okay.

Mr. GALVIN. I think your point is well taken, though, that in the private sector I think there is less awareness of who to call. You have got a panel of people who work in Government and who spend time putting together cybersecurity program, so we more than anybody are going to know the right individuals to call.

But I think you are correct that depending on the nature of the entity, particularly a privately-held organization, I am not sure they would know who to reach out to.

Mr. LANGEVIN. I think that is why we have to work at the Federal level here to help get the word out more. One of the first places to go, in addition to FBI, would also be the NCCIC or US–CERT to request Federal assistance.

But, Mr. Raymond, if I could, in your testimony you mention that NASCIO recommends that the States have a cyber disruption response plan. I know you highlighted New Hampshire, Massachusetts, and my home State of Rhode Island. I know what we have been doing in Rhode Island, that our cyber disruption team that we have created has visited all the stakeholders at the table, emergency management people, State police. We have our colleges and universities, as well as the private sector at the table. It has really proven to be very effective at bringing the stakeholders to the table to plan for a response to a cyber disruption event.

Is there a way for the Federal Government that we can encourage this type of approach?

Mr. RAYMOND. I believe as it related to education and continuing to hold exercises, continuing to participate through homeland security and having the States describe their disruption plans, I think all of those encouragement points are very helpful in organizing States' response to incidents like that.

Participation. NGA is holding a cyber policy academy for several States. Connecticut is one of those participating. That helps brings best practices across the States. I know that DHS is a good partner in that exercise as well.

Mr. LANGEVIN. Thank you all.

I yield back.

Mr. DONOVAN. The gentleman yields back.

The Chair now recognize the Vice Chairman of the Subcommittee on Emergency Preparedness, Response, and Communications, the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman.

Thank you, panel, for being here and the professional testimony. Very detailed, very important to us.

Mr. Raymond, I have a question here. Two-part question, so I may break it up. How can the roles of information-sharing organizations such as MS–ISAC and ISAC be more strongly defined and effectively implemented?

Mr. RAYMOND. I know that we actively work with MS–ISAC, and we find that it is fairly defined. I am not sure I understand how more strongly——

Mr. WALKER. Let me add a little more description. Should their responsibilities be strengthened to increase information-sharing efficiency? Is that fair?

Mr. RAYMOND. Yes. I believe the velocity of information sharing specifically across all players can be improved.

Mr. WALKER. Okay.

General Spano, what efforts does the MS–ISAC take to gauge customer satisfaction with the States that they are engaging with?

Mr. SPANO. Sure. So we have an executive committee that is comprised of several of the representatives from the CISO's office and the security professionals. We have monthly calls with all the members. We have over a thousand members, although the 56 are the ones that we actively are pursuing monitoring with. We have an annual conference that they attend. We provide newsletters, efforts, the NCSR we manage on behalf of DHS to get their self-assessments to work. So it is a very strong and growing collaborative environment.

Mr. WALKER. In your testimony, I believe you described the value add of a State being a member of the MS–ISAC?

Mr. SPANO. Correct.

Mr. WALKER. What additional services or capabilities do you see the MS–ISAC being able to provide taking up the next 5 to 10 years?

Mr. SPANO. The next 5 to 10 years, I believe that as we help solidify the basic hygiene of the security framework, such as the controls, as the foundations at the State level, and begin to help them evolve from the basics of just trying to keep their systems patched

and configured correctly, I think the whole state or posture of cybersecurity will eventually begin to increase at a much more rapid pace. That is one specific area.

As technology evolves to the Internet of Things and into the cloud environment, there may be a different dimension to cybersecurity that has not yet fully matured or evolved or is understood.

Mr. WALKER. Sure.

Mr. SPANO. So we have started to move out by offering those hardened images within Amazon Web Services, and we are talking to the other cloud providers like Microsoft to be able to provide the same type of hardened machine images in their cloud so that as the States begin to move toward cloud they can do it much more securely than they are now, because there are tremendous advantages and cost savings that could help fuel resources to help in the cybersecurity area.

Mr. WALKER. My next question was, what kind of steps do you see there to effectively get us there? But I think you just touched on some of that.

Let me take, if I could, please, going back to Mr. Raymond, what do you currently see as the greatest limitation of the States' ability to defend just against the general cyber attacks? Can you speak to that for a second, talk about the problems there?

Mr. RAYMOND. Different States are organized very differently. We a critical infrastructure provider from State data centers to State networks. I think if we look at sort-of the complexity of the business that we serve, from schools, libraries, in some instances hospitals, so the diversity of the population that we serve and that sort of discreet nature of how funding comes in, doesn't allow us to leverage things as broadly as we would like. So I would say that that is one of the primary challenges.

Mr. WALKER. Can I open that up to anybody else on the panel? I have got 57 seconds left. Anybody else want to touch on the States, sort-of the obstacles there?

Mr. SPANO. I think one of the bigger challenges that they have that makes implementing cybersecurity tougher is a more strategic problem in how software and applications are developed. So many of the software products are coming out of the box with inherent vulnerabilities, and I think they are poorly crafted and require a lot of lift to continue to sustain it.

That is not going to be solved in any sweeping legislation, but it has to be addressed, because the competitive nature of providing software and services and applications to get the speed and agility that you need to compete means you are getting beta versions and you are a little bit sloppier in the production. The applications that you are building, even internally, to do specific things are oftentimes poorly crafted and have security vulnerabilities that tax your cyber professionals.

Mr. WALKER. My time has expired.

Mr. Ghilarducci, you looked like you were in agreement there. Did you need to add anything to that?

Mr. GHILARDUCCI. I would just say that cyber, what I call low-hanging fruit, just cyber hygiene training across the board can go a long way in making sure that State employees and State networks are as robust against attacks. That is one of the things that

there is really not a lot of consistent and standardized training that is really made available, and I think that more of that would help a great deal.

Mr. WALKER. Thank you, Mr. Chairman.

Mr. DONOVAN. The gentleman's time has expired.

The Chair now recognizes the gentlewoman from New Jersey, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman.

Good morning, gentlemen. Thank you for your testimony.

Mr. Galvin, frequently the first person to decide what to do in response to a cyber incident is not the CEO or even senior leadership, it is the operational personnel level and often physical security professionals who are vastly more comfortable protecting against physical threats than threats to a network.

My question is: What are the most important relationships emergency responders should maintain with private-sector employees at all organizational levels?

Mr. GALVIN. It is a very good question, Congresswoman. Thank you for it.

I think your observation is entirely accurate, that the person who is sitting at the facility overseeing operations is the person who is going to see the symptoms or the effects of a cyber attack first and foremost. I think there are several important relationships. One, within any organization, there has to be training to make sure that the person who is operating the facility is aware of what they should do in order to pick up the phone and contact, in our case our help desk or our CSOC, cyber security operations center.

Then from there it goes from a technical professional who is going to field the call and take a look at the nature of the threat and make a determination as to whether this is an opportunistic thing that is just a latent incident that has been there active for a while versus something that is emergent. Then that person escalates it internally in our organization, and I would suspect that a lot of organizations are similar. There is a kind of a tiered operation that goes on. It goes to a second- or a third-level person in order to investigate and follow up further on.

So I think the relationships are first and foremost between the operations personnel and the technical personnel, and then second is the escalation in the partnerships that happen within an organization as well as awareness as to where to escalate it further if the threat cannot be contained.

Mrs. WATSON COLEMAN. Thank you. This is a question I would like to start with you, Mr. Galvin, and then kind-of move on down as quickly as we possibly can. This has to do with sort-of just imagine a cyber Katrina.

So our question is, I mean, if we fail to develop, implement, and train on doctrine to respond to a cyber event with physical or collateral consequences because it is something we have not seen before, then we will be inventing the wheel as we try to drive the car when we have these attacks. So my question is: From your perspective, what is the most important action the Federal Government can take to ensure that the communities can effectively respond to a cyber event of this nature?

Mr. GALVIN. Again, I think it relates to the readiness and the preparedness. We haven't really talked about this yet, but one of the things that keeps me awake at night, and I am sure it keeps a lot of CIOs awake, is industrial control systems or operational technology.

So we have talked a little bit about IT systems and the fact that there is patching required. We are used to that as technology professionals—oh, there is a fix that came out. You know, Microsoft has patch Tuesday, and it has turned into cyber threat Wednesday, right? Because they release the vulnerability, people know about it, and they try to leverage it.

But there is no analog to the operational technology world, the things that control lighting systems or fire alarm systems or ventilation systems or things of that nature, and those pose a real threat for us.

I am sorry. I am getting lost in your question. But——

Mrs. WATSON COLEMAN. What do you see the Federal Government——

Mr. GALVIN. Yeah. So, again, I think it has to do with the preparedness, making sure that the plans are in place to respond and that there is coordination between organizations, not just within a single organization.

Mrs. WATSON COLEMAN. Thank you.

Is there anyone else who would like to respond to this question? Mr. Raymond.

Mr. RAYMOND. Thank you.

I think continuing to sponsor and participate in exercises that allow the States to demonstrate their preparedness as Internet of Things continues to grow, unmanned vehicle systems, all of that will continue to get more complex. So being an important sponsor to allow us to play and work through these exercises in advance and think through them helps us really prepare for real events when they do occur.

Mrs. WATSON COLEMAN. Thank you. Thank you.

One quick question, since we can't go down there. On a scale of 1 to 10 being the very best, how well are we doing in incorporating risk into emergency response plans and developing contingency operations?

I should just probably give that to you, Mr. Ghilarducci. Did I slay that name?

Mr. GHILARDUCCI. You did great. Thanks.

Well, I appreciate the question, Congresswoman. We don't need to reinvent the wheel with regards to all-hazard planning. I mean, we have a national construct, a National Incident Management System, and having those capabilities in place to respond to the consequences, the cascading consequences of a cyber attack, should be reinforced and exercised and built upon.

The delta or the challenge is that the traditional systems that we depend upon for communications and situational awareness may be actually impacted by a cyber attack. So we need to make sure we have continuity of operations redundancies put in place. This was an area where the Federal Government can support States. You want to leverage that public-private capability so that you are uti-

lizing the most information you can get to be able to make the right decisions.

So in your training and in your focus you need to also plan for—you know, don't just always plan for the technology is going to be operational. Start to do exercises and plans where you lose all that. How are you going to continue to communicate? How are you going to continue to get resources and get situational awareness in a timely way to make sure you protect lives and property?

So those are some of the things. But it has to start with the construct of that all-hazards environment and our NIMS construct.

Mrs. WATSON COLEMAN. Thank you. Thank you very much.

I yield back my time, even though I am over it.

Mr. DONOVAN. The gentlewoman yields back the time that she doesn't have.

We have a few more moments, and our panel travelled so far, I would just like to offer a second round of quick questions for my colleagues.

I just would like to start. We spoke about your challenges, and each of you told us about the challenge of lack of resources, competing, the competition for talent with industry, the inability to share information because of its classifications.

Would each of you just share with us what you think your biggest achievement is or your biggest success, without divulging trade secrets to our enemies, that maybe some of your colleagues would be able to piggyback on and use in their various environments?

Mr. GHILARDUCCI. I will start. I guess two areas. Again, it continues to evolve for us, and we are working hard at it. But that is the establishment of a public-private nongovernmental academic cybersecurity task force to be able to share information and best practices and recommendations and ideas to help us as a State drive those ideas forward, and the establishment of this integrated cybersecurity fusion center, if you would, that collocates with our primary fusion center and our critical infrastructure protection team, they can come together and all be looking at similar threat streams together with an effort to be able to mitigate prior to the event actually having the greatest impact.

So I think those are two areas. Then spinoffs from those is working with K through 12 and community colleges. We have actually implemented a cyber warrior program in California that has just taken off—I hate to use the word like wildfire, because we have a lot of those—but has really taken off in California. The cyber warrior program for high school students and community college students has really been well-received, and really we are trying to make that cyber warrior work for us.

Mr. DONOVAN. Thank you, sir.

Lieutenant Colonel.

Mr. COONEY. I think it would be the establishment of our cyber analysis unit at our fusion center. I think we were fortunate to find the right people and the right mix between technical capability and the ability to do intelligence analysis. It has worked well for us in an area that, as I mentioned in my testimony, that when it comes to cyber intrusion and the intel up front in the prevention realm, this is still relatively new for us. We got into it in about 2014 and

so far we have made some good progress. So I would say if other States could emulate that, then they may find that beneficial.

Mr. DONOVAN. Thank you, sir.

General.

Mr. SPANO. Yeah, I would say that the success of the ISAC in terms of showing how public and private can come together to address an issue of such National importance. Within the ISAC, I probably would highlight our CERT function, which is probably one of the best, certainly, in the Nation. I would like to say that it is probably world-recognized in terms of its ability to conduct forensics and analysis for a plethora of customers, predominantly, of course, focused at the SLTT.

Mr. DONOVAN. Thank you. Mr. Chairman.

Mr. Raymond.

Mr. RAYMOND. Thank you. One of the things that I think we are really proud of in Connecticut is that we have been sort-of baking telecommunications and networking into our incident response teams. So we have had several weather events over the past few years and through that it has become really critical that citizens rely on communication technology much more so than they ever had before.

So we do have a response team associated with restoring commercial networks and communication structures. Having those relationships at the ready has allowed us to respond very quickly when Superstorm Sandy came and to be able to restore communications as much as possible.

Mr. DONOVAN. Thank you, sir.

Mr. Galvin.

Mr. GALVIN. Thank you. At the Port Authority, the technology, the policies, the procedures, and the personnel that we have put in place, we have been able to detect and automatically block 90 percent of the critical incidences that we can see on our network, and we have been able to reduce our critical incident response time by two-thirds in the past year.

So we are proud of these things, but there is a lot of work that remains to protect our critical technology assets. As many people on the panel have already talked about and I won't repeat, the threat continues to evolve and the attack surface continues to expand with mobile devices and the emerging Internet of Things. So we are confident, but we are continuing to work diligently.

Mr. DONOVAN. Thank you, sir.

The Chair now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman.

Mr. Galvin, in your testimony you note that the Port Authority has undertaken an effort to better understand cyber vulnerabilities and address them. What is the biggest challenge in carrying out this task? What has the Port Authority learned in the process that might help other ports or critical infrastructure owners conduct a similar assessment?

Mr. GALVIN. Thank you very much.

So I think the size of the task is enormous. We have approximately 690 applications to assess. I think the lesson that I would give to other organizations is to start now. It doesn't decrease in

effort or size as time goes on, because there are new techniques, new technologies that every day get introduced into the organization whether or not you are aware of them. They do require an assessment.

So it is a huge effort, and the limiting factor, I think, is the size of the staff and the ability of our organization to absorb what we learn.

Mr. PAYNE. Thank you.

Mr. Ghilarducci, you have observed that risk assessments used by some States do not adequately address the top cyber threats or systematic interdependencies. How can we help States better assess their cyber vulnerabilities? Should FEMA be improving the bureau guidance, or should the Federal Government be providing separate guidance on how to conduct cyber assessments more thoroughly?

Mr. GHILARDUCCI. Well, the guidance, I mean, really, the standards for assessments that we are using really are the NIST standards. I think that we would all agree that a little bit more meat could be put on the bones around doing assessments that speak a little bit more to the various aspects of the emergency management or public safety spectrum.

I know we are looking at networks, but when you look at the networks' vulnerabilities, we also need to think about in the long term what would be the consequences should we lose certain networks and sort-of play that out in a little longer bit way. So FEMA would be a good entity to be able to provide some additional guidance there.

The other thing is DHS, through their protective service analysts that work with our critical infrastructure protection folks, they do provide some additional support, and we appreciate that. But we probably need to get some area associated with the cyber networks, particularly when looking at private sector, given that most of the infrastructure is owned by the private sector.

We need to continue to work to link those together with regards to the assessment process, because sometimes information sharing is a little bit challenging, because of proprietary and competitive kind of issues, but we need to find a place that we continue to share information to strengthen our capability as much as possible.

Mr. PAYNE. You also talked about States playing catch-up in developing a whole-of-the-government approach to cybersecurity and noted that even in California only 13 organizations have participated in the cyber hygiene partnership.

Why do you think more agencies within the States are not participating? What can the Federal Government do to encourage improved buy-in for cybersecurity efforts among State and local agencies or even in the private sector?

Mr. GHILARDUCCI. Well, I think maybe Mr. Raymond and others may be a little bit more to talk about the challenges in State government. I know for us it has been, I think, one, framing and understanding of the threat. It means different things to different people. We need to be more outgoing, external, like we do with a lot of other preparedness programs.

This is where the Federal Government, through cyber hygiene initiatives and other kind of training opportunities to build that

knowledge base as to what it means to sit at a device or get onto the internet and what kind of challenges you could be faced with with regards to threats. So training and education is one thing.

The second piece is, I think because there is a lack of knowledge, particularly at the Executive level in making decisions on funding allocations for doing assessments, quite a few times it is, you know, because you don't understand it, it is not made as a priority as it should be.

Let's face it, we as a collective country, and it is just across the board, are behind the power curve with regard to this threat. We all are working very hard collectively, but we do need to do more to step this up. You can't just say it is a priority, we need to put resources behind it to really and truly make it a priority. Just like we have done with other kinds of threats, whether it is natural or human-caused threats, we throw a lot of resources at that to make sure that we are in front of it and are effectively all knowledgeable about it.

Mr. PAYNE. Okay.

I yield back, Mr. Chairman.

Mr. DONOVAN. The gentleman yields.

The Chair recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I just want to go back to something we had talked about in terms of knowing who to call.

Mr. Ghilarducci, maybe I have a question for you. I just wanted to follow up with a point that Mr. Galvin had made about the private sector knowing who to call.

So just so I understand, so if PG&E has a cyber incident, do you recommend that they contact you or DOE or DHS first? Are you concerned about losing visibility if critical infrastructure providers go Federal first?

Mr. GHILARDUCCI. We have the California Utilities Emergency Association, it is an entity that is funded and supported by all of the major utilities in California, embedding into your cyber integration center. It gives them that one sort of belly button, so to speak, to be able to make the call and open all of the contacts in a one-call sort-of format.

It is challenging, I think, for them now because they do have a lot of people that they need to be reporting to. Inadvertently, what happens is that someone, some entity that needs to know what is going on falls through those cracks.

The other thing is that, historically, there hasn't been a lot of desire, I guess, so to speak, to let too many people know what is going on because of demonstrating vulnerabilities that an organization may have.

So by utilizing authorities and procedures that are being put in place through this integrated approach, it gives the utilities and the privates, the health industry similar kind of thing, a single belly button to make the call. We are all looking at it at the same time, and all of the required notifications can be made at one point.

Mr. LANGEVIN. Okay. Thank you.

Yeah, I think that the point about being reluctant to share, by the way, we have got to work at getting over that, because, obvi-

ously, if one is vulnerable, everybody is vulnerable, and that is what, hopefully, information sharing will help to mitigate.

You know, we have been talking a lot about assessments this morning, but equally important is not only knowing the vulnerabilities that may exist in your assets, in your systems, but also knowing the value of the data that you are holding.

So for Mr. Spano, Mr. Raymond, in Rhode Island, where I am from, our Governor, Governor Raimondo, set up a cybersecurity commission to examine the State cyber posture. One of the biggest initial findings had to do with managers not understanding the value of the data or systems and their vulnerability to attack.

Incidentally, this is the same problem that the Federal Government faced with the OPM attack, knowing that their systems were vulnerable, but also not understanding the value really of the data that they were responsible for protecting.

In your experience, how well do State agencies, particular those that aren't focused on IT, understand their exposure and also the value of their data?

Mr. SPANO. The value question is hard to quantify other than to say that the question of the scope and standards of protection has been one that has been discussed and debated since sort-of the evolution of the internet into the challenges that we are facing today: What do I protect and how much protection is enough?

We have got the full classification of systems. So I think there is a clear understanding of Secret, Top Secret. It is within that Unclassified regime of understanding personal identifiable information, HIPAA information. I think, by and large, there is a rudimentary understanding at sort-of the basic masses of employees that deal in those environments and with that information.

There are isolated and pockets of excellence where managers are being trained in how to deal with HIPAA and identify PII, but by and large it is a challenge with educating your existing workforces against the basic cyber threats and the basic protections that they can do, as well as sort-of the identification of what that value is of information.

Mr. LANGEVIN. Okay. Thank you.

Mr. Raymond.

Mr. RAYMOND. I think that the States' response—it has been my experience that there are sort-of 2 buckets, right? One is for those who have regulated data, whether it is HIPAA, protected medical information, FERPA data, IRS, those organizations are very much aware of the value of the information that they have.

I think for those that have nonregulated data but that may be important to protect, I think that the reliability of—or the awareness of what they have and the importance to protect it may be a little bit less.

I know in Connecticut we have a data classification policy that makes you look at what data you have and how valuable it is in terms of treating it for data sharing or at least protecting, and I think having that kind of approach for all States can really raise that visibility level that you describe.

Mr. LANGEVIN. Very good.

Thank you, Mr. Chairman. I yield back.

Mr. DONOVAN. The gentleman yields back.

The Chair now recognize the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me thank the Chair for his courtesies. Let me acknowledge the Chair and Ranking Member sitting, wearing many hats, Mr. Payne, to the full committee Chair and the full committee Ranking Member. We have overlapping committees, and I just came out of the Judiciary Committee, so I thank you for your courtesies.

This is a very important hearing, which is one of the reasons I did the mad dash, because I chaired this committee when it was the Transportation and Infrastructure Committee, which included all of the Nation's technological networks. I remember visiting water and sewer plants and seeing the openness and the expanse and wondering what potential terrorist act or manipulation of the technology dealing with it. I just came back from Silicon Valley, and they are pleading for individuals who can code or to write code.

So I want to offer to you some thoughts. Obviously, you have not looked at it, but I have a bill, H.R. 53, Cybersecurity Education and Federal Workforce Enhancement, which is to target in and focus in on building up the workforce for the Federal Government, dealing with technology. Also H.R. 60—one is H.R. 53 dealing with education—H.R. 60, the National Guard Act to develop a civilian force that can be activated in the event of a major cyber attack or event.

Now, if we were domestic, we know that we have NORTHCOM that would rise up and be part of dealing with any attack to the United States in a very massive way. I pushed NORTHCOM to be engaged on State and local. But this is technology, this is a cyber attack.

So if you can answer the question, the importance of building the workforce, and as well the importance of having well-experienced individuals for a massive attack that deals with infrastructure, such as water and sewer, such as our electrical grid, and the one that I live with every day, the petrochemical industry, which is highly automated at each stage of the process through energy extraction, transportation, processing, and distribution. As you well know, that is an arm of the movement of the economy in this Nation.

So if you could answer those, I would appreciate it. I will listen to you. Thank you. Is there someone who wants to take—thank you.

Mr. RAYMOND. I think education and workforce are incredibly important for us being able to respond. I would just add one comment. Specifically around the Guard and Guard response, I think that as it relates to us being able to have and retain workforce, because many of these folks are highly trained individuals and they can gain higher salaries in the private sector, having that capability of applying that in the event it happens at a State level is important.

We do work very closely. We have a monthly cyber meeting where members of the Guard participate in that for awareness capabilities. So it is one sort of creative way for the States to be able to utilize that capability and bring those skills to bear.

Ms. JACKSON LEE. Thank you.

Mr. GALVIN. I have a comment as well.

Ms. JACKSON LEE. Thank you. I appreciate it.

Mr. GALVIN. I think there are several different skills that are involved in doing incident response in cybersecurity. They not all of them require coding skills. I think the ability to think creatively, to think on your feet, to stay calm under pressure, I think those are all important skills that don't necessarily require coders.

On the other side, after an incident is detected and you are trying to figure out how to protect yourself in the future from similar attacks, because the nature of cybersecurity events is you have something that is novel and that is unique, and then you have multiple copies of it replicated with slight variations. So if you can protect yourself against one, you can kind of replicate the protection going forward. That is where you need a coder, a skill, someone who can take apart the threat or at least work with someone who can take it apart, because these are getting increasingly more complex as time goes on.

I think the other thing that you brought up was having a well of individuals to respond in the event of an attack on the grid or water systems or other such critical infrastructure is extremely important. Frankly, I think you have to talk to the operations people who would oversee the facilities to talk about what kind of staff those people are. If it is an attack on the grid, they are not IT people, because we don't function when there is no electricity.

So the question is really back to your response plan, and back in the day when a lot of us did initial kind of major systems implementations, there was always the plan, like, what happens if we are not going to go live and we have to go back to the old system? That was an old product that was dusted off.

So we have to go back and start looking at having those kinds of plans in place. Like, if the payroll system goes down, you go back to writing checks and doing things like that. So we need to start thinking about that in the face of these kinds of very major attacks on electrical infrastructure, for example.

Ms. JACKSON LEE. Let me pursue, if I could—thank you for that. I think it is important to emphasize calmness, creativity, and thinking on your feet. But this whole concept of code, what I gleaned from Silicon Valley, they are looking at it from one perspective, we don't have enough individuals Nation-wide. Maybe you would comment. I want to be able to see a far reach to be able to have those that can take apart a threat, which I believe that we are susceptible to.

So anyone want to comment on building that code, coding and coders, body of infrastructure in the human resource?

Mr. SPANO. Yeah, we talked about that a little bit earlier in terms of sort-of the urgency or the burning platform of it is a challenge to look at this problem as we have and other challenges where capacity could solve it. The challenges we face in cyber are challenges of complexity. Capacity can't solve a complexity issue, so we have to think about it in a much different way.

The workforce is not a simple fix of just going out and trying to figure out how you are going to compete with the availability. It is how do you produce a pipeline where there is zero unemployment?

That starts back from K through 12 and STEM and getting much more interest in those areas at a much younger age, encouraging colleges and universities to develop more curriculum and more degrees. It is tied to loan forgiveness and scholarship for service beyond that to encourage them to move into those areas.

So it has to be comprehensive and looked at across a broader spectrum of time.

Ms. JACKSON LEE. Yes, sir.

Mr. GHILARDUCCI. Thanks for the question. I think it is a good one. I agree with everything that has been said.

I think it is important that we sort-of understand kind-of talking about pre-event and post-event. Really the pre-event is where you need that workforce multiplier, those folks that are the coders, the folks that are going to interdict and mitigate prior to the event actually taking place.

The consequences of power outages or a dam release or something where there is infrastructure impact, our systems that are in place currently for consequence management need to be leveraged, and those are the ones that are going to be responding to the consequences. Unless there is an on-going series of cyber attacks, the attack itself may be done once and then you have got now a resulting series of consequences that you have to deal with.

The key thing, I think, is really in the pre-event phase, is trying to have that workforce. You mentioned the National Guard. I think the National Guard across the States is a model, a good model, that could be utilized for building real-time capabilities, where in the case of California there are a lot of people that work in Silicon Valley, actually, or in the IT industry, that are also guards men and women, and they bring them in on State Active Duty and be able work on the cyber topic. But they give you a workforce multiplier that you can continue to build upon.

But that is not exclusive, mutually exclusive, to the need, as the general was saying, in building out workforce from the high school level moving forward.

So I think that it is important that we think about it from the standpoint of, what do we have to prevent, interdict, and mitigate to minimize the impact? Then our consequence managers, the people who are going to respond, we need to train them with an understanding that, unlike a wildfire or earthquake, you may be operating in an environment with no IT, no situational awareness through the computer network, and you may have to go back to pen and paper to be able to get the job done. Those are the things that I think are important to understand.

Ms. JACKSON LEE. I want to thank the Chairman for his indulgence. If I can just, as I close, I would cite the petrochemical industry as one that argues for all that you said.

Anybody just want to comment on that?

Just because these industries are dealing not only with technology, but they are dealing with chemicals, it is just a combination that you need this holistic viewpoint.

Mr. SPANO. I think that is shared across finance, health care, electricity, and other critical infrastructures equally as well. Some are at varying levels of maturity in their thought, strategy, and execution.

Ms. JACKSON LEE. Well, let me say that I could listen to the experts that are here quite more extensively, but let me say that I am hoping to move these bills and also reviewing something called COIN technology—you may not have heard of it—or may have heard of it—that is supposed to be dealing with the bigger picture that you all are looking at.

Being on this committee for so long, I will just say that when we started, we knew that 80 percent of the infrastructure, which includes all that you are speaking about, was in the private sector. It may have gone up now, maybe 85 percent. So we know what our work is, and we know what our work is going forward, and this is a very important hearing for collaboration between Government and the private sector.

I thank you to the Chairman and Ranking Member, and I yield back.

Mr. DONOVAN. The gentlewoman yields back.

I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittees may have some additional questions for the witnesses. We will ask you to respond to these in writing. Pursuant to the Committee Rule VII(E), the hearing record will be held open for 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 12:03 p.m., the subcommittees were adjourned.]