CYBERSECURITY CHALLENGES FOR STATE AND LOCAL GOVERNMENTS: ASSESSING HOW THE FEDERAL GOVERNMENT CAN HELP

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

JUNE 25, 2019

Serial No. 116–29

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
38–782 PDF WASHINGTON : 2020

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Cedric L. Richmond, Louisiana
Donald M. Payne, Jr., New Jersey
Kathleen M. Rice, New York
J. Luis Correa, California
Xochitl Torres Small, New Mexico
Max Rose, New York
Lauren Underwood, Illinois
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Nanette Diaz Barragán, California
Val Butler Demings, Florida

Mike Rogers, Alabama
Peter T. King, New York
Michael T. McCaul, Texas
John Katko, New York
John Ratcliffe, Texas
Mark Walker, North Carolina
Clay Higgins, Louisiana
Debbie Lesko, Arizona
Mark Green, Tennessee
Van Taylor, Texas
John Joyce, Pennsylvania
Dan Crenshaw, Texas
Michael Guest, Mississippi

Hope Goins, *Staff Director*
Chris Vieson, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

Cedric L. Richmond, Louisiana, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Kathleen M. Rice, New York
Lauren Underwood, Illinois
Elissa Slotkin, Michigan
Bennie G. Thompson, Mississippi *(ex officio)*

John Katko, New York, *Ranking Member*
John Ratcliffe, Texas
Mark Walker, North Carolina
Van Taylor, Texas
Mike Rogers, Alabama *(ex officio)*

Moira Bergin, *Subcommittee Staff Director*
Sarah Moxley, *Minority Subcommittee Staff Director*

CONTENTS

Page

STATEMENTS

WITNESSES

FOR THE RECORD

CYBERSECURITY CHALLENGES FOR STATE AND LOCAL GOVERNMENTS: ASSESSING HOW THE FEDERAL GOVERNMENT CAN HELP

Tuesday, June 25, 2019

U.S. House of Representatives,
Committee on Homeland Security,
Subcommittee on Cybersecurity,
Infrastructure Protection,
and Innovation,
Washington, DC.

The subcommittee met, pursuant to notice, at 3:07 p.m., in room 310, Cannon House Office Building, Hon. Cedric L. Richmond (Chairman of the subcommittee) presiding.

Present: Representatives Richmond, Langevin, Rice, Underwood, Slotkin, Thompson (ex officio), Katko, Taylor, and Rogers (ex officio).

Mr. Richmond. The Subcommittee on Cybersecurity, Infrastructure Protection and Innovation will come to order.

The subcommittee is meeting today to receive testimony on cybersecurity challenges for State and local governments, assessing how the Federal Government can help.

Good afternoon. I want to welcome the panelists to today's hearing on cybersecurity at the State and local level. This is a topic that I believe deserves far more attention than it gets.

Since joining this subcommittee, I found that, while we can all agree that cybersecurity is an important topic, it can start to feel unapproachable to people on the ground. As Chairman, I want to spend some time looking at how cybersecurity impacts real people, like the ones I represent in the Second Congressional District of Louisiana. I know that my constituents work long hours and have hard jobs, sometimes more than one. Many of them are not thinking about phishing emails or ransomware or whether a hostile foreign government has gained access to the networks that control their drinking water, their transportation, or their medical care.

While the Federal Government has an important role to play in securing these networks, State and local governments own them. The staffing, structure, and resources available to State and local agencies vary across the country, but many of them are operating with a shoestring budget. Like Federal agencies, they are increasingly being targeted with sophisticated cyber attacks. Time and time again, we have seen that these attacks can be debilitating, taking out the tools and services people need to access health benefits, buy a home, or even call 9–1–1.

As any city official who has recovered from one of these cyber disruptions can tell you, the aftermath can have a hefty price tag. This is a drain on taxpayer dollars, time, and labor, all of which are in short supply at the State and local levels.

We also know that these attacks are becoming more frequent and more advanced. According to the security firm, Recorded Future, there have been at least 170 ransomware attacks carried out on county, city, or State governments since 2013, including 20 reported so far this year. That is just the incidents that were reported. The actual numbers are probably far higher.

But there is another problem as well. Today, we rely on the internet to an extent that we never have before. Access to connected devices and an understanding of how to use them securely is the very foundation of economic mobility. Yet we also know that many in our communities do not have the same means, access, or opportunity to build a level of comfort with technology.

While we talk a lot about how automation might impact the work force, we talk less about how poor cyber hygiene and low tech literacy can present a real economic barrier to entry. Right, now studies show that the most vulnerable underserved among us, low-income, immigrants, or elderly populations, are the most likely to fall victim to an on-line scam or click the wrong link. These mistakes can be costly, especially for someone on the margins. Negative experiences like these may also lead many to steer clear of important on-line services, like on-line banking, health management tools, or even email.

This response, left unchecked, will only serve to deepen economic divides and allow our most vulnerable populations to fall further behind. We have to confront this head-on. I look forward to hearing from this panel on how we might do that.

This is not a State or local problem but a National one, and we should invest accordingly at the Federal level. Ultimately, we cannot expect underresourced, understaffed State and local governments to defend their networks from State-sponsored hackers from Russia, China, and Iran. Toward that end, I am working on a comprehensive package to improve the cybersecurity posture of our State and local governments.

I look forward to hearing from our witnesses today about opportunities to address this important National security issue.

[The statement of Chairman Richmond follows:]

STATEMENT OF CHAIRMAN CEDRIC L. RICHMOND

JUNE 25, 2019

This is a topic that I believe deserves far more attention than it gets. Since joining this subcommittee, I have found that—while we can all agree that cybersecurity is an important topic—it can start to feel unapproachable to people on the ground. As Chairman, I want to spend some time looking at how cybersecurity impacts real people—like the ones I represent in the 2d District of Louisiana. I know that my constituents work long hours and have hard jobs, sometimes more than one. Many of them are not thinking about phishing emails or ransomware or whether a hostile foreign government has gained access to the networks that control their drinking water, transportation, or medical care. And, while the Federal Government has an important role to play in securing these networks, State and local governments own them. The staffing, structure, and resources available to State and local agencies vary across the country—but many of them are operating with a shoestring budget. And, like Federal agencies, they are increasingly being targeted with sophisticated cyber attacks.

Time and again, we've seen that these attacks can be debilitating—taking out the tools and services people need to access health benefits, buy a home, or even call 9–1–1. As any city official who has recovered from one of these cyber disruptions can tell you, the aftermath can have a hefty price tag. This is a drain on taxpayer dollars, time, and labor—all of which are in short supply at the State and local levels. We also know that these attacks are becoming more frequent and more advanced. According to security firm Recorded Future, there have been at least 170 ransomware attacks carried out on county, city, or State governments since 2013—including over 20 reported so far this year. That's just the incidents that were reported. The actual numbers are probably far higher.

But there's another problem, as well. Today, we rely on the internet to an extent that we never have before. Access to connected devices—and an understanding of how to use them securely—is the very foundation for economic mobility. Yet we also know that many in our communities do not have the same means, access, or opportunity to build a level of comfort with technology. While we talk a lot about how automation might impact the workforce, we talk less about how poor cyber hygiene and low tech literacy can present a real economic barrier to entry. Right now, studies show that the most vulnerable, under-served among us—low-income, immigrants, or elderly populations—are the most likely to fall victim to an on-line scam or click on the wrong link. These mistakes can be costly, especially for someone on the margins. And, negative experiences like these may also lead many to steer clear of important on-line services—like on-line banking, health management tools, or even email. This response, left unchecked, will only serve to deepen economic divides and allow our most vulnerable populations to fall further behind. We have to confront this head-on, and I look forward to hearing from this panel on how we might do that. This is not a State or local problem, but a National one—and we should invest accordingly, at the Federal level.

Ultimately, we cannot expect under-resourced, under-staffed State and local governments to defend their networks from state-sponsored hackers from Russia, China, and Iran. Toward that end, I am working on a comprehensive package to improve the cybersecurity posture of our State and local governments. I look forward to hearing from our witnesses today about opportunities to address this important National security issue.

Mr. RICHMOND. With that, I now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Mr. Chairman.

Thank you, all of our witnesses, for being here today. It is an important topic that couldn't possibly be more timely, as you all well know.

Our State and local governments are prime targets for cyber attacks. A May 2019 report by Record Future found that ransomware attacks on State and local governments increased by 39 percent in 2018 to 53 attacks. You know that all too well, Ms. Bottoms. In the first 4 months of 2019 alone, there have already been 21 attacks, including my home State of New York.

In 2018, the National Association of State Chief Information Officers found that many States typically spend only 1 or 2 percent of their budgets on cybersecurity. Most employ fewer than 15 full-time cyber professionals. It is not surprising, particularly given the burgeoning budget challenges many State and local governments face and the talent pipeline issues we have discussed in previous hearings.

It will take work on a collective level from Federal, State, and local governments, as well as outside stakeholders, to improve the situation. But it is clear that action is needed and needed now.

This hearing today is an important step, and I commend the Chairman for convening it. I look forward to hearing from our witnesses about their ideas about how to help.

I will soon introduce a bill, the State and Local Cybersecurity Improvement Act, which will direct the Cybersecurity and Infrastructure Security Agency, or CISA, within the Department of Homeland Security to develop a resource guide for State and local officials to navigate the challenges of protecting their networks.

My bill will also create two new grant programs. The first is a one-time grant for State and local governments to identify their high-value assets and system critical architecture. To protect something, you must know it is worth protecting. The second grant program that will be part of this bill will help State and local governments conduct exercises to train, prepare, and evaluate their ability to respond to an attack.

Working through an exercise allows a government to identify weaknesses in their current plan and establishes protocols and procedures to be prepared in the worst-case scenarios. My bill will help State and local governments be better prepared to defend their cyber networks. But the work we need to do to address this issue does not end with my bill. This is a collaborative effort. It is Democrats and Republicans. It is all of you at the table and everyone at every level of government. That is what we are going to need to attack this problem in an effective manner.

I look forward to working with my colleagues on this issue moving forward, and I want to thank the Chairman and our witnesses for speaking with us today.

Mr. Chairman, I yield back.

[The statement of Ranking Member Katko follows:]

Statement of Ranking Member John Katko

June 25, 2019

Our State and local governments are prime targets for cyber attacks. A May 2019 report by Record Future found that ransomware attacks on State and local governments increased by 39 percent in 2018, to 53 attacks. And in the first 4 months of 2019 alone, there have already been 21 attacks, including in my home State of New York.

In 2018, the National Association of State Chief Information Officers found that many States typically spend only 1 to 2 percent of their budget on cybersecurity. Most employ fewer than 15 full-time cyber professionals.

This is not surprising, given the budgeting challenges many State and local governments face and the talent pipeline issues we have discussed in previous hearings.

It will take work from Federal, State, and local governments, as well as outside stakeholders, to improve this situation, but it is clear that action is needed.

This hearing today is an important step, and I look forward to hearing from our witnesses about their ideas about how to help.

I will introduce a bill, the State and Local Cybersecurity Improvement Act, which directs the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security, to develop a resource guide for State and local officials to navigate the challenges of protecting their networks.

My bill also will create two new grant programs. The first is a one-time grant for State and local governments to identify their High-Value Assets and system-critical architecture. To protect something, you must know what is worth protecting.

The second grant program helps State and local governments conduct exercises to train, prepare, and evaluate their ability to respond to an attack. Working through an exercise allows a government to identify weaknesses in their current plan and establishes protocols and procedures to be prepared in case the worst happens.

My bill will help State and local governments be better prepared to defend their cyber networks. But the work we need to do to address this issue does not end with my bill. I look forward to working with my colleagues on this issue.

Mr. RICHMOND. The gentleman from New York yields back.

I now recognize the Chairman of the full committee on Homeland Security for 5 minutes.

Mr. THOMPSON. Good afternoon. I want to thank Chairman Richmond for holding today's hearing on an especially timely topic, the cybersecurity challenges in the State and local governments.

Just last week, Riviera Beach, a small city in Florida, agreed to pay a $600,000 ransom demand after hackers crippled city computer systems. Unfortunately, Riviera Beach is not alone. Hackers have been wreaking havoc on cities from Atlanta to Baltimore to Albany, and actually many more. These bad actors range from unaffiliated cyber criminals to sophisticated state actors, including Iran, and their interest in breaching State and local networks is only growing.

Since the Russian Government engaged in a historic campaign to meddling in the 2016 elections, officials at all levels of government have devoted time and resources to improve the security of election infrastructure. For its part, Congress appropriated $380 million, a down payment, for foreign grants to State and local election officials to replace unsecure election equipment, improve network security, and provide cybersecurity training to election officials. Additionally, for 2 fiscal years, Congress has provided the Cybersecurity and Infrastructure Security Agency additional funding to provide cybersecurity services upon request to election officials.

But administering elections is only one of the many important responsibilities carried out by State and local governments. These attacks that have come about have disrupted networks and local police departments, officers that process real estate transactions, and public health department, just to name a few.

So I am looking forward to the testimony from our witnesses today. As a former mayor myself, I understand the problems cities have, and mayors more specifically. So I look forward to Mayor Bottoms' testimony. But I am also eager to hear from MS–ISAC, which serves as the cyber threat information-sharing hub for State and local governments and spearheads State and local coordination on securing election infrastructure.

Finally, I look forward to understanding the disperate impact of cybersecurity incidence on vulnerable populations and how the Federal Government can partner with State and local government to address them.

I thank our witnesses for being here today, and I yield back the balance of my time.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 25, 2019

Just last week, Riviera Beach—a small city in Florida—agreed to pay a $600,000 ransom demand after hackers crippled city computer systems. Unfortunately, Riviera Beach is hardly alone. Hackers have been wreaking havoc on cities from Atlanta to Baltimore to Albany. These bad actors range from unaffiliated cyber criminals to sophisticated state actors—including Iran—and their interest in breaching State and local networks is only growing. Since the Russian government engaged in a historic campaign to meddling in the 2016 elections, officials at all levels of government have devoted time and resources to improve the security of election infrastructure. For its part, Congress appropriated $380 million—a down payment—to fund grants to State and local election officials to replace unsecure election equipment, improve network security, and provide cybersecurity training to election officials.

Additionally, for 2 fiscal years, Congress has provided the Cybersecurity and Infrastructure Security Agency additional funding to provide cybersecurity services—upon request—to election officials. But administering elections is only one of the many important responsibilities carried out by State and local governments. So far this year, there have been over 20 reported cyber attacks against government agencies. These attacks disrupted networks in local police departments, offices that process real estate transactions, and public health departments, just to name a few. The impacts ranged from jeopardizing 9–1–1 calls, grinding real estate transactions to a halt, and preventing health officials from warning the public when a bad batch of illegal drugs causes overdoses. Unfortunately, the sophistication of hackers is outpacing the speed at which State and local governments can implement IT modernization programs and phase out legacy technologies. Moreover, the attack surface is growing as more jurisdictions are integrating "smart city" technologies into the execution and delivery of government services.

As other sectors improve their cybersecurity posture, State and local governments struggling to keep pace with technology are becoming low-cost, high-value targets. It is time for the Federal Government to do more. Every year, States assess cybersecurity as one of the 32 core capabilities in which they are least proficient. At the same time, States rarely use their Homeland Security Grant to invest in cybersecurity as they stretch these funds to support traditional terrorism preparedness and response capabilities.

Make no mistake, State and local governments need to invest in security, especially as they invest in smart city technology. But it is time to improve the way the Federal Government helps them. Toward that end, I am pleased that Mayor Keisha Lance Bottoms is here today to share the lessons learned from the ransomware attack in Atlanta and to understand how the Federal Government can better help victims prevent, respond to, and recover from cyber attacks. I am also eager to hear from the MS–ISAC, which serves as the cyber threat information-sharing hub for State and local governments, and spearheads State and local coordination on securing election infrastructure. Finally, I look forward to understanding the disparate impacts of cybersecurity incidents on vulnerable populations and how the Federal Government can partner with State and local governments to address them. Addressing the cybersecurity challenges ahead will require strong partnerships among all levels of government, and I am eager to understand how Congress can help ensure that Federal resources are most effectively leveraged.

Mr. RICHMOND. The gentleman from Mississippi yields back.

I now recognize Mr. Rogers, the Ranking Member of the full committee on Homeland Security, for 5 minutes.

Mr. ROGERS. Thank you, Mr. Chairman.

I thank our witnesses for being here today, especially Mr. Cilluffo from Auburn University's McCrary Institute for Cyber and Critical infrastructure security located in my district.

The McCrary Institute serves as an invaluable resource to our State and the Nation with its cybersecurity and critical infrastructure work. Cybersecurity is a tremendous challenge facing all levels of government.

Our State level governments have seen first-hand through increased ransomware attacks that leave citizens without services and cities in panic. I am glad that our hearing today will discuss how Federal Government is already lending a helping hand and how we can improve the level of assistance.

I appreciate Mr. Cilluffo highlighting the great work we are doing in Alabama to help address these issues, like the cyber magnet school to address the talent shortage, and the Alabama Security Operations Center, which provides centralized cybersecurity management for Alabama's State agencies. I had the honor of visiting there about a month ago; it was pretty impressive.

In many ways, Alabama is setting the example for other States as we confront the challenges of cybersecurity.

With that, I yield back, Mr. Chairman.

[The statement of Ranking Member Rogers follows:]

STATEMENT OF RANKING MEMBER MIKE ROGERS

Thank you, Mr. Chairman.

And thank you to our witnesses for being here today. Especially Mr. Cilluffo, from Auburn's McCrary Institute for Cyber and Critical Infrastructure Security in my district.

The McCrary Institute serves as an invaluable resource to our State and the Nation with its cybersecurity and critical infrastructure work.

Cybersecurity is a tremendous challenge facing all levels of government.

Our State and local governments have seen that first-hand through increased ransomware attacks that leave citizens without services and cities in a panic.

I am glad that our hearing today will discuss how the Federal Government is already lending a helping hand and how we can improve the level of assistance.

I appreciate Mr. Cilluffo highlighting the great work we are doing in Alabama to help address these issues—like our Cyber Magnet School to address the talent shortage and the Alabama Security Operations Center, which provides centralized cybersecurity management for Alabama's State agencies.

In many ways, Alabama is setting the example for other States as we confront the challenges of cybersecurity.

Thank you Mr. Chairman. I yield back.

Mr. RICHMOND. The gentleman from Alabama yields back.

I would like to remind other Members of the subcommittee that, under the rules, opening statements may be submitted for the record.

I want to welcome our panel of witnesses here today. First, I am very pleased to welcome Mayor Keisha Lance Bottoms of the city of Atlanta, Georgia, who oversaw the city's response to a major ransomware attack in March 2018. Under Mayor Bottoms' leadership, the city took a number of bold corrective actions to manage and mitigate damage and prevent future attacks.

Thank you, Mayor, for your participation and your willingness to share the lessons you have learned in cyber incident response.

Next, we have Mr. Thomas Duffy from the Center for Internet Security, who is currently serving as the chair of the Multi-State Information Sharing Analysis Center, MS–ISAC. The MS–ISAC serves as an important partner and liaison between DHS and State and local officials when it comes to sharing information and coordinating around cyber threats. I look forward to hearing his insights on how we might tackle this problem.

Next, we also have Mr. Ahmad Sultan, who is here today in his personal capacity to discuss the research conducted while serving at UC Berkeley's Center for Long-Term Cybersecurity. His research focused on how underserved residents, including low-income residents, seniors, and foreign language speakers, face higher than average risk of becoming victims of cyber attacks and are less equipped to respond. I am sure that his comments will shed light on an important area of cybersecurity that is typically overlooked.

Last but certainly not least, I would like to welcome Mr. Frank Cilluffo, the director of the McCrary Institute for Cyber and Critical Infrastructure at Auburn University. Mr. Cilluffo previously served as a Presidential appointee in the Department of Homeland

Security, as an adviser to former director Tom Ridge. He has also testified before this committee and elsewhere on the Hill dozens of times.

Welcome back to the committee, Mr. Cilluffo, and thank you for your testimony.

Without objection, the witnesses' full statements will be inserted in the record.

I now ask each witness to summarize his or her statement for 5 minutes, beginning with you, the Honorable Keisha Lance Bottoms.

STATEMENT OF KEISHA LANCE BOTTOMS, MAYOR, CITY OF ATLANTA

Ms. BOTTOMS. Good afternoon. My name is Keisha Lance Bottoms, and I am the mayor of Atlanta, Georgia, the cradle of the civil rights movement and the 10th largest economy in the United States. Thank you to Chairman Richmond and to Chairman Thompson and to each of you for having me here today. It is an honor to join you.

In the early morning hours of March 22, 2018, 77 days into my term as mayor and only 4 days into the tenure of our new COO, Atlanta's government experienced a ransomware cyber attack which impacted our operations and our ability to provide services to our residents and our visitors.

To paint a broader picture of that day, the city of Atlanta has nearly 9,000 employees, and it goes without saying that many rely on technology to do their jobs and to keep the city running. We were incapacitated.

Fortunately, our daily mission-critical services, such as fire, police, and ambulance, were not severely impacted, and neither was our water supply. However, some departments and government entities suffered irreparable damage, including our police department which lost stored dash cam video footage. The Atlanta Municipal Court had to cancel and reschedule hearings. Our customer service interface, known as ATL311, was knocked off-line. Many other applications were impacted or affected, delaying the delivery of city services.

As the first day unfolded, it became clear to us that criminals had attacked the city's computer systems, and we moved quickly to mitigate those circumstances. The first few hours of the attack were critical for limiting damage and determining our steps going forward. We notified law enforcement and key partners, including our insurance carrier, our government partners, the media, and the public.

We also needed to learn in detail what systems, functions, and operations were impacted. That may sound simple, but during an emergency, the process of identifying every compromised system was challenging, especially without the assistance of technology.

Out of an abundance of caution, we took some systems off-line and hired an outside security firm to assist with our response. We soon discovered that attackers were demanding a ransom payment of $51,000 in bitcoins to unlock our systems. We refused to pay.

The cost of recovery, to date, has been approximately $7.2 million, and that number is still climbing. Some costs have been reimbursed under our cyber insurance policies, which, thankfully, for the first time, we had obtained just a few months before the attack.

Last November, Federal authorities charged two Iranians with the attack and outlined their massive scheme to breach computer networks of local governments, health care systems, and other public entities.

Our cyber attack was not unique. Digital extortion is now a common occurrence affecting many organizations in the public and private sectors, and cyber threats are becoming much more hostile and frequent. We must continue to understand how to protect ourselves against these attacks when they occur.

The good news is that Atlanta is rebounding from this attack and sharing its experience with other cities. But the reality is that, as elected officials, we often make investments in infrastructure that people can see. In my nearly 2-year campaign for mayor, not once did a constituent ask me about my investment in cybersecurity.

Following our unfortunate experience, we have been advising other cities to help them better understand the continuity measures that are needed. We are adopting a more flexible and hardened infrastructure using advanced technologies and the cloud to diversify and minimize our risk. We are also emphasizing the importance of cross-functional response teams, including our Federal and State government partners.

But no city can do this effectively without strong partnerships. Through our process, Atlanta has worked with the FBI, Department of Homeland Security, the Secret Service, and the private sector. The work we did to prepare for the Super Bowl earlier this year is a great example of that collaboration. We are staying proactive so that we can understand and better manage this ever-changing landscape.

We have also learned that you can never completely protect your computer network. Quite frankly, that remains our biggest challenge. Atlanta is more prepared and resilient than ever, but we continue to need strong partnerships. Many cities, especially small cities, simply lack the resources needed to develop the safety net that is needed to protect against these attacks.

The Federal Government should also expand programs that share real-time threat information, which is often critical in avoiding and mitigating threats. Also, we should have Federal programs in place to provide cybersecurity disaster relief funding that will help offset some of these costs. Last, we need your help to ensure the safety and security of the electoral process as city and State governments administer the elections that are the foundation of our democracy.

With the support and assistance of partners such as the Department of Homeland Security and this distinguished committee, all of our cities and our country can be safer and better prepared.

Thank you.

[The prepared statement of Ms. Bottoms follows:]

PREPARED STATEMENT OF KEISHA LANCE BOTTOMS

JUNE 25, 2019

Good afternoon. My name is Keisha Lance Bottoms and I am the mayor of Atlanta, Georgia, the cradle of the Civil Rights Movement and the anchor of the 10th-largest economy in the United States.

I want to thank Chairman Bennie Thompson and Subcommittee Chairman Cedric Richmond for inviting me today to testify at this important hearing. I am honored to be here.

In the early morning hours of Thursday, March 22, 2018—77 days after I was sworn in as the 60th Mayor of Atlanta—the city experienced a ransomware cyber attack which impacted our operations and our ability to provide services to our residents and visitors.

Fortunately, mission-critical services such as fire, police, and ambulance services, and our water supply, were not affected.

However, some departments and governmental entities suffered irreparable damage.

The Atlanta Municipal Court had to cancel and reschedule hearings, suffering a major interruption. ATL311, our customer service interface for our residents, was knocked off-line.

Many other applications were impacted or affected, delaying the provision of services by the city.

As that first day unfolded and the city learned more details about the disruption, it became clear to us that criminals had attacked the city's systems.

As this committee knows, one of the most common and successful ways that criminals can attack entities is through phishing. Phishing scams use social engineering to trick a user into clicking on a link which can then infect the system with malware. Depending on the malware used, it can take over and encrypt the user's computer. Ransomware can also delete or permanently corrupt files and destroy them forever, something we experienced in Atlanta.

The city of Atlanta moved quickly to address the impacts and to mitigate the attack, notifying law enforcement and key partners, including our insurance carrier, outside counsel, Government partners, and the media. We also hired an outside cybersecurity firm to assist with our response.

While like other crimes, in the case of a cybersecurity attacks, it can take days and even months to fully understand the depth and breadth of what may have been impacted.

The city assessed which systems, functions, and operations were impacted. That might sound simple, but during an emergency, identifying every compromised system was difficult to accomplish, especially without the assistance of technology.

Although the overall impact was not substantial throughout our infrastructure, we took some systems off-line out of an abundance of caution.

The city soon learned that the attackers were demanding a ransom payment of $51,000 in Bitcoin to unlock our systems, which we refused to pay.

The cost of recovery to date has been about $7.2 million and we expect it will go higher.

Some costs have been reimbursed under Atlanta's cyber insurance policies, with the hope that more will be reimbursed.

However, cyber insurance policies vary greatly, and not all policies cover the wide-ranging impacts that a cyber attack can do to a company or a city. It is critical to seek expert advice and counsel to ensure that the policies purchased can cover the damages that can be sustained.

As this committee knows, in November 2018, the U.S. Department of Justice charged two Iranians with the attack and outlined the wide-ranging plan they crafted to attack countless local governments, health care systems, and other public entities.

Unfortunately, the city of Atlanta's cyber attack was not an isolated occurrence. As organizations integrate technology into every aspect of our lives, cybersecurity risk is ever present. If not secured, systems across public and private entities will continually be subject to attack and digital extortion.

Cities such as Savannah, Georgia; Dallas, Texas; and Baltimore, Maryland have been attacked. The attack in Baltimore affected its 9–1–1 system, which further underscores how these attacks threaten the actual health and safety for each of us.

Cyber threats are becoming more hostile and frequent, so all organizations must understand how to protect themselves against these attacks when they do occur.

The good news is that the city of Atlanta is using its experience to become a "model city" for how municipalities can protect against, and prepare for, cyber attacks.

We are adopting a more flexible and hardened infrastructure by utilizing advanced technologies in order to diversify and minimize risk.

We are emphasizing the importance of cross-functional incident response teams that include Federal and State government partners.

We are strengthening our human capital to make certain that the best and the brightest are guarding our systems.

We are in a good place going forward. Atlanta and the State of Georgia represent one of the Nation's elite cybersecurity hubs, ranking third in the Nation with companies that focus on information security, and generating more than $4.7 billion in annual revenue.

More than 115 cybersecurity firms call Georgia home, including Cybersecurity 500-ranked Secureworks, Pindrop, NexDefense, and Ionic Security.

Based on the city's "lessons learned" we can now help other cities to take cybersecurity seriously and plan to put in place manual processes for mission-critical applications and services to specifically address cyber risks.

This includes ensuring cities have carried out a thorough risk assessment of their systems, including both infrastructure and business practices.

No city can do this effectively without partnerships. The city of Atlanta has worked with the FBI, the Department of Homeland Security, the Secret Service, and the private sector. The work done to prepare for Super Bowl LIII (53) was a great example of these collaborative efforts.

The priority at the city of Atlanta is to build a culture of cybersecurity where all our technology experts and partners are around the table.

We intend to stay pro-active in order to understand and manage the ever-evolving landscape.

We are re-focusing on operational basics—Detection, Response, and Recovery.

On detection, we need to be able to quickly identify anomalies and potential issues; on response, once a problem is identified, we need to rapidly seek to contain the risk; and on recovery, we will better understand the impacts of an attack and have cyber-specific recovery and business-continuity plans in place ready to be deployed immediately.

One component of a "down to the basics" plan is to have an on-going program to educate employees and help them identify a phishing email; as well as require the use of strong passwords, and prioritize funding and empower cyber leadership, as we have done in Atlanta.

Regardless of the protective measures that are employed, cybersecurity risks are now part of our everyday lives. We've learned that you can never completely protect a computer network.

But there are steps that can be taken.

For example, cities should establish clear processes and be ready to implement their cyber incident-response plan, just as they do in anticipation of other emergencies.

While the city of Atlanta is more prepared and more resilient, many local and State governments are not, and need the help of the Federal Government.

Specifically, the Federal Government can help by passing legislation and providing funding to assist State and local governments in preventing, preparing for, and responding to cyber threats and incidents. It is also important to emphasize the need for the Federal Government to provide emergency funding and support during an actual cyber attack. Having access to funds at the time of an attack would not only accelerate responsiveness and restoration; but, would also result in fewer municipalities paying ransoms and ultimately decrease the occurrence of local governments as targets.

Second, the Federal Government can assist by empowering its agencies to develop and share best practices with State and local governments. Many small municipalities do not have the resources necessary to development and implement these best practices.

Third, the Federal Government should expand its programs that share real-time threat information with State and local governments as this information is often critical in avoiding or mitigating threats.

Next, when an attack does occur, the Federal Government should have programs in place to provide cybersecurity disaster relief funding to help offset recovery and restoration costs borne by State and local governments.

Last, many State and local governments administer elections and need help in ensuring the safety and security of the electoral process.

We are living in a different digital world now. Nation-state actors and other foreign adversaries are attacking our State and local governments and we need a strong Federal partner to defend against those threats.

We know the threats will continue. What we're planning for today may look different tomorrow.

With the support and assistance of partners such as the U.S. Department of Homeland Security and this distinguished committee, all our cities, and our country, can be safer by being prepared.

Thank you.

Mr. RICHMOND. Thank you, Mayor Bottoms, for your testimony.

I now want to recognize Mr. Duffy to summarize his statement for 5 minutes.

STATEMENT OF THOMAS DUFFY, CHAIR, MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS–ISAC), SENIOR VICE PRESIDENT OF OPERATIONS, CENTER FOR INTERNET SECURITY

Mr. DUFFY. Thank you.

Chairman Thompson, Chairman Richmond, and Ranking Member Katko, and Members of the subcommittee, thank you for inviting me here today. My name is Thomas Duffy, and I am the chair of the Multi-City Information Sharing and Analysis Center, or MS–ISAC, which is operated by the Center for Internet Security.

We have a cooperative agreement with the Department of Homeland Security to work with State, local, Tribal, and territorial governments across the country. We serve as a focal point for cyber prevention, protection, response, and recovery of the Nation's State, local, Tribal, and territorial governments.

I have spent my career in service to State and local governments, including the past 15 years with the MS–ISAC. Today, I will discuss the current level of cyber maturity in State and local governments, the major security concerns, and the recommendations on how the Federal Government can help.

Membership in the MS–ISAC and the more recently created Elections Infrastructure ISAC has tripled in the past year-and-a-half, which is a clear indication that the State and local governments have a growing need for assistance, guidance, and support. We conduct an annual cybersecurity maturity assessment called the Nation-wide Cybersecurity Review, which measures the gaps and capabilities of cyber programs of the State and local governments.

So what have we learned from these annual reviews? We have learned that the States continue to report higher overall maturity scores than the local counterparts. Not surprising. While improvements have been noted, there is still much to be done at all levels of government.

We have also learned that the same top 5 security concerns dominate this discussion year after year. No. 1 concern in 2018 was lack of sufficient funding; No. 2 was the increasing sophistication of threats; No. 3 was the lack of documented processes; No. 4 was emerging technologies; and No. 5, as mentioned earlier, is the inadequate supply of cybersecurity professionals.

Addressing these challenges requires resources as well as State and National strategies. We need to increase a pool of cybersecurity professionals, plan for investments in our IT infrastructure, and secure that security is built into the products and services.

So what can the Federal Government do to assist? First, let me note that DHS has been very supportive and proactive in addressing the increasing cyber challenges faced by State and local governments, especially in the election sector. There are two areas I would recommend for cyber support, one that requires funding, which you are used to, and one that only requires some interagency cooperation, which would be nice to see.

First, the Federal Government should consider establishing a dedicated State and local cybersecurity grant program. When the initial Homeland Security grants were created, cybersecurity threat is not what it is today. Most of the funds were dedicated to antiterrorism activities, which was appropriate. Over time, the grant funds have decreased while the cyber threat has expanded exponentially, and the terrorism threat still exists. Thus, there is a smaller pool of funding for a much larger pool of threats. More money is going to sustain activities, leaving less money for new initiatives.

I would suggest if a cyber grant program is established, priority be given or funds set aside to programs that support State and local partnerships. Leveraging the combined resources of State and local partnerships will serve as a force multiplier. Really, you get the value out of the funds.

Second, the Federal Government should adopt a single audit approach when auditing State programs for compliance with security guidelines with the cognizant Federal agencies. In 1984, the Single Audit Act was passed, which proved to be a cost-effective method to audit non-Federal entities. Once one audit is conducted in lieu of multiple audits of individual programs, then the single audit standard is applied. The same should apply to cybersecurity audits of State programs by Federal agencies. This would save resources, both at the State level and the Federal level, resources that could be reinvested to improving our cybersecurity posture.

While State and local governments have made progress in key areas, so have our adversaries. The dizzying array of cybersecurity requirements has made it difficult to develop effective programs, a lack of funding stalls progress, and a lack of capable talent compounds the negative impacts of ransomware and other attacks. We must do better.

In closing, our success or failure will be determined on our ability to work together at all levels of government to evade, counter, or neutralize the endless risk that State and local governments face. Each of these efforts requires resources—time, money, and energy—that are currently in short supply. If we are to make the progress required of us in meeting our collective missions, we must work together on this National problem.

I thank you for the opportunity to address the subcommittee today.

[The prepared statement of Mr. Duffy follows:]

PREPARED STATEMENT OF THOMAS DUFFY

JUNE 25, 2019

Chairman Thompson, Chair Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for inviting me today to this hearing. My name is Thomas Duffy and I serve as the senior vice president of operations and security services at the Center for Internet Security, a global nonprofit focused on improving cybersecurity for public and private organizations. I also serve as the chair of the Multi-State Information Sharing and Analysis Center (MS–ISAC), which is the focal point for cyber threat prevention, protection, response, and recovery for the Nation's State, local, Tribal, and territorial governments as well as all 79 Fusion Centers.

I have spent my career in service to State and local governments, including the past 15 years with the MS–ISAC. I appreciate the opportunity today to share our thoughts on the current state of cybersecurity in State and local governments, focusing on how the Federal Government can help. I look forward to offering ideas on how we can collectively build on the progress being made to secure the State and local government cyber infrastructure.

In short, I will: (1) Introduce you to the current level of cyber maturity in and local governments (2) the major challenges faced by and local governments and (3) recommendations on how the Federal Government can help.

ABOUT CENTER FOR INTERNET SECURITY AND THE MS–ISAC

The Center for Internet Security's (CIS') was established in 2000 as a nonprofit organization and its primary vision is to lead the global community to secure our connected world through the identification, development, validation, information sharing, and sustainment of best practice solutions for cyber defense. CIS was instrumental in establishing the first guidelines for security hardening of commercial IT systems at a time when there was little security standards, best practices, or leadership.

The MS–ISAC was formed in 2004 under the auspices of the State of New York, and transitioned to CIS in 2010. The Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC) was formed in 2018, in response to the need to have a dedicated focus on protecting our Nation's election infrastructure.

Today, CIS works with the global security community using collaborative deliberation processes to define security best practices for use by Government and private-sector entities. The approximately 200 professionals at CIS provide cyber expertise in three main program areas: (1) The Multi-State and more recently the Elections Infrastructure Information Sharing and Analysis Center, the MS–ISAC and EI–ISAC respectively; (2) the CIS Benchmarks; and (3) the CIS Critical Security Controls. I describe each briefly below.

MS–ISAC.—[1]In 2010, the U.S. Department of Homeland Security (DHS), under the then-National Protection and Programs Directorate (NPPD), partnered with CIS to host the MS–ISAC, which has been designated by DHS as the focal point for cyber threat prevention, protection, response, and recovery for the Nation's State, local, Tribal, and territorial governments as well as all 79 Fusion Centers Nationwide. MS–ISAC members include all 56 States and territories and more than 5,000 other State and local government entities. MS–ISAC's 24x7 cybersecurity operations center provides: (1) Cyber threat intelligence that enables MS–ISAC members to gain situational awareness and prevent incidents, consolidating and sharing threat intelligence information with the DHS National Cybersecurity and Communications Information Center (NCCIC); (2) early warning notifications containing specific incident and malware information that might affect them or their employees; (3) IP and domain monitoring (4) incident response support; and (5) various educational programs and other services. Furthermore, MS–ISAC provides around-the-clock network monitoring services with our so-called "Albert" network monitoring sensors for many State and local government networks, analyzing over 1 trillion event logs per month. Albert is a cost-effective Intrusion Detection System (IDS) that uses open-source software combined with the expertise of the MS–ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity. In 2018, MS–ISAC analyzed, assessed, and reported on over 56,000 instances of malicious activity to over 6,000 MS–ISAC members.

[1] Find out more information about the MS–ISAC here: *https://msisac.cisecurity.org/*. List of MS–ISAC services here: *https://www.cisecurity.org/wp-content/uploads/2018/02/MS-ISAC-Services-Guide-eBook-2018-5-Jan.pdf*.

EI–ISAC.[2].—In 2018 CIS was tasked by DHS to stand up an information sharing and analysis center focused on the Nation's elections infrastructure. Leveraging the resources of the MS–ISAC, CIS established the Elections Infrastructure Information Sharing and Analysis Center (EI–ISAC). The EI–ISAC is now fully operational with all 50 States participating and over 1,700 total members, including elections vendors. The EI–ISAC provides elections officials and their technical teams with regular updates on cyber threats, cyber event analysis, and cyber education materials. During the 2018 primaries and mid-term elections the EI–ISAC hosted the National Cyber Situational Awareness Room, an on-line collaboration forum to keep elections officials aware of cyber and non-cyber incidents and potential cyber threats. More than 600 elections officials participated in these forums. Moreover, the MS–ISAC was processing data from 135 Albert sensors monitoring the networks, which supported on-line elections functions such as voter registration and election night reporting. The Albert sensors processed 10 petabytes of data during 2018, resulting in over 3,000 actionable notifications to elections offices.

CIS 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-detailed security setting recommendations for a large number of commercial IT products, such as operating systems, database management systems, virtual private cloud environments, and for most of the major vendors network appliances. These benchmarks are vital for any credible security program. The CIS Security Benchmarks are developed though a collaborative effort of public and private-sector security experts. Over 200 consensus-based Security Benchmarks have been developed and are available in PDF format free to the general public on the CIS or NIST web site. An automated benchmark format along with associated tools is also available through the purchase of a membership. CIS has also created a number of security configured cloud environments, called "hardened images" that are based on the benchmarks that we are deploying in the Amazon, Google, and Microsoft cloud environments. These hardened images help ensure that cloud users can have confidence in the security provided within the cloud environment they select. The CIS-hardened images 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:

- 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
- Payment Card Industry (PCI) Data Security Standard v3.1 (PCI) (April 2016)
- CIS Critical Security Controls.

CIS Controls.—[3]In 2015, CIS became the home of the CIS Critical Security Controls, previously known as the SANS Top 20, the set of internationally-recognized, prioritized actions that form the foundation of basic cyber hygiene and essential cyber defense ground truth. They are developed by an international consensus process and are available free on the CIS web site. The Critical Security Controls or just the CIS Controls have been assessed as preventing up to 90 percent of pervasive and high risks cyber attacks.[4] The CIS Controls act as a blueprint for system and network operators to improve cyber defense by identifying specific actions to be done in a priority order—achieving the goals set out by the NIST Cybersecurity Framework (CSF). Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[5]

The MS–ISAC, and more recently the EI–ISAC, are operated pursuant to a Cooperative Agreement with Department of Homeland Security. Members include all 50 States, all 50 State election directors, almost 6,000 local governments, 88 Tribal governments, all 5 U.S. territories and the District of Columbia. Local government members represent over 80 percent of the U.S. population.

[2] A list of EI–ISAC services can be found here: *https://www.cisecurity.org/ei-isac/ei-isac-services/*.

[3] Find out more information about the CIS Controls and download them for free here: *https://www.cisecurity.org/critical-controls.cfm*.

[4] Up to 91 percent of all security breaches can be auto-detected when release, change, and configuration management controls are implemented. IT Process Institute: *https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1533052750.pdf*.

[5] NIST Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC"—Council on Cyber Security (the predecessor organization to CIS for managing the Controls) Critical Security Controls).

CYBERSECURITY CHALLENGES FACED BY STATE AND LOCAL GOVERNMENTS

Cyber protections at all levels of government are critical, and central to the fiduciary responsibility to protect the data that is entrusted to Government by our citizens and businesses. Local governments connect to State governments, State governments connect to the Federal Government. All levels of government have a shared responsibility for safeguarding information. Data on citizens is tracked from cradle to grave, from the issuance of your birth certificate, to the filing your death certificate.

Regarding the question "has the cybersecurity posture of and local governments improved?"—the answer is yes. There are, however, other related and equally important questions that should be asked. If the question is "have and local governments kept pace with advancing threats and the rapidly expanding cyber infrastructures that need to be protected?", the answer is probably not. If the question is "are State and local governments prepared to build, maintain, and evolve their cybersecurity programs commensurate with the risks that they will face in the future?", the answer is again, probably not. Both State and local governments continue to make news for ransomware, cyber crime, and other cybersecurity-related issues every week.

The cyber threat landscape continues to evolve faster than our preparedness activities and protective measures, and the number of entry points to our systems continues to grow at an accelerated rate. We are constantly playing a game of catch up. There is no silver bullet to solve the problem. Software providers continue to issue patches for system vulnerabilities daily! Keeping up with this is an enormous challenge for all organizations, large and small.

The MS–ISAC conducts an annual cybersecurity maturity assessment, called the Nation-wide Cybersecurity Review (NCSR), of State and local governments. The NCSR, based on the NIST Cybersecurity Framework, is a self-assessment tool developed by CIS in concert with State and local cybersecurity professionals.

What have we learned from the annual NCSR over the past few years?

The assessment uses a scale of 1–7 to measure cybersecurity maturity, and establishes a score of 5 as the minimum-security level organizations should strive for. The State average in 2018, was 4.7, with 44 percent States achieving the baseline of 5. The local government average is 3.4, with only 18 percent achieving the baseline minimum of 5. There have been improvements over time, with the States improving by 5 percent over the past 3 years and local governments improving by 17 percent. States on average report higher maturity scores than local governments. While improvements have been noted, there is much that still needs to be done, especially at the local government level.

One constant finding of the NCSR has been the top 5 security concerns, which remain unchanged for the past 5 years, the only difference being that the order of priority has changed every year. The top 5 concerns in 2018 were:

1. Lack of sufficient funding.—State and local governments struggle with balancing operational needs to improve their IT infrastructure and providing adequate cyber defense simultaneously. Threat actors continually attacking State and local governments with ransomware and breaching their legacy defense mechanisms to steal private data, causing an increase need to provide incident response, improve IT network defense, and reprioritize budgets to implement security best practices and security controls that often require major operating system and proprietary software migrations. The cybersecurity budget must to compete with other programs, such as education, infrastructure like roads and bridges, health care and law enforcement, for funding. The value of security investments is not obvious to public. Public officials don't run on a platform of "I am going to upgrade our IT infrastructure!". It is only after it is too late, that they realize a missed opportunity to prevent a major compromise, that requires a major investment in cybersecurity.

2. Increasing sophistication of threats.—It is no secret that threat actors, threat groups, and/or advanced persisted threats funded by nation states to carry out cyber espionage are increasing. Sophisticated malware like Emotet, which "reinvents" itself weekly to avoid detection by traditional defenses, is a good example of the bad guys making cyber defense a 24x7x365 job. In addition, threat actors are using realistic and effective spear phishing and phishing campaigns to gain access to State and local government systems and end-users' workstations and mobile devices.

3. Lack of documented processes.—Mature organizations have formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness. This not found in most State and local governments. Many processes in managing government systems remain ad hoc. This is well-documented in the NCSR. The priorities are to "keep the lights on", respond to emergencies, managing new projects, roll out new technologies, etc. One of the enhancements planned for 2019 in the NCSR is to included links to policies and standards where this is identified as a need in the NCSR submission. However, resources will be required to implement the policies and standards and ensure they are tested, verified, and reviewed regularly.

14. Emerging technologies.—The future is now. Major urban areas are in the progress of building 5G communications infrastructures to support the rapidly growing need for connectivity to support autonomous vehicles, data streaming services, consumer electronics, and smart devices. IoT devices are now finding their way into daily government operations. HVAC systems are now connected to the internet as are medical devices. Drone technology is being deployed across all levels of government. Each of these technologies require organizations to expand the scope of protective measures that need to be implemented, tested, and verified regularly. They also introduce new opportunities for attackers to exploit networks looking for vulnerabilities or lapses in security. Status quo will not protect your network. The defenses need to continually evolve. We must proactively put in place security measures that effectively defend against current and future cyber threat attacks.

5. Inadequate supply of security professionals.—The NCSR clearly highlights what is a National problem—the shortage of skilled cybersecurity professionals. This impact of this lack of talent is even more impactful for State and local governments entities due to lower pay. State and local governments are at a major disadvantage in recruiting cybersecurity professionals. Vacant positions mean some critical work may not be accomplished.

Each year, the DHS issues a National Preparedness Report on the challenges that all organizations, public and private, face in preparedness. It includes a capabilities assessment in 32 core areas reported by every State. The 2018 report noted:

1. Cyber threats are a rapidly-evolving threat, joining nation-state threats and terrorism as an area of significant public concern.
2. Since 2012, States and territories have consistently reported cybersecurity as their least proficient capability.

Just this past weekend CISA reported on "a recent rise in cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies." Improving our cybersecurity posture will take time. We must act now.

RECOMMENDED ACTIONS FOR THE FEDERAL GOVERNMENT

Addressing these challenges requires resources as well as State and National strategies. We need to: Increase the pool of cybersecurity professionals, plan for investments in our IT infrastructure, and ensure that security is built into products and services.

What can the Federal Government do to assist State and local governments?

DHS has been very supportive in addressing the increasing challenges of State and local governments posed by expanding cyber threats, including funding of the Multi-State ISAC and Election Infrastructure ISAC, allowing State and local governments to participate in the Federal Virtual Training Environment (FedVTE), allowing State and local governments to participate the Scholarship for Service Program sponsored by the National Science Foundation. It has also developed the National Cybersecurity and Technical Services program that provides network scanning and penetration testing among its many service offerings. It has been very active in improving the security of our Nation's election infrastructure and developing and sponsoring local, State, and National cyber exercises. A National-level election exercise sponsored by DHS last week.

There are two areas that I would recommend consideration be given to additional Federal cyber support to the State and local community.

First, DHS should establish a dedicated State and local government cybersecurity grant program. When the initial Homeland Security Grant programs were created, the cybersecurity threat was not what it is today. Most of the funds were dedicated to anti-terrorism efforts, as was appropriate. Over time the grant funds have decreased, while cyber threat has expanded exponentially and the terrorism threat still exists. Thus, a smaller pool of funding is available for a large pool of threats. More money is going to sustain activities, leaving less money for new initiatives. If a cyber grant program is established, priority should be given, or funds set aside, to programs that support State and local partnerships. Leveraging the combined resources of State and local governments will serve as force multiplier. There are several great examples of State and local partnerships including the Wisconsin Cyber

Response Team that was organized by the State to recruit local government staff to be regional cyber incident responders for local governments. Local government staff that met minimum qualifications were chosen to be part of the regional teams and received advance training by the State, that led to led to incident response certifications. The regional teams have responded to over 30 incidents since its inception.

Second, the Federal Government should adopt a "single audit" approach when auditing State programs for compliance with the security guidelines of the cognizant Federal agencies. In 1984, the Single Audit Act was passed. The Act refers to a "single audit" because it consolidated multiple audits of non-Federal agencies required for each award into a single audit. The stated purpose was to promote sound financial management of Government funds by non-Federal organizations, promote uniform guidelines for audits, and reduce the burden on nonprofits by promoting efficient and effective use of audit resources. It proved to be a cost-effective method audit of non-Federal entities. One audit is conducted in lieu of multiple audits of individual programs and single audit standard is applied. The same should apply to the security audits of State programs by Federal agencies.

The following are some of the Federal agencies that audit State systems: Centers for Medicare & Medicaid Services, Internal Revenue Service, Social Security Administration, Department of Agriculture, and Department of Health and Human Services. Although the compliance/audit requirements are often based on NIST SP 800–53, they vary in the amount of time required by the State to meet the requirements. For example, some Federal agencies send an on-site audit team to the State to review security controls while other Federal agencies rely on the completion of a written questionnaire. Regardless, there are multiple audits being conducted that duplicate each other, and place a drain on scarce State resources dedicated to protecting State systems. Let these resources be freed up to develop and implement new cyber protective measures. The "single audit" concept would create savings for both the Federal and State governments, savings that could be re-invested to enhance their cybersecurity posture.

CLOSING

Defending our Nation from rapidly-advancing cyber threats has become a critical, yet incredibly difficult task. The overwhelming vulnerability inherent in the "internet of everything" caught us off guard, forcing most organizations into reactive mode, and the asymmetry of cyber warfare ensures that the good guys are always at a disadvantage. All this while we increasingly rely on a safe, secure, and trustworthy internet to do everything from ordering groceries to ordering drone strikes.

And while State and local governments have made progress in key areas, so have our adversaries. The dizzying array of cybersecurity requirements has made it difficult to develop effective programs, a lack of funding stalls progress and a lack of capable talent compounds the negative impacts of ransomware and other attacks. We must do better.

Our success or failure will be determined by our ability to have all levels of government work together to evade, counter, or neutralize the endless risks that State and local governments state face. Each of these efforts require resources—time, money, and energy—that are currently in short supply. If we are to make the progress required of us in meeting our collective missions, we must work together.

Mr. RICHMOND. Thank you, Mr. Duffy, for your testimony.

I now recognize Mr. Sultan to summarize his statement in 5 minutes. Thank you.

STATEMENT OF AHMAD SULTAN, AFFILIATED RESEARCHER, CENTER FOR LONG-TERM CYBERSECURITY, SCHOOL OF INFORMATION, UNIVERSITY OF CALIFORNIA, BERKELEY

Mr. SULTAN. Chairman Thompson, Ranking Member Rogers, Chairman Richmond, Ranking Member Katko, and Members of the subcommittee, thank you for inviting me to testify on the topic of cybersecurity challenges for State and local governments. My name is Ahmad Sultan, and I am testifying in my personal capacity as the author of a white paper published by the Center for Long-Term Cybersecurity and which was facilitated by the city and county of San Francisco.

The findings of my research detailed in my written testimony are alarming, but they are not surprising. Underserved respondents in San Francisco defined as low-income earners, seniors, or immigrants have poor cybersecurity outcomes. Poor outcomes is a researcher's way of saying that their devices have been infected with viruses and malware, hacked, or phished for money. They don't follow best practices for preventative care and they don't have enough knowledge about curative care.

So for today's hearing, I will focus on ways in which we reconcile the macro with the micro, reconciling Government's attempts to enhance National security with a play of individuals and their struggle to use digital devices to improve social mobility. Stated simply, while organizations and Government invest millions of dollars to defend themselves from cyber attacks, a critical part of society is falling through the cybersecurity cracks, underserved and vulnerable populations.

This comes at a time when an increasing number of our daily activities are governed by internet services. Low levels of cyber hygiene, which refers to best practices that improve on-line security, pose serious challenges to the well-being of underserved populations.

Fear of cyber threats creates a distinct on-line experience filled with fear, low confidence, and distrust. It prevents underserved users from taking advantage of economic opportunities on the internet. These include job search services, listing platforms, social networking, and email. These services are crucial to remaining competitive in today's job market.

Like a mirror to the physical world, low levels of cyber hygiene and knowledge are associated with low-income household and low-educational attainment. Most figures on poor cybersecurity outcomes are also underreported. In fact, most underserved respondents I surveyed and spoke to didn't even know about basic concepts: Spam, viruses, or on-line scams. Internet evangelists had promised a digital reality that would even the playing field across demographics.

But today, we are replicating the same gender and race-based patterns of inequality on-line that the existing social structures around us enforce off-line. This inequality in outcomes is a form of market failure that governments need to correct.

The reason cybersecurity experts adapt concept from public health literature like cyber hygiene is because of the unique interconnectedness of networks and society. Poor cybersecurity practices can cause viruses and malware to spread. This, in turn, can impact people, businesses, and infrastructure. It deepens inequalities for those already most vulnerable to existing economic and social forces but also reduces trust in on-line services for all.

Take, for example, the concept of zombie botnets. Hackers can control hundreds of thousands of devices without the device owner's knowledge or consent. They can program them to attack specific targets, including businesses and infrastructure. Even local government staffs suffer from porous practices. The increasing frequency of ransomware attacks on local government systems is a testament to that fact, and these attacks are bound to increase as more city services are digitized.

The risk of ignoring cyber preparedness is too high. 5G networks and AI systems promise smart cities. Important municipal services will be powered by strong mobile connections and trained machine learning systems. We need to pursue a holistic approach where cybersecurity concerns are addressed at a societal level, much like public health issues.

While the underprivileged in society are disproportionately affected and most likely to be targeted by attackers and scammers, awareness of cybersecurity threats and best practices needs to seep into public discourse. Digital literacy is not enough; it needs to be paired with cybersecurity awareness.

This is not just a State and local government problem. Cyber vulnerabilities are not bound by geographical boundaries. It is incumbent upon Federal, State, and local governments to collaborate to solve the problem.

But State and local governments face many constraints of increasing awareness. These include fiscal and budgetary challenges, lack of social and technical expertise, low organizational capacity, and geographically-bound networks.

Promoting cyber hygiene through trainings, public service initiatives, and public-private partnerships can lead to significant gains in the life of underserved populations, while protecting businesses and Government systems from cyber threats. But to achieve these gains, State and local governments will require financial support and guidance from the Federal Government. It is my hope that policy makers recognize the challenges ahead and rise to the occasion.

Thank you again, Chairman Richmond and Representative Katko. I am happy to answer any of your questions.

[The prepared statement of Mr. Sultan follows:]

Prepared Statement of Ahmad Sultan

June 25, 2019

Chairman Richmond, Ranking Member Katko, and Members of the subcommittee. Thank you for inviting me here today to testify on the topic of cybersecurity challenges for State and local governments.

My name is Ahmad Sultan and I am testifying in my personal capacity as the author of a white paper published by the Center for Long-Term Cybersecurity. This paper was adapted from my Master's thesis at UC Berkeley's Goldman School of Public Policy, titled "Cybersecurity Awareness for the Underserved Population of San Francisco". The research was funded by the Center for Long-Term Cybersecurity, and it was commissioned by the city and county of San Francisco's Committee on Information Technology. The scope of my testimony is based on my expertise in cybersecurity before joining ADL. Any views presented here are not on behalf of or necessarily reflective of ADL positions or beliefs.

The topic of today's hearing should be of interest to Government policy makers, researchers, and to individual targets of cyber attacks. Thanks to the rise of mobile devices, the "digital divide" which is the gap between those who have access to on-line services and those who do not—has been shrinking, yet there exists a stark contrast in the on-line experience of low-income and high-income individuals.[1] As the adoption of digital services becomes more wide-spread, a new divide has emerged between those who can manage and mitigate potential cybersecurity threats and those who cannot.

[1] Digital gap between rural and nonrural America persists. (n.d.). Retrieved from *https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/*.

While the increasing frequency of cyber attacks, which caused catastrophic data breaches[2] have led to organizations and governments investing billions of dollars to defend themselves, a critical part of society is falling through the cybersecurity cracks: Underserved populations, defined as low-income earners, seniors, or immigrants.

This comes at a time when an increasing number of Americans' daily activities are facilitated and governed by internet services. Low levels of cyber-hygiene, which refers to the best practices and steps that internet users take to maintain system health and improve on-line security, pose serious challenges to the economic, social, and emotional well-being of underserved populations, weaken the security of systems in businesses and government, and pose existential threats to the democratic values of liberty, equality, and justice for all.

The findings of my own research into the topic of cybersecurity awareness, detailed later in this testimony, are alarming but not surprising. Underserved respondents in San Francisco have poor cybersecurity outcomes and do not follow best practices. A large number of respondents do not know about the existence of common threats like viruses and on-line scams.

Yet, the interconnected nature of on-line networks means that poor cybersecurity outcomes for underserved populations can affect countless others. It not only deepens inequalities for those already most vulnerable to existing economic and social forces, but reduces trust in on-line services for all. With 5G networks and Artificial Intelligence systems promising smarter cities where key Government services are powered by strong mobile connections and trained machine learning algorithms, the risk of ignoring poor cybersecurity outcomes are at an all-time high.[3] It is imperative that we work diligently toward raising awareness and educating underserved populations about cybersecurity.

Solutions exist but they require close coordination between Federal, State, and local governments.

WHY SHOULD GOVERNMENT CARE?

A large number of Americans from low-income households have low digital literacy and cybersecurity skills, and many do not own internet-connected devices or have broadband internet at home. While internet adoption has been sporadic over the last few years,[4] improved internet access in cities across the country means millions of Americans are expected to become active internet users, many of whom will have little knowledge on cybersecurity. Even as connectivity increases, the cybersecurity divide threatens to exacerbate existing inequalities.

According to recent estimates by Pew,[5] roughly 3-in-10 American adults with household incomes below $30,000 a year (29 percent) do not own a smartphone. More than 4-in-10 do not have home broadband services (44 percent) or a traditional computer (46 percent). And a majority of lower-income Americans are not tablet owners. By comparison, each of these technologies is nearly ubiquitous among adults in households earning $100,000 or more a year, coupled with higher levels of educational attainment and cybersecurity outcomes.

The lack of cybersecurity preparedness for large swathes of underserved populations is concerning for a variety of reasons. These include:

- *Cybersecurity inequality*.—Underserved populations who tend to be the most vulnerable to real-world social and economic forces are also the most vulnerable to cyber threats like scams, viruses, harassment, and disinformation. Like a mirror to the physical world, low levels of cyber hygiene and cybersecurity knowledge are associated with low-income households and low education attainment. Most figures on poor cyber outcomes are also underreported. This is because many underserved users are unaware of cyber threats and do not know if their devices have been hacked or if they have been victim to a cyber scam. This inequality in cybersecurity outcomes is a form of market failure that gov-

[2] Includes the 2015 Office of Personnel Management breach in which an estimated 21.5 million records of personally identifiable information were stolen, and the 2014 Sony Pictures Hack, which included 47,000 unique Social Security numbers.

[3] Toward AI Security: Global Aspirations for a More Resilient Future—CLTC UC Berkeley Center for Long-Term Cybersecurity. (n.d.). Retrieved from *https://cltc.berkeley.edu/towardaisecurity/*.

[4] Demographics of Internet and Home Broadband Usage in the United States. (2019, June 12). Retrieved from *https://www.pewinternet.org/fact-sheet/internet-broadband/*.

[5] Digital divide persists even as lower-income Americans make gains in tech adoption. (n.d.). Retrieved from *https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/*.

ernments need to correct through trainings and strategic public-private partnerships.

- *Digital Inequality*.—Internet users exist on a cybersecurity spectrum that includes users who can defend against cyber threats and those who cannot. Low levels of cyber hygiene create a distinct on-line experience filled with fear, low confidence, and distrust that I have seen lead to a complete withdrawal from internet use. Without addressing the underlying causes for the distinct differences in the on-line experience, underserved populations are being denied a wide range of opportunities and conveniences.
- *Diminished Economic Opportunities*.—Fearing cyber threats, large numbers of underserved users are not taking advantage of economic opportunities on the internet. These include job search services like LinkedIn, listing platforms like Craigslist, social networking, email, or on-line banking. All these services are crucial to remaining competitive in today's job market. They are also excluded from obtaining lower prices through on-line shopping, on-line health services, and digital financial inclusion services.
- *First Amendment Protections*.—The internet, and social media platforms in particular, are viewed as the new public squares. Cyber threats can be used to silence speech, create fear, and disrupt key Democratic processes.

Yet, poor cybersecurity outcomes are not exclusive to underserved populations as the lack of awareness of best practices and capacity for negligence exists at all levels of society. A holistic approach is required where cybersecurity outcomes are addressed at a societal level, much like public health issues. This is because poor cybersecurity practices can cause viruses, scams, and data breaches to spread and impact countless people, devices, infrastructure and entire organizations in unpredictable ways. The increasing frequency of attacks on local government systems are a product of poor cyber hygiene, even in populations that have higher digital literacy. In just the last 3 years, the State and local governments of Colorado, Baltimore, Atlanta, San Francisco, Jackson County, Riviera Beach, Imperial County, Sammamish have had to deal with ransomware attacks.[6] [7]

The reason cybersecurity researchers and experts adapt lessons and concepts, like cyber hygiene, from public health literature is because of the unique interconnectedness of society and networks. Human error is the weakest link in both fields and has the potential to inadvertently cause unimaginable damage. While the underprivileged in society are disproportionately affected and most likely to be targeted by attackers and scammers, awareness of cybersecurity threats and best practices needs to seep into public discourse at a societal level. Digital literacy is not enough, it needs to be paired with cybersecurity awareness.

This is not just a State and local government problem. Cyber vulnerabilities exist across the country, and cyber attacks can flow seamlessly between State and city lines. It is incumbent upon Federal, State, and local governments to provide programs and engage in strategic partnerships that aim to improve cybersecurity outcomes.

HOW CAN THE FEDERAL GOVERNMENT HELP?

State and local governments face many constraints to improving cybersecurity awareness. These include fiscal and budgetary challenges, lack of social and technical expertise, low organizational capacity, and geographically-bound networks. While I provide a detailed list of recommendations in a later section of this document, some ways that the Federal Government can assist State and local governments include:

- *Direct funds toward local cybersecurity awareness trainings*.—Local governments can partner with nonprofits to roll out trainings aimed at improving the cybersecurity knowledge and outcomes for underserved residents. These trainings can be expensive as they require devices and equipment, qualified trainers, monetary or other incentives for participants, and fixed locations scattered throughout the city. Local government budget might not be able to justify prioritizing these expenses.
- *Design baseline training programs*.—Not all State and local governments have the capacity or expertise to design a cybersecurity training program. The Federal Government should work with local governments to design a baseline training program which details the core topics that all training programs should ad-

[6] Calvert, S., & Kamp, J. (2019, June 07). Hackers Won't Let Up in Their Attack on U.S. Cities. Retrieved from *https://www.wsj.com/articles/u-s-cities-strain-to-fight-hackers-11559899800*.

[7] As More Governments Get Hacked, Concerns Grow Over Mounting Costs. Retrieved from *https://www.governing.com/topics/finance/gov-government-costs-hacked.html*.

dress. While the Federal Government should design the baseline topics and curriculum, the programs should be informed by and tailored to the ground realities of each city and should not limit any government from going further than its selected baseline topics.

- *Develop and rollout public awareness campaigns*.—Public awareness campaigns are more cost-effective and can scale better to reach larger audiences when developed centrally. This streamlines the process of disseminating content to schools, broadcast TV, on-line and physical publications, social media platforms, and radio.
- *Coordinate public-private partnerships*.—The Federal Government is uniquely positioned to work with private technology companies to create advice resources, cross-company collaborations in areas like phishing scams and coordinated disinformation campaigns, and technological solutions like cybersecurity chat bots and apps for smart phones that no longer receive security updates. As I will explain later in this testimony, underserved populations tend to place a high level of trust on advice resources provided by private technology companies. It would be highly inefficient for every State and local government to individually approach technology companies for their own respective solutions.

STUDY: CYBERSECURITY AWARENESS FOR UNDERSERVED POPULATIONS

A growing number of cities across the United States have invested in digital literacy training programs that aim to educate underserved populations in the basics of computer usage and commonly-used software.[8] Such programs often combine the provision of digital services, such as free public wi-fi, with digital literacy training to help groups who are at risk of digital and social exclusion. These initiatives are often led by nonprofits and local governments and aim to improve citizens' skills and confidence, as well as increase their motivation to engage in on-line activity.

San Francisco has a digital literacy initiative under its Office of Digital Equity,[9] where the city government works with local partners in the nonprofit space to provide digital literacy training to its residents, the vast majority of whom come from low-income households, are immigrants, and seniors. Early discussions with city residents were revealing: They expressed frustration at their inability to prevent and resolve cyber attacks such as phishing scams, viruses, and harassment. They were afraid of using important on-line services like banking apps and social media platforms.

The theory of change in digital literacy programs normally involve encouraging internet use to increase employment, education, creativity, and entrepreneurship. But vulnerable populations are easily discouraged from using important internet services when faced with complex threat vectors.

We widen digital inequities and reduce the efficacy of digital literacy trainings when we do not actively teach cybersecurity. Moreover, by neglecting the duty to educate and inform, we leave a large portion of the population at the mercy of bad actors who can exploit digital vulnerabilities for their own gain.

RESEARCH FINDINGS

I conducted a survey of underserved residents in the city and county of San Francisco to understand the scope and nature of the underserved communities' cybersecurity outcomes, and to create evidence-based solutions. These residents were either low-income earners ($25,000 household income or less), senior citizens (65 years of age or older), or foreign language speakers (whose primary spoken language is not English). The 48-question survey was designed to gauge the scope and nature of residents' cybersecurity outcomes, and to understand their cybersecurity knowledge and abilities.

A total of 295 respondents were surveyed. This included 153 respondents from the underserved population. While this is not technically a representative sample, these were the maximum number of respondents I could survey who were enrolled in digital literacy programs across San Francisco. Their experiences revealed through surveys, semi-structured interviews and roundtable discussions reflect social and structural inequities that have persisted for too long. In addition to the 153 underserved respondents, 142 respondents from the comparison group were also surveyed.

POOR CYBERSECURITY KNOWLEDGE AND SKILL LEVEL

Underserved respondents generally have a poor understanding of basic cybersecurity concepts such as on-line scams and viruses. They also have low skill level and

[8] *https://www.digitalinclusion.org/digital-inclusion-trailblazers/.*

[9] *https://sfcoit.org/digitalequity.*

motivation to follow best practices as gauged by cyber hygiene-relevant questions. These include setting a complex password for on-line accounts and employing preventative methods when reading and interacting with the contents of an email.

I designed a Knowledge and Skill index to make meaningful comparisons between the underserved and comparison group respondents. The maximum combined score for the Knowledge and Skill index is 18.0.

- Average cybersecurity Knowledge and Skill index score for the underserved respondents = 9.0/18
- Average (and Median) cybersecurity Knowledge and Skill index score comparison group respondents = 15.0/18

Underserved respondents struggle with fundamental cybersecurity knowledge questions. When asked about their knowledge of core cybersecurity concepts, 20 percent indicated they did not know about on-line crime, 21 percent were not familiar with email spam, 26 percent did not know about computer or phone "viruses," and 31 percent did not know about anti-virus software. Respondents indicated they did not understand the risks associated with sharing their private account passwords or writing down their passwords on paper.

VICTIMS OF CYBER CRIME

A large number of respondents from the underserved group reported being targets of cyber scams and internet viruses. Respondents provided information about the types of personal information that has either been stolen from them on-line, or that they have divulged to a complete stranger on-line. Together, these results paint a picture of an underserved population in San Francisco that is highly vulnerable to internet fraud.

- Nearly 26 percent of the underserved respondents reported that they have been a target of a cyber scam, compared with 15 percent for the comparison group.
- Nearly a third (31 percent) of those scammed have been scammed 3 times or more.
- Forty percent of underserved respondents reported that their computer and/or phone has been infected by a virus at least once.

AWARENESS OF CYBER CRIME VICTIMHOOD

Although many underserved respondents reported being a victim of cyber crime, an equally large number of respondents are not aware whether they have been a victim to a cyber scam, if their devices have ever had a virus, or if they ever provided personal information to a complete stranger on-line.

- Nineteen percent of underserved respondents do not know if they have ever been a victim to a cyber scam.
- Forty-one percent do not know if their device has ever had a virus.
- Forty-four percent think they have provided personal information to complete strangers on-line but cannot remember the exact details.

INTERNET WITHDRAWAL IS RELATED TO LOW CONFIDENCE

A significant portion of the underserved sample self-assess as having either "high confidence" (36 percent) or "low confidence" (38 percent) in their ability to protect themselves from on-line crime. High-confidence respondents can be described as being "over-confident" in their cybersecurity skills while demonstrating poor levels of precaution and possessing low levels of cybersecurity knowledge, while "low-confidence" respondents can be described as being "overly concerned" about existing risks on-line while possessing and demonstrating above-average cybersecurity knowledge and precaution.

- Self-assessed "low-confidence" underserved respondents are more concerned about the existence of cyber crime than underserved and comparison group respondents.
- For example, 47 percent of low-confidence underserved respondents do not use on-line banking due to cyber crime, compared to 8 percent in the comparison group. These services also include social media use, downloading software, and email.
- This suggests that trust and security play a larger role in determining on-line service usage for the underserved as compared to the comparison group.

CYBERSECURITY ADVICE RESOURCES DETERMINE CYBERSECURITY OUTCOMES

Underserved respondents tend to rely on informal resources for advice about cybersecurity which leads to worse cybersecurity outcomes. In fact using on-line resources for advice on cybersecurity is expected to increase a respondent's cybersecurity index score by roughly 0.23 points. The only other predictor with a statistically significant coefficient is Educational Attainment—the higher the level of schooling achieved, the higher will be the cybersecurity index score.

- 39 percent of underserved respondents rely on friends/relatives for cyber advice
- Only 21 percent of underserved respondents refer to websites, and 7 percent refer to Government websites.
- More than a third of respondents (34 percent) do not seek cybersecurity advice from any resource. Comparison group respondents are more likely to seek help (82 percent) and are more than twice as likely to rely on websites for cybersecurity advice (48 percent).

RECOMMENDATIONS

Federal, State, and local governments have a variety of options and approaches available to improve cybersecurity awareness of underserved populations.

GAIN AN UNDERSTANDING OF THE SITUATION IN YOUR COMMUNITY

The Federal Government should work with cities seeking to improve cybersecurity awareness of local underserved populations to gain a baseline understanding of their specific situation. They can do this by designing and directing funds toward surveys or informational workshops to assess major areas of interest and/or lack of knowledge among residents. Based on my experience, I recommend partnering with local community organizations that serve low-income residents, English language learners, and senior citizens. In addition to assessing cybersecurity awareness, use this initial outreach as an opportunity to assess what modes of training (e.g. 1-hour workshops, half-day workshops, etc.) might be most suitable for different constituencies. It is also important to identify what translation or technology resources might be required to facilitate trainings for the largest number of underserved citizens.

DEVELOP TAILORED TRAININGS TO BOOST CYBERSECURITY AWARENESS

Many cities already offer (or are planning to offer) digital literacy trainings. My findings suggest that such programs should include explicit targeted cybersecurity awareness and training components, which the Federal Government can direct funds toward. A customized cybersecurity awareness program that is tailored to the specific needs of the community—with topics and content prioritized on research-based understanding of the local community's specific needs—could help improve the knowledge and skill level of participants, which would improve cybersecurity outcomes and increase internet service engagement. Potential long-term benefits include improved economic and social indicators for members of the underserved population.

Trainings should be customized for different audiences, and should target areas where citizens possess lower levels of digital literacy. Trainers should also incorporate an awareness of the cultural sensitivities and trust habits of the disparate communities. Analysis of survey responses from San Francisco, for example, suggests that respondents from different communities access different knowledge sources. For example, while a larger percentage of Hispanic/Latino respondents rely on teachers for advice on matters of cybersecurity, African American and Caucasian respondents said they are more likely to refer to websites, while Asian respondents are more likely to refer to friends and relatives.

DEVELOP A PUBLIC SERVICE CYBER HYGIENE CAMPAIGN

The Federal Government can promote cyber-hygiene awareness and suggest best-practices through public service announcements and a cybersecurity campaign on television, in schools, digital platforms, public libraries, radio, and other communication channels.

PUBLIC-PRIVATE PARTNERSHIPS

In addition to providing training to residents directly, the Federal Government has the opportunity to partner with private-sector technology companies and service providers to address system-level cybersecurity concerns, such as the technological protections that are built into devices and systems. Effective system-level protections make it easier for residents to maintain good cyber hygiene.

DEVELOP A CYBERSECURITY ADVICE WEBSITE

Members of the public already have access to reliable and free resources for cybersecurity, including the United States Computer Emergency Readiness Team advice website.[10] Yet in many cities, information about cybersecurity and related resources is disaggregated and difficult to find.

The Federal Government can work with private-technology firms to develop reliable websites that provide cybersecurity advice. It may be feasible to develop a phone chatbot that can help residents with basic information security questions.[11] Such chatbots can be designed to communicate in several languages, and provide clearly defined answers on core cybersecurity knowledge questions, as well as offer step-by-step instructions based upon best practices. Chatbots should also be designed to be highly secure and transparent, with reminders to users not to share personally identifiable information, as this software could in theory be vulnerable to attacks aimed at capturing data and subverting the quality of information provided.[12]

PARTNER WITH COMPANIES TO DEVELOP APPS FOR USE ON OLDER AND UNSUPPORTED PHONES

Underserved populations tend to use older smartphones that are often unsupported by software makers. As a result, older smartphones are not guaranteed to get new security updates, and some software updates for older devices are not compatible with new phones.[13] This is especially a problem for users with Android phones, where the market consists of hundreds of smartphone manufacturers using different and modified versions of Android's OS. According to Google's own figures, two-thirds of Android devices world-wide run older versions of the OS that are no longer receiving security updates.[14] For Apple's iOS devices, that figure is 5 percent.[15] Apple does provide software updates to phones older than 5 years. Even if they follow best practices in cyber hygiene, users with older smartphones are still highly vulnerable to cyber crime because patches are not automatically installed for known vulnerabilities.

The Federal Government should engage smartphone manufacturers like Apple, Google, and Samsung to develop workarounds that protect older smartphones that cannot accept the latest round of security updates. These workarounds could include prompting older smartphones to activate device encryption settings, password manager apps, virtual private networks (VPN), and two-factor authentication software. Companies that develop operating systems should also be asked to develop stricter app security review and enforcement guidelines that can review the catalog of existing apps as well as newly-submitted apps for security bugs.

As a potential challenge, Google has little control over the updates sent to Android phones in which the OS has been heavily modified by the manufacturer, who in many cases retains control over software updates. The Federal Government will need to develop a strategy with Google to reach smartphone manufacturers who are outside of the Google software update landscape.

CREATE A DIGITAL PHISHING/SCAM COALITION

More than half of all emails are spam[16]—and that figure continues to rise. Spam is the primary delivery mechanism for cyber attacks like phishing and malware.[17] And while phishing attacks disguised as fake invoice emails are a popular form of phishing, there are 9 other forms of phishing emails that are harder to spot, such as Mail Delivery Failure emails and order emails. In fact, reports of W–2 tax filer

[10] "Tips." Virus Basics/US–CERT. Accessed September 11, 2018. *https://www.us-cert.gov/ncas/tips.*

[11] Security chatbots have become increasingly popular over the last few years. For example, Endgame developed Artemis, a language agnostic platform that integrates to Amazon's virtual assistant Alexa and provides cybersecurity advice to analysts. See "Four Ways Chatbots Are Transforming Cybersecurity." Endgame. June 16, 2017. Accessed September 11, 2018. *http://www.endgame.com/blog/executive-blog/four-ways-chatbots-are-transforming-cybersecurity.*

[12] "Expect a New Battle in Cyber Security: AI versus AI." Symantec. Accessed September 11, 2018. *http://www.symantec.com/blogs/expert-perspectives/ai-versus-ai.*

[13] For more on security updates and smartphone compatibility, refer to Emspak, Jesse. "When Does an Old Smartphone Become Unsafe to Use?" Tom's Guide. April 09, 2017. Accessed September 11, 2018. *http://www.tomsguide.com/us/oldphones-unsafe,news-24846.html.*

[14] "Distribution Dashboard/Android Developers." Android Developers. Accessed September 11, 2018. *https://developer.android.com/about/dashboards/.*

[15] Apple Inc. "App Store." Purchase and Activation—Support—Apple Developer. Accessed September 11, 2018. *https://developer.apple.com/support/app-store/.*

[16] "Latest Intelligence for August 2017." Symantec. Accessed September 11, 2018. *https://www.symantec.com/connect/blogs/latest-intelligence-august-2017.*

[17] "2018 Internet Security Threat Report." Symantec. Accessed September 11, 2018. *http://www.symantec.com/securitycenter/threat-report.*

phishing scams—one of the most dangerous and effective email phishing scams, according to the IRS[18]—increased by 870 percent between 2016 and 2017.

To address this challenge, the Federal Government should build coalitions of organizations that can target popular and successful phishing scams. Models for such public-private initiatives include the Digital PhishNet initiative, developed jointly by the FBI's National Cyber-Forensics & Training Alliance,[19] and the Advance Fee Fraud Coalition, developed by African Development Bank, Microsoft, Yahoo, and the Western Union Company.[20] Companies should target overlapping scams and phishing efforts by utilizing contacts in the private sector.

Federal Government officials can also partner with international initiatives such as the Unsolicited Communications Enforcement Network (UCENET),[21] which identifies and shares threats to the broad on-line community and facilitates enforcement compliance checks. Private-sector representatives are encouraged to designate a spam enforcement contact, coordinate with law enforcement agencies, and report on new technology trends that affect anti-spam strategies.

CONCLUSION

It has been an honor to appear before this distinguished panel of policy makers and practitioners. Thank you, Chairman Richmond and Ranking Member Katko, for your dedication to addressing cybersecurity vulnerabilities, and for thinking about ways in which the Federal Government can assist State and local efforts.

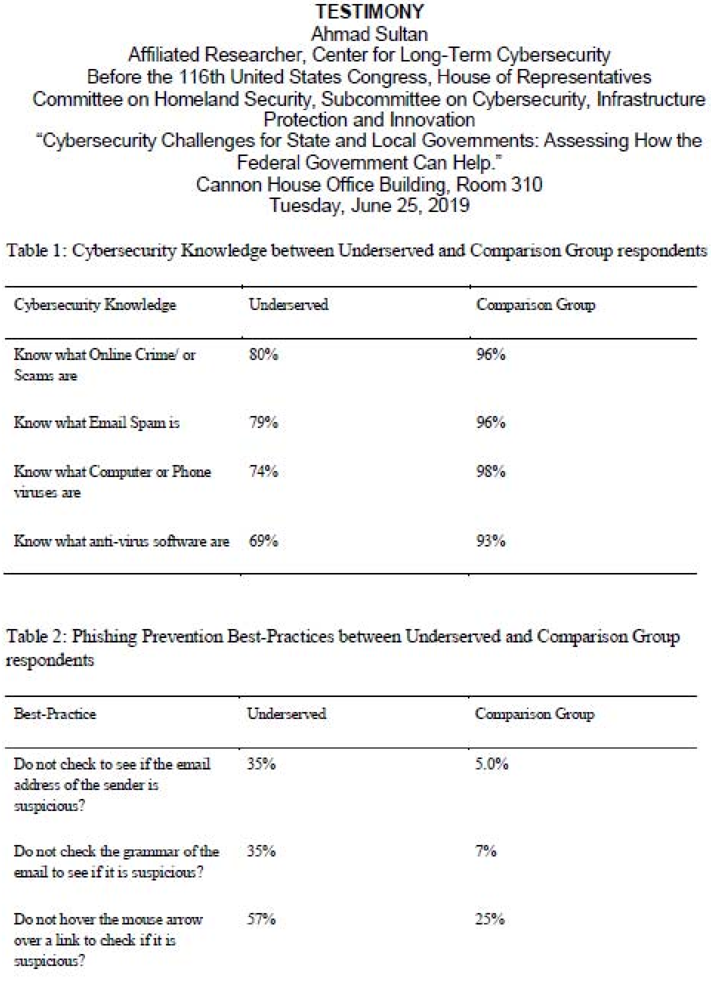
Promoting cyber hygiene through trainings, public service initiatives, and public-private partnerships can lead to significant gains in the lives of underserved populations and protect businesses as well as Government systems from cyber threats. But to achieve these gains, State and local governments will require support and guidance from the Federal Government. It is my hope that policy makers recognize the challenges ahead and rise to the occasion. Thank you and I will be happy to answer any of your questions.

[18] "Dangerous W–2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others." Internal Revenue Service. Accessed September 11, 2018. *http://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others.*

[19] The Digital Phishnet (DPN) collects and develops intelligence regarding high priority and sophisticated phishing and identify theft schemes. DPN uses threat intelligence received from approximately 300 companies. For more visit: *http://www.ncfta.net/*.

[20] The collaborative effort was designed to educate internet users so they are better able to protect themselves against fraudulent activities on-line and to improve INTERPOL's data collection efforts on cyber fraud. For more on this: *http://www.affcoalition.org/*.

[21] Formerly known as the London Action Plan (LAP): *https://www.ucenet.org/history/*.



TESTIMONY
Ahmad Sultan
Affiliated Researcher, Center for Long-Term Cybersecurity
Before the 116th United States Congress, House of Representatives
Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
"Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help."
Cannon House Office Building, Room 310
Tuesday, June 25, 2019

Table 1: Cybersecurity Knowledge between Underserved and Comparison Group respondents

Cybersecurity Knowledge	Underserved	Comparison Group
Know what Online Crime/ or Scams are	80%	96%
Know what Email Spam is	79%	96%
Know what Computer or Phone viruses are	74%	98%
Know what anti-virus software are	69%	93%

Table 2: Phishing Prevention Best-Practices between Underserved and Comparison Group respondents

Best-Practice	Underserved	Comparison Group
Do not check to see if the email address of the sender is suspicious?	35%	5.0%
Do not check the grammar of the email to see if it is suspicious?	35%	7%
Do not hover the mouse arrow over a link to check if it is suspicious?	57%	25%

Do not inspect the 'Subject line' to check if it is suspicious?	37%	9.0%

Figure 1: Withdrawal from Online Services between Underserved (US), Low-Confidence Underserved (LC), and Comparison Group (CG) respondents

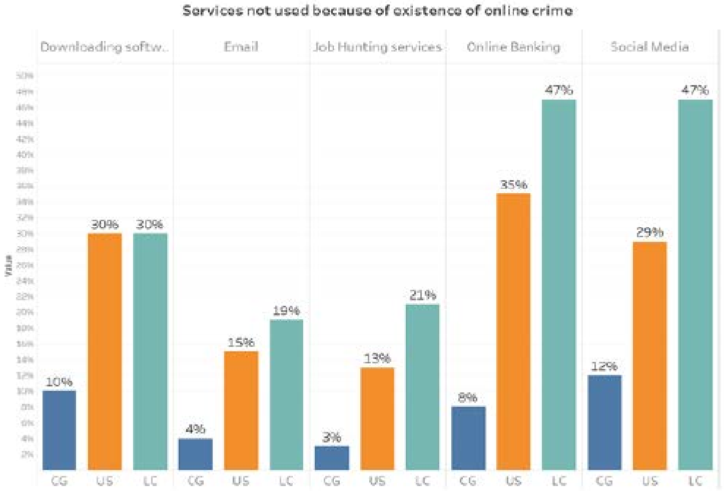
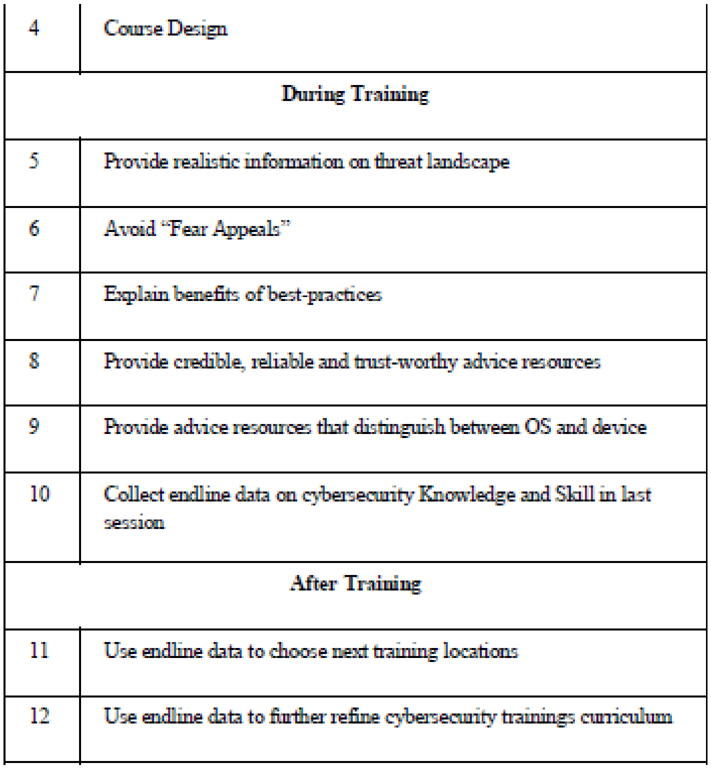


Table 3: Requirements for a successful cybersecurity training program

Before Training	
1	Target training location by income and digital literacy and cybersecurity outcomes
2	Engage with community leaders to finalize training locations
3	Training-of-Trainers



4	Course Design
During Training	
5	Provide realistic information on threat landscape
6	Avoid "Fear Appeals"
7	Explain benefits of best-practices
8	Provide credible, reliable and trust-worthy advice resources
9	Provide advice resources that distinguish between OS and device
10	Collect endline data on cybersecurity Knowledge and Skill in last session
After Training	
11	Use endline data to choose next training locations
12	Use endline data to further refine cybersecurity trainings curriculum

Mr. RICHMOND. Thank you, Mr. Sultan.

We now have Mr. Cilluffo.

STATEMENT OF FRANK J. CILLUFFO, DIRECTOR, MCCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE, AUBURN UNIVERSITY

Mr. CILLUFFO. Thank you, Chairman Richmond, Ranking Member Katko. A real privilege to have Chairman Thompson here. Of course, the great Ranking Member and Congressman from the State of Alabama, Mr. Rogers. It is a privilege to join you today.

As we all know, cybersecurity challenges are daunting enough to deal with at the Federal level. At the State and local, Tribal and territorial levels, where resources and, in many cases, expertise are in relatively shorter supply, these challenges are exponentially more difficult to tackle. Recognizing this mismatch and taking steps to address it is an absolute imperative. Your leadership in confronting this issue head-on today and in legislation that I am happy to hear coming from both the Chairman and the Ranking Member that is reportedly under discussion is commendable.

For too long, State and local have been an afterthought in our National cybersecurity planning efforts. This must change. States and localities perform many essential functions, as you mentioned, Mr. Chairman, that affect real people every day 24/7. The potential consequences are serious. Bear in mind that cyber threat actors can cause loss of life, property damage, and, of course, financial loss by disrupting critical infrastructure or using ransomware and other forms of malware.

The bad guys have taken notice, including that State and local are softer targets and are increasingly in their crosshairs. The ransomware incidents that victimized in Atlanta and Baltimore are case in point but are by no means the end of the story.

The scale and scope of the problem is striking. Data on reported ransomware attacks reveal that 48 States and the District of Columbia have been hit. Targets include police and sheriff departments, schools and libraries, health agencies, transit systems, courts, and the list goes on and on and on. No jurisdiction is too small or too large.

While ransomware might be front and center right now, and understandably so, we need to recognize that the cyber threat landscape includes many more disruptive and destructive modalities of attack. Quite honestly, ransomware is at the low end of the most concerning cyber potential attacks we can witness. Cyber attackers will continue to target weak links. That is the bottom line.

Cyber needs at the State and local level are truly many. More money, more experts, more tools, more threat intelligence information sharing and awareness, more collaboration between governments and industry, among governments, and regionally, just to name a few.

Against this background and backdrop, what should the Federal Government do? I think Mr. Duffy hacked my email because my recommendations are very similar to his.

First, as things now stand, less than 4 percent of grant monies from the Homeland Security Grant Program are directed to cybersecurity. This is clearly not reflective of current threat environment. Congress should enact a dedicated Federal grant to shore up State and local cybersecurity capabilities through CISA at the Department of Homeland Security. It should be risk-based, have built-in metrics, and include a level of matching funds, since simply throwing money at the problem is not the answer. Topping the list of needs include identifying highest-value assets, exercises, training, and, of course, technical support.

Second, CISA should expand its field presence to provide technical assistance and incident response support. In effect, a geek squad for those really bad days so the mayor could call someone.

No. 3, pull a page and leverage lessons learned from the emergency management community by building regional approaches to capacity building and pooling of resources and expertise among States to offer mutual assistance. The EMAC model in emergency preparedness environment has serves us well and I think ought to be replicated and tweaked for cyber.

No. 4, obviously circumscribed election assistance since trust and faith in the electoral process is the very bedrock of our democracy. Some good momentum here, but we need to continue doubling down and make sure we are ready for the next round of elections.

So while I touched largely on technology training, incident response, and work force, this is by no means exhaustive.

I want to close on a little bit of a good news story, and that is this is not all the Federal Government's problem, of course. The Federal Government can, must, and should do more to support our men and women at State and local, but ultimately there is a lot of good activity occurring at the State and local level, and I think it should be recognized.

One in particular I am proud of, and I might be biased, because I serve as a trustee, but in the State of Alabama, they have created a new magnet school focused 7 through 12 grade for cyber and engineering. This is what we need to do. When we talk work force, it is not only at the collegiate level, at the places of higher learning like my great university, but it is really at the K–12 level. I think we need to be spending more time, more money, more resources to be able to get them and get them young, because they are the women and men who are going to be driving the solution sets going forward.

So I have never had an unspoken thought. I can go on forever, but I will close here. The one thing, Mr. Chairman, I should say is, while I am testifying on behalf of the McCrary Institute, a lot of these thoughts came from a committee I chaired for the Homeland Security Advisory Council that I was co-chair. I am just not speaking on behalf of DHS.

So thank you, Mr. Chairman.

[The prepared statement of Mr. Cilluffo follows:]

Prepared Statement of Frank J. Cilluffo

June 25, 2019

Chairman Richmond, Ranking Member Katko, and distinguished Members of the subcommittee, thank you for this opportunity to testify before you today. As we all know, cybersecurity challenges are daunting enough to deal with at the Federal level. At the State, local, Tribal, and territorial (SLTT) levels, where resources and in many cases expertise are in relatively shorter supply, these challenges are exponentially more difficult to tackle. Recognizing this mismatch and taking steps to address it is an absolute imperative in a country as large, varied, and decentralized as the United States.

Your leadership in confronting this issue head-on today and in legislation that is reportedly under discussion[1] is deeply commendable as these are important steps in breaching a real and pressing gap in our National and economic security posture. We must work to safeguard the continuity of commerce and the delivery of mission-critical services for the American people. Unless and until we foster and have in place a robust baseline capability across the board, from a State and local standpoint, we will remain more vulnerable than we ought to be to nation-state and non-state cyber actors with malicious intent.

In testifying before you today, I will be sharing thoughts about how to move forward smartly. These ideas pertain only to those Federal entities that fall within the jurisdiction of the committee. Moreover, a number of these recommendations are based on the May 2019 Interim Report of the Homeland Security Advisory Council's

[1] Maggie Miller, "House Homeland Security Republicans to introduce slew of cybersecurity bills," *The Hill* (June 18, 2019), *https://thehill.com/policy/cybersecurity/448971-house-homeland-security-republicans-to-introduce-slew-of-cybersecurity?wpisrc=nl__cybersecurity202&-wpmm=1.*

State, local, Tribal, and territorial cybersecurity subcommittee.[2] I served as co-chair of that effort, together with Paul Goldenberg (co-chair) and Robert Rose (vice-chair). However, I testify before you today in my capacity as director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security.

SETTING THE SCENE

State and local governments face the full panoply of threats that the Federal Government does, from hostile nation-state actors to cyber criminals and everything in between. To the extent that the Federal Government is effectively outgunned and outmatched in this fight, the State and local level are all the more so. The potential consequences are serious: Bear in mind that cyber threat actors can cause loss of life, property damage, and financial loss by disrupting critical infrastructure operations or other means.

Nor is the cyber threat spectrum static. It continues to expand and evolve, sharpening focus on State and local targets. The ransomware incidents in Atlanta[3] and Baltimore[4] that disrupted city operations are cases in point and by no means will they be the end of the story. To the contrary, the scale and scope of the problem is striking, affecting everywhere from relatively robust States to major metropolitan areas to smaller cities and counties. Data on reported ransomware attacks reveal that 48 States and the District of Columbia have been hit. Targets include police and sheriff departments, schools and libraries, health agencies, transit systems, and courts—the list goes on and seemingly, no jurisdiction is too small or too large to go unaffected. The first known case of ransomware targeted the Swansea Police Department in Massachusetts in November 2013 and since then entities from Anchorage to Augusta have joined the ranks.[5]

Cyber attackers and adversaries will continue to target weaker links in the U.S. chain so long as it remains profitable or otherwise beneficial to these threat actors to do so. To make matters worse, the internet of things with all that it entails from smart cars to smart cities and beyond will expand the surface of attack by orders of magnitude. Security must therefore be more than a footnote or afterthought, especially where critical infrastructure is concerned. In addition, both cyber and physical infrastructure are vulnerable to attack, and the one can cause disruption or destruction in the other. This convergence of cyber domain and the physical world is another significant feature of the threat landscape.

Looking ahead, State and local infrastructure and the cyber vulnerabilities that inhere in it will take on added salience for defenders and attackers alike. Election year 2020 reinforces the point: States and local communities will again be at the tip of this spear, taking a multiplicity of approaches to administering voting. There is no one model or mechanism of cybersecurity governance in use at the State level, whether for elections or taken more broadly. Approaches are varied and so too are capabilities. The same is true at the local level, only more so.

There are examples and pockets of State and local government cybersecurity excellence to be sure; but there are also significant gaps and seams where the Federal Government can help and can do so without subverting the principle that the level of government that is closest to the people knows best how to serve them. Cyber needs at the State and Local level are many: More money, more experts, more tools, more information/awareness and more collaboration (between Government and industry, and among governments and regions)—to name just a few.

Against this background what can and should the Federal Government do? How best can the Federal Government leverage its resources in the broadest sense of the word, to help State and local governments amplify their strengths and mitigate their weaknesses? Enhancing the pool of financial resources available to support a range of cybersecurity purposes is just one—albeit very important—way. Other ideas are set out below.

[2] *https://www.dhs.gov/sites/default/files/publications/19_0521_final-interim-report-hsac-state-local-tribal-territorial-subcommittee.pdf.*

[3] Benjamin Freed, "One year after Atlanta's ransomware attack, the city says it's transforming its technology," *StateScoop* (March 22, 2019), *https://statescoop.com/one-year-after-atlantas-ransomware-attack-the-city-says-its-transforming-its-technology/*.

[4] Emily Stewart, "Hackers have been holding the city of Baltimore's computers hostage for 2 weeks," *Vox* (May 21, 2019), *https://www.vox.com/recode/2019/5/21/18634505/baltimore-ransom-robbin-hood-mayor-jack-young-hackers*.

[5] Allan Liska, "Early Findings: Review of State and Local Government Ransomware Attacks" (Recorded Future: 2019), *https://go.recordedfuture.com/hubfs/reports/cta-2019-0510.pdf.*

MOVING FORWARD SMARTLY

Directed Federal Funding

Funding is crucial of course and building capability is impossible without it. Purchasing, maintaining and upgrading equipment, hardware, and software comes at a financial cost. So too does recruiting and retaining skilled workers. Educating the next generation and expanding the cyber workforce by training or retraining the existing talent pool also requires an investment of dollars, time, and effort. For all of these purposes and more, a Federal grant program to shore up State and local cybersecurity capabilities is needed and long overdue. As things now stand, less than 4 percent of grant monies from the Homeland Security Grant Program are directed to cybersecurity. This is not a tenable situation. Nor is the answer to redirect existing monies for cyber purposes. Robbing Peter to pay Paul simply will not work.

A dedicated Federal grant program should have built-in safeguards to ensure that there is return on Federal investment in the form of measurable State/local and by extension National capabilities. Simply throwing Federal money at the problem is not the answer. Instead, there must be a thoughtful strategy and accompanying metrics to support the request for funds and any subsequent grant. The program would therefore be risk-based and tailored to particular context. Among the purposes that such a program could and should support would be both State-level and regional exercises. Notably momentum for directed Federal funding is building as evidenced for example by the recommendations in the May 2019 Interim Report of the Homeland Security Advisory Council's State, local, Tribal, and territorial cybersecurity subcommittee.[6]

Amplify Training Opportunities

The Federal Government could further assist by providing opportunities for State and local officials to gain and hone cybersecurity skills, as well as how to identify and counter foreign influence. While education and training programs certainly do exist they are neither as numerous nor as evenly available across the country as would be ideal. A National focal point where those whose community is underserved by training opportunities could advance their skills and career and by extension the National interest, would serve us all well.[7] All the equipment, tools, and resources in the world will be of little assistance if the technical expertise needed to employ them to full advantage is not cultivated in the requisite official quarters.

Among the beneficiaries of such training could be State and Major Urban Area Fusion Centers, whose cyber-specific capabilities have long lagged behind their other homeland security and law enforcement capabilities.[8]

Leverage Lessons Learned

Over the past 20 years, the country has learned many lessons about preparing for, responding to, and bouncing back from major incidents such as terrorist attacks and natural disasters. These experiences have ultimately made us smarter, stronger, and more resilient as a Nation, though we still have a ways to go. Among these lessons is the value of taking a regional approach to capacity building and mutual assistance, which builds upon existing relationships and arrangements, and follows logically and naturally from proximity and geography, rather than duplicating efforts and according formal borders/boundaries undue influence. The EMAC—Emergency Management Assistance Compact—concept is as relevant here as in the traditional emergency management context. Pioneered in the South, use of the construct has expanded over time[9] and would transpose well to the cyber domain. The basic idea is to pool resources and expertise in order to offer mutual assistance.

When it comes to cybersecurity, such an approach would for example have States undertake planning, incident response, and resilience enhancement measures from a regional perspective. Here the Federal Government could and should act in support of these efforts including by acting to expand awareness of best practices and guidance on how best to implement them.[10]

[6] *https://www.dhs.gov/sites/default/files/publications/19_0521_final-interim-report-hsac-state-local-tribal-territorial-subcommittee.pdf.*

[7] Note also that the HSAC's SLTT Cybersecurity Subcommittee Interim Report recommends the creation of a National Cybersecurity Academy to train SLTT Government employees—an idea whose time has come.

[8] Frank J. Cilluffo, Joseph R. Clark, Michael P. Downing, and Keith D. Squires, *Counterterrorism Intelligence: Fusion Center Perspectives* (June 2012).

[9] EMAC Overview (August 2006), *https://www.fema.gov/media-library-data/20130726-1726-25045-0915/060802emac.pdf.*

[10] Note that the HSAC's SLTT Cybersecurity Subcommittee Interim Report also highlights the value of a regional approach.

A further lesson learned over time relates to recognizing the importance of being out in the field rather than at headquarters. There is no substitute to having boots on the ground. To this end, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) should extend its operations and work toward having State cybersecurity coordinators for all 50 States to provide technical assistance and incident response support. This would broaden and complement existing DHS efforts and field personnel (State Cybersecurity Advisors) focused on community engagement and awareness as well as the provision of enhanced strategic advisory services. The arrangements proposed here would also help convey and highlight the Federal consequence management capabilities and tools that can support and supplement State capabilities—in effect a bad day "geek squad."

Circumscribed Election Assistance

One of the most significant cybersecurity challenges to State governments relates to the 2020 election and in particular preparing to administer the vote and ultimately doing so. Protecting the integrity of the process from beginning to end is of paramount importance as this exercise provides the bedrock for our democracy; trust and faith in the process is the glue that binds us together. The Federal Government can and should share more widely and actively its unique informational and other assets with State-level counterparts for the targeted purposes of identifying and mitigating threats in this context.[11]

To be clear, this would involve concerted Federal efforts to create and maintain a rich picture of the threat from the National perspective and a companion effort to support State officials in responding effectively and timely to that dashboard as it specifically pertains to them/their State.[12] Such a division of labor is properly respectful of the division of powers and capitalizes upon the strengths that reside at each level of government. By working together in this way, the Nation stands the best chance of defeating adversary attempts to exploit not just our technology but also our hearts and minds, by means of weaponizing information and influence. Fortunately, we are seeing some positive indicators already, with (DHS) CISA deepening its outreach to and work with the Nation's Governors.

This series of recommendations focuses on technology, training, incident response, and the workforce. The list is not exhaustive and speaks instead to the actions that could have the highest impact on the cybersecurity challenges of greatest priority in the context of State and local government.

ENDING ON A GOOD NEWS STORY

In addition to assessing how the Federal Government can help State and local governments to address cybersecurity challenges, it is important to acknowledge that there is good work under way outside the Federal sphere and that State and local entities are taking substantial steps to help themselves. Keep in mind that States have a correlative and on-going responsibility to lead and lean forward, and should not expect the Federal Government to supplant State efforts or to be there all the time. In this regard consider for example the Alabama School of Cyber Technology and Engineering (full disclosure: I serve on the School's Board of Trustees). This magnet school for grades 7 through 12 will stand up in August 2020 in the Huntsville Research Park. Our vision for the ASCTE is to "educate, develop, and inspire the next generation of leading National professionals and technologists in engineering and cyber technology."[13]

This effort complements the many cybersecurity programs and initiatives including partnerships with industry and government that are under way at Auburn University and other educational institutions within the State of Alabama and in the Southeast more broadly. While the coasts of this country tend to garner the bulk of attention when it comes to coverage of cyber and science & technology matters more generally, it is important to recognize that other jurisdictions are quietly plowing ahead on significant efforts in these same issue areas that are so critical to our National security. These under-reported successes serve us all well since Federal measures alone will not get us to goal or keep us there even if they could.

[11] But note that the Multi-State Information Sharing and Analysis Center (MS–ISAC) does yeoman's work in terms of amplifying situational awareness (for example by providing threat alerts to all 50 States and manifold localities); and helping to coordinate incident response. For details, see *https://www.cisecurity.org/ms-isac/*.

[12] A variation of this idea is proposed in the HSAC's SLTT Cybersecurity Subcommittee Interim Report.

[13] *https://www.alabamasce.org/school*.

Thank you once more for this opportunity to participate in this important conversation and assessment.[14] I look forward trying to answer any questions that you may have.

Mr. RICHMOND. Thank you, Mr. Cilluffo.

I thank all the witnesses for their testimony.

I will remind each Member that he or she will have 5 minutes to question the panel. I will now recognize myself for questions.

The first question, I will just direct it to you, Mayor Bottoms. Historically, cities and States have spent a much smaller percentage of their overall budgets on cybersecurity than Federal agencies and similarly situated private entities. A recent study from National Association of State Chief Information Officers shows that most States spend only 1 to 2 percent of their overall IT budget on cybersecurity.

So the question for you would be, in Atlanta, what are the limitations does your city face when trying to develop and implement robust cybersecurity controls, strategies, and resource plans?

Ms. BOTTOMS. Thank you for the question. When we experienced our cyber attack, it was very clear to us that we simply were not prepared. It was not where we had made the necessary investments.

People don't see cybersecurity. They see sidewalks, they see potholes. We were allocating our resources accordingly and we were also putting patches on gaping holes.

That being said, it is the reason that we did not pay our ransomware, because we knew that we needed to build a stronger, safer system. We have allocated resources accordingly. Now there is also an expectation from the public that it is necessary for us to budget for our cybersecurity network in the same way that we budget for our other priorities within the city.

We are also messaging that to the public, that this is equally a priority, and that messaging is a lot easier now, because the public has felt that impact. In many ways, people are becoming very sensitized to cyber attacks.

We are continuing to work with our private partners as well. We are very fortunate in Atlanta that we have a very booming tech industry, also with Georgia Tech and the Atlanta University Center. So there is an interest in helping us in ways that other cities may not have that benefit. But also, it is important that Federal funding trickle down into our cities to allow cities like Atlanta, and especially our smaller cities, opportunities to purchase cyber insurance and in the same way that we did to be able to actually bill the system that is needed. Because in so many cities, that system simply does not exist at this point.

Mr. RICHMOND. As a chief executive of a city, how hard is it to retain the cybersecurity professionals and the talent that you need to do this when we have a severe shortage of cybersecurity professionals and the private sector pays a lot more than the public sector? So how are you addressing that challenge, and how can we help with that?

Ms. BOTTOMS. It is extremely difficult for us, because we are competing with the private sector. We really are looking for people

[14] I would also like to thank my colleague Sharon Cardash, deputy director of the Center for Cyber and Homeland Security, for her assistance in preparing this testimony.

and are fortunate that we have people who actually are interested in public service. But funding is always necessary and would be extremely helpful for us to offset and to be able to compete accordingly.

We have increased our budget in our DIT department, but it is still not enough. It is always a challenge for us to attract and retain talent, because we simply cannot pay what the private sector pays.

Mr. RICHMOND. You mentioned it a second ago and you said that now you are fortunate. When I look at our cities, and I will just take my own, for example, that constituents are concerned with sanitation being on time, street lights, police officers, and potholes. The city of Atlanta is now very keenly aware of the threat of cybersecurity.

What advice would you have for other mayors who have not been attacked yet but still face those competing pressures of real brick-and-mortar infrastructure compared to cyber infrastructure?

Ms. BOTTOMS. You have to plan and prioritize accordingly. We were very fortunate in that it was not our 9–1–1 system, but it very well could have been. Ironically, our public may say that they received a bit of a reprieve because they couldn't pay traffic tickets and they couldn't pay their water bills.

But that being said, our cities must prioritize and anticipate in the same way that we anticipate for any other major disaster to hit our cities, because, really, that is what it is. It is simply a disaster when it hits your city.

Mr. RICHMOND. Well, I see that my time has expired, so I want to thank the witnesses.

I will now recognize the Ranking Member, Mr. Katko, for 5 minutes of questioning.

Mr. KATKO. Thank you, Mr. Chairman.

I want to make a couple of observations before I ask some questions. First of all, Mayor Bottoms, I want to commend you for having the political courage to stand up to this ransomware attack and not pay the ransom. That takes guts, and I commend you for that.

Just out of curiosity, you said there was two Iranians that were charged with this?

Ms. BOTTOMS. There were two Iranians.

Mr. KATKO. Have they been brought to justice yet?

Ms. BOTTOMS. They have been charged. I am not sure what the status is. But we were very fortunate in that they were actually identified, which is very unusual, as I understand it.

Mr. KATKO. Very unusual. That is why I am curious. Were they in the United States or don't you know?

Ms. BOTTOMS. They were not.

Mr. KATKO. OK. All right. Well, that is just a great example of the threats that we face.

Mr. Duffy and Mr. Cilluffo, I think you both kind-of touched on this, the importance of the Federal, State, and local partnerships. You know, as a Federal organized crime prosecutor, I would be dead without Federal, State, and local task forces. It is really the same concept. The synergistic qualities of having all these different players come to the table, work together under the same roof, there is no substitute for that. They all bring different strengths to the table. I commend you for understanding how important that is as well.

Mr. Cilluffo, I am very disturbed about the less than 4 percent of Homeland Security funds grant money going toward cybersecurity. You know, I was thinking back to pre-9/11. We had plenty of alarms out there, and we didn't pay enough attention or prioritize those alarms, and we paid a dear price for that.

It kind-of seems like we are doing the same thing again here. We understand the concerns. The alarm bells are going off awfully loud. Before we have a catastrophic cyber event, we better get our act together and prioritize with more funding and more attention.

On a somewhat smaller but important scale, that is what that bill I was talking about to you all was about. It would develop basically a front page for CISA so any State or local government could go to that page and understand exactly where the resources are instead of trying to fish around for them. So that is step 1 of the bill.

Step 2 are to grant programs for State and local grants to identify high-value assets so you can prioritize what needs to be protected most, and then we can address those accordingly.

The third thing would be is to grant State and local governments—to provide grants to State and local governments to conduct exercises, tabletop and what have you, to train, prepare, and evaluate responsibilities.

So those are the things that I think are important. I would like to hear feedback from all of you, if we have time, as to what you think about the bill and whether it would help. Mr. Duffy, you could start.

Mr. DUFFY. Yes, I certainly think the bill would be very helpful. You know, certainly the exercises are critical. I can say that DHS and FEMA have been pretty active in the exercise area. They just held the National-level election exercise last week. I know some of the House member staffs were participating in that.

There is a National cyber storm exercise coming up. There is a guard exercise coming up. Certainly, more exercises are needed. More participants need to be active in the exercise program.

I think the State and local partnership is critical. A lot of States—I mean, 5 years ago, the States weren't doing much with the local government relative to cybersecurity. That has changed quite a bit. You know, they do recognize that the local system is connected to State. So local problems can become State problems in a hurry. State systems connect to Federal Government. So, again, State problems could be Federal problems in a hurry.

A lot of States, such as New York, Wisconsin, Iowa, have been using the Homeland Security money to help the local governments. I know New York State just released a $50,000 grant to counties. So they are working on that.

Mr. KATKO. Right.

Mr. DUFFY. Certainly, Wisconsin is doing it with the State-wide incident response team with using members of local government as volunteers. So there is money out there, but they need more of that.

Mr. KATKO. All right. Message received.

Mr. Cilluffo.

Mr. CILLUFFO. Well, Mr. Katko, I think the legislation, as you laid it out, nails it. I mean, every one of those items is needed and needed desperately. There is an old adage: Policy without resources is rhetoric. But it is more than just the resources. The resources are important. That puts skin in the game. But at the end of the day, you do need to get to the point that you can build the relationships.

The Joint Terrorism Task Forces, the JTTFs, those entities are worth more than any weight in gold in terms of building trust between the women and men who have to work together in very tough situations. So I do think that exercises—we shouldn't be picking up the playbooks on game day. We have got to be exercising this beforehand. We shouldn't be needing the offensive and defensive coordinators on game day. Everyone needs to get to know one another.

While we are doing some of this at the Federal level, and Congress Langevin knows very well, there is a commission looking at some of how of the inner agency gets together that we had the privilege to serve on together at the Federal level. But that is not anywhere near where it needs to be at the State and local level. So whatever advocacy, count on me being there.

Mr. KATKO. I am out of time, but I do want to observe that this is perhaps one of the best qualified panels I have seen in a hearing in quite a while, so I appreciate the witnesses.

I yield back.

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

I know recognize the Chairman of the full committee, Mr. Thompson, for 5 minutes.

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

Mayor Bottoms, one of the challenges we have as Members of Congress, people say, well, if you would just give us the money, we can fix it. But our challenge is, do we set parameters of guidelines with the money so that at the end of the day we can measure how successful the goal has become?

So if Congress did somehow get in the business of helping State and locals fortify its cyber systems, do you see any pushback with the resources coming with some criteria by which the money would be sent?

Ms. BOTTOMS. Absolutely not, Mr. Thompson. What I see is it would be welcome, because we have a challenge with, No. 1, hiring professionals as we compete with the private sector. Also, in having—I believe it should be at least a baseline standard with what our systems and security systems should be in place.

For many years, again, we were allocating small amounts of money per our budget toward our system, and we were not addressing the real needs and upgrading in the way that we should. With this cyber attack, it made us allocate a much larger portion of our budget than we ordinarily would have to do something as simple as create the cloud. I think that with partnership with our Federal partners and with the allocation of resources, I think that it will help put cities on a much stronger footing and also create a baseline of standards that many cities may not even be aware of until they are faced with something as disastrous as a cyber attack.

Mr. THOMPSON. Mr. Duffy, you talked a little bit about this in your comments. Do you want to share your opinion on that?

Mr. DUFFY. Yes. I think anything when they are distributing grant money, there certainly should be conditions relative to how smart was the money spent. Just throwing money at the problem is not the solution. Money has feet. One thing they need to do is identify what their gaps are, what are their weaknesses, and identify how are they using that money to plug those holes that are in their networks. What are the metrics you want so they can prove that the money was well spent. As I said, throwing the money at it won't solve the problem. But metrics and accountability should go hand-in-hand with any grants that are out there.

Mr. THOMPSON. Mr. Cilluffo, are you comfortable with the responses that have been received?

Mr. CILLUFFO. Congressman Thompson, absolutely. I do just want to underscore it is important. We have learned lessons the hard way after 9/11 in terms of how all the funds were disbursed and used. But I think it is now a much more refined process, and I think we need to do the very same with respect to cyber.

I mean, we absolutely need the resources, but we need to also make sure we are measuring what matters. The one thing that I would like to see is a match coming from State and local, that they are committed, that they are willing to put a percentage of whatever outcome of their own resources to maximize the impact. But it is needed.

Mr. THOMPSON. Thank you.

I yield back, Mr. Chairman.

I will yield my minute to the Chair.

Mr. RICHMOND. I just wanted to make a point. I am not needling my colleagues on either side of the aisle, but this goes back to the Federal Government and our role as the Federal Government of helping municipalities and others who are—some things are beyond their capacity, whether it is talent-wise or money-wise.

So do you think that we can provide more cybersecurity in this country with less money? Does anybody think we can provide more cybersecurity with less resources?

Mr. DUFFY. I would say no.

Mr. RICHMOND. OK. Can we secure more airports with less TSA agents? No?

Mr. SULTAN. No.

Mr. CILLUFFO. I think you can do more. That doesn't mean it is going to be 100 percent, because cybersecurity—it is not an end state.

Mr. RICHMOND. Well, no. My question is going toward this general thing. When we go through our budget cycles, the mantra is usually we are going to do more with less. I am just asking, is this an area that we believe we can do more with less money, just like TSA?

I just wanted to highlight that we have different challenges in this country in this time and day. It costs money to protect the American people. It is not that we just want to spend, spend, spend. What we really want to do is protect, protect, protect our people, their assets, and their resources.

With that, I will recognize the gentleman from Texas, Mr. Taylor, for 5 minutes.

Mr. TAYLOR. Thank you, Mr. Chairman. I appreciate this hearing. I think this is important.

Just to kind-of go through one specific item that has come to my attention. Sometimes cities lose control of their data, right? So cities provide municipal services, water service, electric service. They have everybody's address. They have got their phone numbers. They have got their credit card information.

Is there a standard or a Federal requirement of some kind to tell the consumer, to tell their citizens, hey, we have lost your data, it got breached? Is there some kind of standard out there that—I am not aware of one, but maybe you can tell me that there is.

Mr. Duffy, do you know of a standard?

Mr. DUFFY. Yes. Well, most States have a breach notification law. So if there is a breach and the breach reaches a certain criteria relative to the number of individuals that are impacted, there is a requirement that they do notify the individuals.

Where it gets rather difficult is, say, someone's credit card is compromised by a local town, and they may not have the person's individual address to identify to contact them. So then they have to work with their credit card company, because they are the ones that have the relationship with the individuals.

But I think almost every State, not quite every State, does have breach notification laws.

Mr. TAYLOR. Did you want to follow up with that?

Mr. SULTAN. Congressman Taylor, I do think—and people have attempted to move toward a National data breach notification law, which I think we really do need, because there is lots of confusion. You have seen one State, you have seen one State. That is a good thing. That is what a Federalist form of government is.

But when it comes to data breach notification, we should have consistency across the board. I know some of your colleagues have pushed for this for a while. My argument is keep pushing.

Mr. TAYLOR. Do you think it is incumbent on the Federal Government to devise standards for cities, counties, you know, subdivisions of the U.S. Government to force cybersecurity? I mean, to have a Federal standard. Hey, this is—you need to response in this amount of time to this. You need to have this standard of security.

Is that something that we should be looking toward doing, Mr. Duffy?

Mr. DUFFY. Well, I think, certainly, the standard should be a goal that folks should strive to achieve. One of the things we suffer from now, there are so many standards out there. There are so many criteria. Just as I mentioned with the Federal auditors. I was speaking to a State chief information security officer yesterday on this topic, and he told me that at the end of April, he had 4 different teams of Federal auditors on all asking different questions. Even the Federal Government doesn't ask the same questions.

Mr. TAYLOR. So who are the 4 different teams? Like where do the 4 different standards come from?

Mr. DUFFY. I can find out for you.

Mr. TAYLOR. OK. Mr. Cilluffo, do you——

Mr. CILLUFFO. You know, I think that the private sector needs to be part of whatever it is we are driving here. So I think that there are standards that may not only be legislated, but here is the—the reality is the private sector is on the front lines of this war. Just like how many cities went into business and how many companies went into business thinking they had to defend against foreign intelligence services. It is an unlevel playing field. It is. But the question is, do we have enough to know what a single standard is? I am not 100 percent sure. I am not smart enough to figure that out.

But I do think we have a series of them. I do think, at least with data breach notification, that is something worth fighting for.

Mr. TAYLOR. Mr. Duffy, I think I cut you off. Did you want to finish?

Mr. DUFFY. No. Just on the data breach notification. I think the importance of a National standard is that businesses, especially small businesses that are now on the internet and doing business around the country, they now have to understand how to respond to a data breach with regulations in place in 50 different States. It is hard for them to be able to follow what they need to do if there is a breach when there is 50 different regulations I have to follow.

Mr. TAYLOR. OK.

Ms. BOTTOMS. Mr. Taylor, may I just add, within hours of our attack, we went before the public to notify the public, because we didn't know if we were dealing with just a cyber ransomware attack or if we were dealing with a data breach. We found it extremely helpful to communicate that to the public, and it was appreciated. I think it gave us a little more leeway. The public was much more appreciative and patient with us during that recovery. So I do think it is helpful.

Mr. TAYLOR. Thank you.

I yield the balance of my time to the gentleman from New York.

Mr. KATKO. Thank you very much, my colleague.

Mr. Cilluffo, just a very quick question. As many cities look to become smart cities, including the city of Syracuse, are they also considering, to your knowledge, cybersecurity risks associated with an internet of things and additional connectivity?

Mr. CILLUFFO. Well, thank you, Congressman Katko. That is an issue that should keep everyone here up at night.

Mr. KATKO. Indeed.

Mr. CILLUFFO. Smart cities are amazing opportunities. But it also exponentially expands the attack surface and can touch individual citizens directly that the only way to try to get our arms around this is to bake security into the design at the early stages, design and planning stages of smart cities. So shame on us if we are not thinking about this, but easier said than done.

The highways of tomorrow are going to be paved in silicon as much as they are in asphalt. The reality is, is this is the future, and to retrofit afterwards is going to be exceedingly difficult, if not impossible. So big issue. Great opportunity. Just let's make sure it is not a footnote or an afterthought in our smart city planning.

Mr. KATKO. Thank you, Mr. Taylor.

Thank you, Mr. Chairman.

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

I now recognize the gentleman from Rhode Island, Mr. Langevin.

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

I want to thank our panel of witnesses, some of whom are very familiar to me and I have had the opportunity to meet with, so thank you for all that you are doing on this topic. I have covered a lot of important issues, and concerning the data breach notification, I agree. You know, we are focused right now on a different topic, but I have got a bill in for a 30-day data breach notification, which would be a 30-day Federal standard, and I think that is something that we should move along.

We talk about cyber work force, of course, and we shouldn't look at this in terms of competition and try to—in terms of how the local, State, or Federal Government can compete for the talent that is out there. We really need to focus on growing the pie itself, not just our piece of the pie at the local, State, or Federal. That is, obviously, looking more deeply into our educational system and how we can incentivize people going into this field.

But let me go back to what we are talking about and the issue of what is the right balance of, you know, State, local, and Federal attention support on cyber. So I have been trying to draw attention to and prioritize cybersecurity now for over a decade, and the problems of getting focus of dollars are, unfortunately, not new and they exist across the private sector and the Federal Government as well.

So one of my concerns, though, is that the Federal investments will supplant rather than complement State and local funding, and I don't want to see that. We see that between the—you know, with the private sector, even critical infrastructure. We say the private sectors, you know, fine to say—they are quick to say, if you want us to do more on cybersecurity, well, then, you pay for it, but, you know, everybody really does have a role here.

So for the panel, I wanted to ask, how can we better ensure that cybersecurity is a priority for leadership in State and local governments? What will incentivize State and local leaders to make adequate investments in this space?

Mr. DUFFY. One of the things that is happening recently with the FEMA grants, I mentioned earlier that we conduct a Nation-wide cybersecurity review of State and local governments, and right now, participation is voluntary. We have had relatively high participation in the State, around 90 percent, but the local government has been low, and that is intended to identify gaps in the capabilities where they should be investing their money.

With the new Homeland Security grant funding, there is a new requirement that recipients and subrecipients must take the Nation-wide cybersecurity review to find out, to identify where their gaps are, where their investments should be made. The nice thing about it, it is a confidential assessment, so the information on the assessment goes to them to help them develop a strategy where they should be making their investments.

I certainly share your concern on it should not supplant funds. You know, it should be for new initiatives. That is always something that I think is real difficult for the guidance writers, but I defer to them on how they get that in there.

Mr. LANGEVIN. Anybody else on the panel care to comment?

Mr. SULTAN. Congressman, I think it is a really good question. I have previously worked very closely with the city and county of San Francisco's administration, especially with their digital staff, and I think if the city administration began having a frank conversation with the digital staff that work for the cities, they would understand that they are highly unequipped at this moment to deal with massive amounts of cyber attacks that are happening on a daily basis.

Right now, the cybersecurity staff are not solely focused on cybersecurity. They usually have dual roles, and cybersecurity is usually a secondary role. So when they begin working and focusing on cybersecurity, they have to read documents that range between 300 to 500 pages. These are referred to as NIST documents that provide standards for cybersecurity.

So when you look at these overworked staff that have to deal with cybersecurity standards, it can be incredibly cumbersome, frustrating, and difficult to deal with as the city isn't focusing on providing sole cybersecurity staff.

Ms. BOTTOMS. As one of the panelists mentioned, I think matching funds in the same way that we seek matching funds for transportation and infrastructure projects, I think that that would be a great incentive for cities, because we are making the investments but often not enough. But I think any opportunity for us to have matching funding will also encourage us to invest more on our end.

Mr. LANGEVIN. I completely agree.

Mr. CILLUFFO. Congressman Langevin, I was just going to bring up that other point. But also in the opening statement by Ranking Member Katko, I think he said it was 1 or 2 percent of the IT spend is going toward security. Best practice in the private sector is 8 to 11 percent. So we really do need to bridge that gap there, and I think Mayor Lance Bottoms said it straight up, and the reality of matching funds would go a long way.

I think it is also great that you have the executive testifying, not the CISO and—because ultimately, cybersecurity is an executive issue. It is not going to be relegated to the IT department. That is important, but it is ultimately understanding how cyber fits in to the risk of the company, country, or city.

Mr. LANGEVIN. Very good.

Thank you all for your answers and your attention to this. I agree with a lot of what has been said, so thank you very much.

Mr. Chairman, I yield back.

Mr. RICHMOND. The gentleman from Rhode Island yields back.

Before I recognize the gentlelady from New York, Mayor Bottoms, I understand you have a hard 4:15 stop?

Ms. BOTTOMS. OK.

Mr. RICHMOND. So let me just—before you get up, ask the gentlelady from Illinois and New York, do you have—did either of you have a specific question for the mayor?

Well, with that, Madam Mayor, thank you for leaving your busy city and coming up here to provide valuable insight to this committee. So with that, we will just pause and give you a second to break. We don't want you to miss your plane back to Atlanta.

Ms. BOTTOMS. Thank you.

Mr. RICHMOND. The Saints and the Falcons will see each other twice this year.

Ms. BOTTOMS. Thank you again.

Mr. RICHMOND. I now recognize the gentlelady from New York, Miss Rice.

Miss RICE. Thank you, Mr. Chairman.

This question is for any or all of you, the Ranking Member, Mr. Katko, and I recently wrote to the New York Metropolitan Transportation Authority expressing concerns over the possibility of buying subway railcars from a Chinese state-owned entity. We did that because we were concerned that State and local governments don't have the proper resources to prepare for the threats posed by state actors since these types of National security decisions have typically taken place at the Federal level.

How do we address this issue of supply chain—the supply chain issue at the local and State level?

Mr. CILLUFFO. Miss Rice, I will take first crack. So I testified recently before Transportation and Infrastructure on the CRRC and State-owned enterprises and the concerns that poses for the country, and I think they are genuine, real risks, especially when we start thinking about ZTE, Huawei, 5G. This is going to be the underpinning of modern societies, and we don't want it built on quicksand. So I think these are big issues.

It took Congress, though, to help bridge a gap because Huawei is cheap. It is much cheaper. When you are in a city and a community and you want to do all you can for your citizens, you are going to find the most cost-effective way to do that. So you raise a really good question.

Miss RICE. Well, it is hard to ignore that, though, Mr. Cilluffo——

Mr. CILLUFFO. Impossible to ignore.

Miss RICE [continuing]. Because they always come in lowest bid. Always.

Mr. CILLUFFO. They are subsidized, on top of it, and they have got concessionary financing on top of that, so it is a triple whammy against some of these States. But I think when the Federal Government takes strong actions to ban certain technologies, that should be a nod toward State and local as well.

Miss RICE. I totally——

Mr. CILLUFFO. At least for Federal grants.

Miss RICE. Yes. I agree with you, and so, hopefully, we are going to get some answers there.

Mr. CILLUFFO. Mr. Sultan, you mentioned this in your written testimony and, Mr. Cilluffo, you referred to the magnet school for 7th through 12th graders. Can you just talk more about that? Because I think one of the biggest problems that we have in this field, on top of the funding—and you have all alluded to this as well—is the talent pool. We have to start building a talent pool because these issues are not going to go away.

So can you explain, Mr. Cilluffo, a little bit more about this magnet school? Do we have to be—I understand the education and curriculum issues are run at the State level, but should this be a mandatory curriculum?

Mr. CILLUFFO. I will be very brief because I am sure Mr. Sultan has some thoughts. I am very proud of this magnet school because we do need to get them younger. I used to run an MBA with the focus on cybersecurity, and I would bring my students to a residency overseas in Estonia. In Estonia, you have got a small country, and I think you have been on a codel with Mr. McCaul, they are teaching coding at kindergarten. So—and then once you start hitting gumnaasium, or high school, they are already going into that particular—we need something similar here.

So we need to make sure that everyone is cyber aware and savvy. So we have got to integrate cyber into all existing curricula and then we need more ninjas. We do need more very deep cyber expert work force, but we need both. I am really—and not just because I am the—we need more women, not only in STEM but in cyber.

Miss RICE. Amen to that.

Mr. CILLUFFO. Quite honestly, my students, they were the strongest, but we really do need to attract different types of students to be part of that solution set. We are just missing out on too much talent.

Miss RICE. Well, we are just starting with the whole STEM reaching out to young girls—well, not just, but, you know, within the last 5 to 10 years, and this should be added to that for sure.

Mr. CILLUFFO. At the top of that list.

Miss RICE. Yes.

Mr. Sultan.

Mr. SULTAN. I just want to add that cybersecurity trainings are incredibly difficult to accomplish successfully. What happens is that, often, people become more scared after cybersecurity training. A lot of trainers use FAIR appeals very effectively and very ineffectively a lot of times. So what happens is that the participants of these trainings become so afraid—and there is a lot of literature on how cybersecurity trainings fail—that they begin to withdraw from using the internet. They begin to withdraw from using key internet services that could enrich their own lives. And so——

Miss RICE. How do you address that issue? I mean, it is what it is. It is frightening.

Mr. SULTAN. It is frightening, but I think a lot of participants, at least those that I have interviewed and surveyed personally, fall on a spectrum of confidence and trust. If you understand where they fall on that spectrum, you can actually change it very easily.

So often at times participants can have over low confidence, low confidence that is below their actual understanding and skill level. So you can actually correct that through measures by trying to discuss with them what their cultural understanding, their background of cybersecurity is, where they get resources, how they can improve those resources, and overall improve their understanding of realistic threat assessment as opposed to exaggerating the threat assessment, which a lot of trainers do.

Miss RICE. Very interesting point. I have a lot more questions, but my time is up. Thank you.

I yield back.

Mr. RICHMOND. The gentlelady yields back.

Now the gentlewoman from Illinois is recognized for 5 minutes.

Ms. UNDERWOOD. Thank you, Mr. Chairman, and thank you all for calling today's hearing on this critically important topic.

Cybersecurity is a challenge for State and local governments across America, but the suburban and rural communities that I represent in northern Illinois don't have the resources that big cities have, and as such, are at an increased risk of cybersecurity attacks.

A city official told us that he relies heavily on informal networks with other city officials and on professional IT associations, such as GMIS International, to ensure that the city's cybersecurity needs are met.

Mr. Sultan, in your testimony, you referenced concerns for cybersecurity inequality between rural and urban or suburban communities. What steps could the Federal Government take to bridge this inequality gap?

Mr. SULTAN. The Federal Government could support local governments, understanding where the baseline is for the rural areas and especially the urban areas as well. Figure out how low-income households and how low-income communities fair in terms of their understanding and skill level on cybersecurity.

They can conduct surveys to better gauge where those populations fall, and then they can actually conduct trainings. They can actually partner with private technology companies to provide software updates to phones that are outdated. They can provide system level support. They can facilitate trainings with the private technology companies, but not to supplant the Federal Government's networks with the populations, because you don't want the private technology companies determining what those trainings look like.

So there are a host of options for the Federal and local governments to improve and understand their populations' cybersecurity needs.

Ms. UNDERWOOD. Thank you. Do you have any recommendations for rural communities that are at just the beginning stages for setting up their infrastructure? You know, the idea that a local community would even know which private company to approach is something that I think we sort-of take for granted for people that are just beginning to bolster their capabilities.

Mr. SULTAN. That is an excellent point, and I think that is where the Federal Government can play a really important role, because the Federal Government has the ability and the opportunity to connect with these private technology companies in ways that are far more realistic and centralized than local governments can.

They can also create public awareness campaigns, push them out into schools, push them out into television, on social media platforms, on radio. Because without a public awareness campaign, people aren't going to be very interested in even participating in those trainings. I had to use a lot of incentives to get vulnerable populations to even come to discuss their needs about cybersecurity. So if you offer a training, the chances are they might not appear.

Ms. UNDERWOOD. Right. Do you have any advice for local governments to better educate their communities on the appropriate personal cybersecurity best practices?

Mr. SULTAN. I think—in terms of staff?

Ms. UNDERWOOD. Uh-huh.

Mr. SULTAN. I think with staff you can improve trainings, but you can also simplify the cybersecurity documentation that they are currently working with. They are using centralized documentation that spans hundreds of pages, they are fairly dry, not very interesting, and I think you can make trainings that are more engaging. So instead of just trying to pass off a document to staff that probably have other responsibilities other than cybersecurity, they are probably responsible for IT and system infrastructure, you could focus on cybersecurity through engaging trainings. Those could be digital trainings. They don't have to be personal trainings so they can scale better.

Ms. UNDERWOOD. Chairman Richmond recently convened this committee to address the lack of diversity in our talent pipeline for the cybersecurity field. We touched on the need for gender diversity in particular. But as you know, that there is a real high number, significant number of unfilled cybersecurity jobs across the country.

So, Mr. Duffy, do you have any feedback or ideas for what Congress and the Federal Government can do to attract more skilled cybersecurity professionals, particularly from diverse backgrounds?

Mr. DUFFY. Yes. One of the things you need to do is certainly identify those individuals that may have not thought they had a talent in cybersecurity. We work closely with the SANS Institute and with the Governors around the country with something called the CyberStart Program. This is something that is basically industry funded. Twenty-six Governors participated in this past year. What the program is, the schools develop these programs or they try to identify individuals who may not have an interest in technology but have a real aptitude. So how do they go about finding those folks that have an aptitude but not the interest, and that is what the program is about.

It is the third year of the program. The first year of the program, there—shouldn't be surprised, like 85 percent of the participants were boys. So in year two, they did it for girls only because they wanted to deal with the gender issue. So this year, they have a combination. One program is for the boys and the girls, but yet a second program is just for the girls only because they are trying to work on the gender issue.

Ms. UNDERWOOD. Excellent. Well, it is my hope that as we have models like this that private industry is supporting, that we can count on the Cybersecurity and Infrastructure Security Agency to develop innovative programs to help States and local officials who don't have expertise and maybe who don't have a local private company to sponsor something in their community. This is something that is important everywhere and we want to make sure that we are properly prepared.

Thank you all so much for being here.

Thank you, Mr. Chairman, for convening this hearing. I yield back.

Mr. RICHMOND. The gentlelady from Illinois yields back.

I want to thank the witnesses for their valuable testimony and the Members for their questions.

The Members of the committee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

I would ask unanimous consent to insert into the record written testimony in today's hearing from Talib Karim of STEM4US!, Inc.

[The information follows:]

STATEMENT OF TALIB I. KARIM, CEO STEM4US!, INC.

JUNE 24, 2019

Good afternoon. My name is Talib I. Karim, and I am a co-founder and chief executive officer for STEM4US!, Inc. As background, I have spent over 2 decades working on cybersecurity and other public policy issues. This includes serving chief counsel and legislative director to Congresswoman Sheila Jackson Lee, a senior Member of the Homeland Security Committee.

STEM4US! is a non-profit organization based in Washington, DC, that works with universities, businesses, Government entities, and other non-profits to scale investments, training, and promotion of the cybersecurity and other STEM fields. Our goal is to transform the STEM workforce by creating 600,000 new cybersecurity professionals by 2030. To ensure that the STEM field reflects the rich diversity of this Nation, we aim to ensure that at least 50 percent of these new cybersecurity workers are African Americans, Latinos, and women. By focusing on diversity, we can foster creativity and offer a range of perspectives and ideas in the cybersecurity realm.

Today, several factors impede the ability of State and local governments to protect critical infrastructures from cyber attacks. Among these structural impediments are regulations at the State and local levels, limited resources, and an expanded attack surface. We wish to raise a few constructive points regarding this important topic.

First, insufficient funding and staff has been identified by members of State and local governments as one of the key barriers to effective cybersecurity. Without the necessary funding, it is difficult for State and local governments to hire the qualified cybersecurity experts necessary for providing cybersecurity protection. Cybersecurity expenditure constitutes a small percentage of the overall budget: According to a 2015 report, most State cyber budgets are between 0–2 percent of the overall IT budget. This means that governments do not have the resources or expertise necessary for a resilient cybersecurity infrastructure. Therefore, it is imperative that cybersecurity becomes a greater spending priority for governments. By addressing the lack of budgetary resources, governments will be able to hire and retain a greater number of cybersecurity personnel.

In order to achieve this goal, STEM4US! proposes what we've called the "Cybersecurity Pell Grant." Under this proposal, Congress would authorize and appropriate $1.5 billion each year, for a 10-year period to fund free cybersecurity and related training. This training would be offered at 250 Historically Black Colleges and Universities and other Minority-Serving Institutions along with community colleges and high schools. If fully funded for 10 years, the grant could create more than 600,000 new, more adequately trained American cybersecurity workers.

If our proposed legislation is enacted, the grants would support 15 weeks of cyber training. The tracks of the cyber training would include cyber defense and incident handling skills as well as drone maintenance and operations. Additionally, each training program would have the capacity to train 300 students per year in 3 cohorts—spring, fall, and summer. Therefore, through this initiative, STEM4US! would create a pipeline of talented and skilled cybersecurity workers. These newly-trained cyber workers would work for Government agencies or contractors in their respective communities. This, in turn, would create a Nation-wide network of cybersecurity personnel who would increase the resiliency of their State and local governments to cyber attacks. These grants would result in a hardening of the Nation's critical infrastructure.

Earlier this year, STEM4US! organized a fly in that allowed our stakeholders to meet with staff from this committee along other House and Senate leaders to discuss our "Cybersecurity Pell Grants" proposal. To advance this idea, we call on the Subcommittee Chair and Ranking Member to partner and both sponsor a bill that would capture this proposal.

The field of cybersecurity is one of the fastest-growing job fields in the Nation, but there is a critical shortage of qualified cybersecurity personnel. Therefore, there is a clear imperative to expand the Nation's cybersecurity workforce. Our proposed "Cybersecurity Pell Grants" would ensure that State and Federal Government agencies have an ample source of cybersecurity workers they need to protect the Nation's cybersecurity infrastructure.

STEM4US! appreciates this opportunity to provide this testimony.

Mr. RICHMOND. Without objection, the committee record should be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 4:25 p.m., the subcommittee was adjourned.]