S. Hrg. 116–451

CYBERSECURITY—2020

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

WHAT STATES, LOCALS, AND THE BUSINESS COMMUNITY SHOULD KNOW AND DO: A ROADMAP FOR EFFECTIVE CYBERSECURITY, FEBRUARY 11, 2020

EVOLVING THE U.S. CYBERSECURITY STRATEGY AND POSTURE: REVIEWING THE CYBERSPACE SOLARIUM COMMISSION REPORT, MAY 13, 2020

Available via the World Wide Web: http://www.govinfo.gov
Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE
40–972 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*
JOSEPH C. FOLIO III, *Chief Counsel*
COLLEEN E. BERNY, *Professional Staff Member*
DAVID M. WEINBERG, *Minority Staff Director*
CHRISTOPHER J. MULKINS, *Minority Senior Professional Staff Member*
JEFFREY D. ROTHBLUM, *Minority Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
THOMAS J. SPINO, *Hearing Clerk*

CONTENTS

WITNESSES

TUESDAY, FEBRUARY 11, 2020

ALPHABETICAL LIST OF WITNESSES

APPENDIX

WITNESSES

WEDNESDAY, MAY 13, 2020

Page

ALPHABETICAL LIST OF WITNESSES

APPENDIX

WHAT STATES, LOCALS, AND THE BUSINESS COMMUNITY SHOULD KNOW AND DO: A ROADMAP FOR EFFECTIVE CYBERSECURITY

TUESDAY, FEBRUARY 11, 2020

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

The Committee met, pursuant to notice, at 9:39 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Portman, Lankford, Romney, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning. This hearing will come to order. I want to thank all of our witnesses for their very thoughtful written testimony. I am looking forward to your answers to our, hopefully, thoughtful questions.

I am just going to ask that my written statement be entered into the record.[1]

I will just keep my comments brief.

This hearing really came about after I sat down with Director Krebs a couple weeks ago, and the point the Director is making to me—and I do not want to steal all of his thunder is—95 percent of ransomware and so many cyberattacks can be prevented, with just basic cyber hygiene. So I want to really talk about that.

So the bottom line and the purpose of this hearing is to—because I have always said the first line of defense in any kind of cybersecurity issues is public awareness, understanding what is out there, the sharing of threat information, which is a key role of Cybersecurity and Infrastructure Security Agency (CISA).

But, again, having read all the testimony, this ought to be pretty good. We have the Federal. We have State and local here, but we have with Ms. Crawford, a pretty relevant example of what happens when an attack occurs within a State under multiple jurisdictions. And what happened, kind of going through that case study, I think it would be extremely effective. To me, it seemed like a pretty good success story when all is said and done based on really what could have happened and how long those industries could have been shut down.

[1] The prepared statement of Senator Johnson appears in the Appendix on page 45.

So, again, just really looking to raise the profile for the public in terms of how serious these cyberattacks are, how pervasive they are, and just basic things you can do to protect yourself, and that is the main purpose of the hearing.

So, with that, I will turn it over to Senator Peters.

OPENING STATEMENT OF SENATOR PETERS[1]

Senator PETERS. Thank you, Mr. Chairman, and also thank you to all of our witnesses for coming here today.

I am especially pleased that we have Chris DeRusha with us here today. He is the Chief Security Officer for the State of Michigan and an important partner in combating cyberattacks in my home State.

Chris, I also want to congratulate you on welcoming a baby boy last month—actually 2 weeks, 2 weeks old now?

Mr. DERUSHA. That is right. About 2½ weeks.

Senator PETERS. Two and a half weeks and——

Chairman JOHNSON. He looks well rested.

Mr. DERUSHA. We are still counting days.

Senator PETERS. Still counting days.

As I mentioned to him in the back room, we were happy to give him a night last night so he could sleep the entire night when he came here to Washington. But thank you for coming and appreciate your wife allowing you to be here with us here today.

The cyber threats facing our Nation are becoming increasingly sophisticated and we are all at risk—families, government agencies, schools, small businesses, and critical infrastructure.

In today's digital world, State and local governments are responsible for safeguarding everything from election systems to very sensitive personal data, including Social Security numbers, credit card information, and of course, medical records.

State and local governments do not always have the tools, unfortunately, to defend against cyberattacks. Financial constraints, workforce challenges, and outdated equipment, I know are all serious challenges for States and cities.

Attackers always look for the weakest link, and that is why we must ensure that everyone from small businesses to our State and local governments have the tools that they need to prevent, detect, and to respond to cyberattacks.

That is why I introduced common sense, bipartisan legislation with my colleagues on this Committee to help bolster our cybersecurity defenses at all levels of government.

I introduced the bipartisan DOTGOV Act with Chairman Johnson and Senator Lankford to help State and local governments transition to a more trusted and secure dot-gov domain.

I also introduced the State and Local Government Cybersecurity Act with Senator Portman. This will help the Department of Homeland Security (DHS) share timely information, deliver training and resources, and provide technical assistance on cybersecurity threats, vulnerabilities, and breaches in States and localities.

In 2016, in my home State of Michigan, hackers used a ransomware attack on the Lansing Board of Water and Light, forc-

[1] The prepared statement of Senator Peters appear in Appendix on page 46.

ing taxpayers to pay a $25,000 ransom to unlock the targeted computer systems. My bill would give cities and States the tools to prevent and respond to these kinds of attacks more effectively.

Recently, Richmond Community Schools in Michigan were closed for a week due to a similar attack demanding a $10,000 payment. Luckily, their data was not compromised, but this attack exposes a dangerous vulnerability as schools maintain a considerable amount of sensitive records related to their students and employees, including family records, medical histories, and employment information.

I introduced the K–12 Cybersecurity Act with Senator Scott to protect students and their data by providing better cybersecurity resources and information to K–12 Schools in Michigan and well as across the Country.

It is clear that these kinds of attacks are only growing and that they pose a serious risk, and I will continue working to ensure that all of our State and local governments have the resources, information, and expertise that they need. I will keep working with my colleagues on this important issue, and you can see that this Committee is very active in this issue as well.

I look forward to hearing your testimony as to how we can continue these important efforts.

Thank you again.

Chairman JOHNSON. Thank you, Senator Peters.

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

Mr. KREBS. I do.

Ms. CRAWFORD. I do.

Mr. DERUSHA. I do.

Chairman JOHNSON. You may be seated.

Our first witness is Christopher Krebs. Mr. Krebs is the Director of the Cybersecurity Infrastructure Security Agency at the U.S. Department of Homeland Security. Previously, Mr. Krebs worked within DHS as the Senior Advisor to the Assistant Secretary for Infrastructure Protection and helped establish a number of national risk management programs.

Prior to joining DHS, Mr. Krebs was the Director of Cybersecurity Policy for Microsoft, leading their work on cybersecurity and technology issues. Mr. Krebs.

TESTIMONY OF THE HONORABLE CHRISTOPHER C. KREBS,[1] DIRECTOR, CYBERSECURITY INFRASTRUCTURE SECURITY AGENCY, DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairman Johnson, Ranking Member Peters, and Members of the Committee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's support to State, local, tribal, and territorial (SLTT) partners and the private sector to mitigate a broad range of cyber threats.

Today I would like to discuss how we at CISA see the current cyber landscape, how we are posed to assist State and local govern-

[1] The prepared statement of Mr. Krebs appear in the Appendix on page 48.

ments, and where we need to go to be most effective. This perspective is informed by events and experiences over the last several years, some successful and others representing humbling moments where we did not quite get it right.

It is important to start by understanding CISA's role. We work with partners across all levels of the government and the private sector to defend today and secure tomorrow.

We are the Nation's risk advisor, providing information and resources to our partners on a voluntary basis so that they make more informed risk management decisions. This approach embraces a sense of shared responsibility across all levels of government and industry and reflects the reality that the landscape, the Nation's critical infrastructure, is primarily owned and operated not by the Federal Government, but by our partners in industry and State and local government.

This distributed landscape is further complicated by a range of issues, including inadequate governance structures, workforce challenges, insufficient resources to maintain networks, outdated technologies, and new technologies maybe we do not really understand.

Unfortunately, these dynamics converge to provide an attractive playing field for a range of threat actors. The headlines tend to focus on the advanced threats posed by State-sponsored cyber actors like China, Russia, Iran, and North Korea.

Just yesterday, the Department of Justice (DOJ) indicted Chinese actors for the Equifax hack. Earlier in the year, increased tensions with Iran led to headlines of imminent cyberattacks on all manner of our Nation's infrastructure, and then there is Russia, Russia's efforts to interfere with our elections and target energy systems.

And yet there is a strong argument that the more pressing threat, the threat that the average American will most likely encounter comes from criminals in the form of ransomware.

According to a recent report from EMSISOFT in 2019, ransomware attacks impacted at least 966 government agencies, educational institutions, and health care providers at a potential cost of $7.5 billion.

What is even more concerning, these statistics are based on what we know. We suspect that the majority of ransomware attacks are not reported to law enforcement or CISA. It is clear that victims are paying, and as they pay, ransomware crews are getting better. In other words, ransomware is a business, and business is good.

We have been working to get a better understanding of the broad range of risks and seeking to find a common set of threads across the threat actors alongside easy-to-understand and achievable defensive measures.

In part, we want to demystify cybersecurity so that the entire team from the Chief Executive Officer (CEO) down, not just CISA, not only understand but are an active part of the defense. In many cases, it is doing the basics like good vulnerability management, using multifactor authentication and managing administrative privileges, offline backups, and having and testing an incident response plan.

But even doing the basics can be hard in today's massive dynamic networks. The point is not 100 percent security. It is to

make it harder for the bad guys to gain a foothold and then move around.

All that said, the steps we have taken thus far have not done enough to meaningfully change the dynamics, particularly with ransomware. There is more that we can do, starting with improving our collective defense posture. We have to continue increasing awareness of the risks and sharing best practices.

We also must make it easier for our State and local partners to work with us in the Federal Government. In part, that is by deploying additional dedicated risk advisors, State coordinators to the field with clear expectations on what services or assistance to expect from the Federal Government and what our State or industry partners need to have in-house or contracted.

We also have to bring more value to our partners by listening and learning to what it is they actually need. Here, the Federal Government can truly shine by developing and deploying scalable capabilities, like our cyber hygiene scanning and remote capabilities, like remote penetration testing, as well as training and exercises, like our recently released ransomware Tabletop Exercise in a Box.

I recognize and appreciate the Committee's strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on.

We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

Chairman JOHNSON. Thank you, Director Krebs.

Our next witness is Amanda Crawford. Ms. Crawford is the Executive Director of the Texas Department of Information Resources (DIR). In this role, she is responsible for implementing the State's technology strategy and defending its technology infrastructure.

Before leading the Department of Information Resources, Ms. Crawford served in multiple positions at the Office of the Attorney General of Texas, including the Deputy Attorney General for Administration and General Counsel (GC). Ms. Crawford.

TESTIMONY OF AMANDA CRAWFORD,[1] EXECUTIVE DIRECTOR, DEPARTMENT OF INFORMATION RESOURCES, STATE OF TEXAS

Ms. CRAWFORD. Thank you, Chairman Johnson, Ranking Member Peters, and Members. My name is Amanda Crawford. I serve as Executive Director for the Texas Department of——

As Chairman Johnson said, I am Amanda Crawford, Executive Director of the Texas Department of Information Resources. Thank you for inviting me to testify on this important topic here today.

Our mission at DIR is to serve Texas Government by leading the State's technology strategy, protecting State technology infrastructure, and offering innovative and cost-effective solutions for all levels of government.

[1] The prepared statement of Ms. Crawford appears in the Appendix on page 54.

Today I will provide the Committee with an overview of the August 2019 Texas ransomware attack and recommendations for how Texas can benefit from greater Federal resources in the future.

State preparation and cooperation were the keys to our successful response in the August ransomware incident. On Friday, August 16, at 8:36 a.m., DIR was notified that eight local governments had been simultaneously attacked by the same ransomware event. At 10:30 a.m., it was reported to me that there were now 19 impacted entities, and the attack had compromised a municipal water system.

At that point, I notified the Office of the Governor, and shortly thereafter, Governor Abbott issued the State of Texas' first statewide disaster declaration for a cyber event. That disaster declaration activated the State Operations Center (SOC) to 24/7 operations.

As you know, things went smoothly from there with DIR leading the incident response effort in partnership with six State agencies, private vendors, the Federal Bureau of Investigation (FBI), DHS, and the Federal Emergency Management Agency (FEMA). All involved should be proud that one week after the incident began, all 23 impacted entities were remediated to the point that State support was no longer needed, and no ransom was paid.

This success can be attributed to the extensive preparation at the State level and cooperation between the responders. These preparations included State legislation that added a cyber event to the definition of a disaster, a frequently tested cybersecurity annex to the State Emergency Management Plan, and a pre-negotiated managed security services contract that is available to all levels of Texas government to prepare for and respond to cyber events.

While Texas is proud of the success and the timeliness of how this event was handled, we must focus on the future. The threat landscape of cybersecurity is ever evolving, and we cannot be caught only able to handle yesterday's battles.

Additionally, we must now focus on the scope of the attack. In August, the managed information technology (IT) service provider that was attacked was small enough that even if all of its clients had been compromised, the response model that we had in place would have worked, but if the numbers had been three or four times greater, the model would have been stretched beyond its design.

In order to prepare for tomorrow's threats, we need additional resources at both the State and Federal level. A few recommendations would be, one, better sharing of classified information with State government. If Texas and other States do not have greater awareness of threats, which could affect us, we cannot be effective in stopping them.

Two, increasing CISA resources per region. One person to deal with close to 9 percent of the United States population and the world's tenth largest economy is simply not sufficient.

Three, clearly communicating what Federal resources are available to State and local governments. This information needs to be plainly articulated and shared with State and local governments, long before we are in the midst of a crisis. A single Federal point of contact for cyber events would be invaluable.

Four, balancing the law enforcement need to protect investigations with the ability to share information about active threats. Having spent nearly 20 years in the Texas Attorney General's office, I am very familiar with law enforcement and the need to protect sensitive investigation information. However, we need to change the default setting in these cyber situations from what can we share to what must we not share. We are appreciative of the partnership with the FBI and would ask that they review whether more information could be released.

Five, expand resources at DHS to shorten wait times for their voluntary services. Due to the popularity of some of CISA's very valuable services, the wait times can be a minimum of 18 months. In cybersecurity, 18 months represents a full generation of change and advancement.

And, six, expanding event notification from Multi-State Information Sharing and Analysis Center (MS–ISAC). MS–ISAC is a valuable partner for Texas' cybersecurity program. Frequently, however, MS–ISAC will not inform us at DIR when an incident has occurred at a Texas local government entity. This puts the State and local governments at a disadvantage from a response recovery or prevention perspective. Old news or partial news does not equip State and local governments for responding effectively to these cyberattacks.

In summary, DHS and MS–ISAC provide very valuable information and services to Texas when it comes to protecting its critical assets and information. While improvements can be made, we are engaged in a continuing dialogue with both organizations to evolve the services and the information we both share.

Texas stands ready to assist in the continuing effort to enhance the security of our Nation's assets and provide input when needed.

I want to again thank the Committee for inviting me here to share our perspective with you and look forward to any questions you might have.

Chairman JOHNSON. Thank you, Ms. Crawford. I can tell by some of the reactions of Director Krebs, he liked some of your recommendations, probably all of them.

Our final witness is Christopher DeRusha. Mr. DeRusha is the Chief Security Officer for the State of Michigan. Previously, he led Ford Motor Company's Enterprise Vulnerability Management and Application Security Program. Mr. DeRusha also served in the Obama Administration as a Senior Cybersecurity Advisor at the Office of Management and Budget (OMB), as an Advisor to the Deputy Undersecretary for Cybersecurity at DHS. Mr. DeRusha.

TESTIMONY OF CHRISTOPHER DeRUSHA,[1] CHIEF SECURITY OFFICER, CYBERSECURITY AND INFRASTRUCTURE PROTECTION OFFICE, STATE OF MICHIGAN

Mr. DERUSHA. Thank you, Chairman Johnson, Senator Peters, and other Committee Members for inviting me to testify today.

As the Chief Security Officer for the State of Michigan, I am excited for this opportunity to highlight the steps we are taking to

[1] The prepared statement of Mr. DeRusha appears in the Appendix on page 65.

better secure our State, but also to discuss some of the enduring challenges that we face at the State and local level nationally.

It is no surprise to the Members of this Committee that the thread environment we face is, in a word, daunting. Attacks on government organizations at all levels continue to rise and demonstrate the ever-expanding resources and skills of our adversaries.

One small example, at the State of Michigan, our firewalls repel over 90 million potientially malicious probes and intrusion attempts every day, and we are far from unique.

I would like to start by providing a brief overview of our efforts at the State level in Michigan. For over a decade now, State-level IT and cybersecurity have been centralized under one agency, the Department of Technology, Management, and Budget. Centralization has enabled the State to enforce common security policies, standards, controls across agencies and leverage economies of scale when we are procuring new technology.

Some successes we have had as a result are standardized risk assessment and security accreditation process for all new systems that come into the State; the ability to apply IT governance and enforce security policies at all of the State agencies; mandatory cyber awareness training and phishing exercises, a common operating picture of threats that we face for the entire State enterprise; and the ability to act with command and control when we respond to incidents.

In Michigan, we work as a team across several organizations with cybersecurity responsibilities, which have been formally delineated in a Cyber Destruction Response Plan. Michigan Cyber Security (MCS), within my group, hosts a Cybersecurity Operations Center with advanced capabilities such as threat hunting, incident response, forensics, and vulnerability management.

Michigan State Police's (MSPs) Michigan Cyber Command investigates computer-based crimes and coordinates cyber emergencies across the State. Where Department of Technology, Management, and Budget (DTMB) is primarily focused on protecting State-level agencies, Michigan State Police works across the State to protect all.

And Michigan is also fortunate to have both Air and Army National Guard units in the State. We work closely with our colleagues in the Guard to formalize our coordination in times of emergency through joint interactions and exercises.

While a close working relationship with DTMB, State Police, and National Guard is essential, another key relationship we have is with DHS's CISA. Michigan is fortunate enough to have a cybersecurity liaison dedicated to our State. By having that direct line to DHS, we are able to incorporate Federal Government threat information into our decisions and streamline access to the Federal expertise and resources.

To that end, the Cybersecurity State Coordinator Act would be a major asset to State and national cybersecurity efforts by ensuring greater continuity between efforts of State and Federal Government, but it would also provide a stronger State voice within CISA, helping them better tailor their assistance to States and localities who have widely varying levels of maturity and needs.

The State and Local Government Cybersecurity Act, Senate Bill 1846, would help States like Michigan access resources, tools, training, and expertise developed by our Federal partners and national security experts.

So I want to sincerely thank both the Chairman and Ranking Member and the numerous Members of this Committee for their bipartisan leadership on these pieces of legislation. The State of Michigan fully supports these efforts in seeing both bills enacted into law.

I would like to wrap up my remarks by highlighting the needs and challenges of our local government partners. Governments at the Federal, State, and local level interact with each other digitally every day. So this interdependency means that improving the security of any of these levels of government requires enhancing security for all.

As much as State governments face shortages of human and financial resources, they are far more scarce for local government. Of Michigan's 83 counties, we are home to approximately 10 million residents, and only three of these counties have uniquely designated chief information security officers. Even their websites face legitimacy challenges as less than 10 percent use the dot-gov domain, opting instead for the easier-to-obtain dot-com, dot-net, or dot-org domains.

The DOTGOV would seek to ease the process for these governments to obtain dot-gov domain names, providing sites themselves with greater security, and offering greater assurances to residents that they are, in fact, looking at a government website. This act is an important step in the right direction, and I am very hopeful this will be enacted into law.

The State of Michigan has also been proactive in developing innovative ways to provide support to county and local governments. In 2018, our Chief Information Security Officer (CISO)-as-a-Service initiative leveraged a centralized pool of cybersecurity experts to advise a pilot group of counties on their security posture and provide an improvement roadmaps. While that benefited those 13 pilot participants, we have over 1,600 local government networks to secure, to work to secure in the State.

So a successor program, Cyber Partners, is trying to pull together a more scalable model to help all counties and local governments.

We are piloting a new initiative that would assess risk posture against the CIS top 20 critical controls, develop prioritized improvement plans for each local entity, and potentially provide additional consultative and managed security service on the back end. This work has been essential to State and county as we prepare for the upcoming 2020 elections as well.

In addition to helping counties and localities improve their defensive postures, Michigan is also taking steps to help them respond to incidents when they do occur. We have the innovative Michigan Cyber Civilian Corps, which is an organization of highly qualified cybersecurity professionals that have volunteered their skills to respond to incidents at critical infrastructure, county, or local government organizations. Currently, 100-plus members, strong and

growing, the group has worked alongside Michigan State Police to help numerous organizations respond to significant compromises.

In closing, our Country's State and local governments are on the frontlines of digital conflict, attacked daily by highly resourced, advanced, persistent threats, and there remains a great deal of work to do to protect the networks we rely on to provide essential services to our Nation's public.

The State of Michigan greatly appreciates the attention paid to this issue by the Members of this Committee, and we look forward to continuing to work with you to secure our critical infrastructure and protect our residents.

Chairman JOHNSON. Thank you, Mr. DeRusha.

I am going to start today. Normally, I kind of defer, but I want to kind of set the tone a little bit.

When I first got here in 2011, that was really when we started seeing some of these big cyberattacks. I cannot remember the exact timing, but when I got here, everybody said we got to do something about cybersecurity.

So when I was sitting over there on the Committee, I would always ask the question: What are the top few things we need to do?

It was always very consistent. The first thing was information sharing, which I think we have come a long ways toward achieving. It is far from perfect, but I think DHS has been recognized as sort of the hub in Federal Government to do it. The other one was a data breach notice, some kind of national preemptive policy.

So, silly me, I thought, well, these ought to be two pretty simple things to accomplish. Nothing could have been further from the truth in terms of data breach for a host of reasons.

Mr. Krebs, real quick, on a scale of zero to 100, we have done nothing to we are at perfection, how far down that road in terms of government and private-sector awareness and defense are we? I realize this is very subjective, but I want a little comfort that we are actually improving. Where were we in 2011?

Mr. KREBS. 2011, from a State and local perspective, even a Federal Government perspective, closer to that kind of zero side. I think we are now maybe about halfway across that spectrum.

One thing I would point to is last year's RSA conference. Every year, it has a theme. Last year's conference theme was to work better, which I take as yes. They are across the C–Suite, across the leadership ranks. We are getting more awareness. That is really the key. It is that leadership is paying attention, is investing, not just the CEO, but the boards, the general counsels. Why is that important? Because awareness at the leadership ranks leads to investment, which builds capabilities.

You cannot have any of those second-or third-rank items without awareness. Awareness takes time, and it takes steady, constant engagement. It will not happen overnight. This will not be fixed next year. This will take years and years and years to continue to get out there and engage.

Chairman JOHNSON. But the beauty about cyber defenses is they really can be—you do not have to build a fence. I mean, you can literally, with the speed of light, where people are prepared, you can understand a threat signature and put up the defense, correct?

Mr. KREBS. That is one aspect of defense. It is layered defense.

We have developed a set of recommendations called "Cyber Essentials," and basically, we have broken it down into the key attributes of success for any effective cybersecurity program. It has a strategic element, a technical element, and a tactical element.

The strategic element, it starts at the top. You have to have leadership, buy-in. You also have to have a security culture across the organization where everybody is a part of it, where people are not at the end point clicking on bad links.

The second piece, the technical piece, is about asset management, good governance across the organization, but also identity management where you are limiting the ability of people to make certain changes across their environment, and then managing.

The last piece, as the way I see it right now, is the most important. You have to have a good incident response plan that you test, and you have to have recoverable backups, and you test them as well. That is what is so critical right now in ransomware, and that is why Director Crawford was so successful across the State of Texas. They had a plan, and they had recoverable backups.

Chairman JOHNSON. So we obviously deal with FEMA as well, and the basic model is the local governments are the first responders. When they are overwhelmed, they call on the State. When the State is overwhelmed, it calls in the National Government.

But FEMA on a national level, Federal Government, is certainly helping, prior to any incident, State and local governments prepare. I view that as the exact same model within CISA.

And it is just not like you are going to come—and we can talk about this later with what happened in Texas. It is not like DHS is going to come and solve your problem. It is about making awareness. It is about setting you up for success if something were to happen, but in the end, it is the individual. It is the enterprise at the State or local government that is going to have to respond and fix this themselves, correct?

Mr. KREBS. Yeah, that is right.

Chairman JOHNSON. With help from——

Mr. KREBS. In fact, the National Cybersecurity Incident Response Plan (NCIRP) is the cyber annex to the National Response Framework (NRF), which FEMA maintains.

I am pushing my team into a position where our advisors are more along the lines of the National Incident Management Assistance Team (IMAT), where we come in, and we are not hands on keyboard recovering the networks of Texas and the individual counties, because we do not know those networks. They have resources in place. Your Managed Security Service Providers Service Level Agreements (MSSP SLA) is a perfect example of the things that need to happen at the State level, but we can come in and say, "Here is what a good incident response plan looks like. Here is how you should prioritize a roadmap to recovery, and oh, yeah," when she is getting hit up by about 50 different vendors, "Here is what you need right now. Here is how to sort through some of that.

Chairman JOHNSON. But I think it is extremely important that we kind of understand what the Federal Government's role is and respond accordingly, so you can set up the system, so you are prepared, so you do not expect the Federal Government to come in and

say, "Here, we are going to solve all your problems," once a disaster hits.

The last point I want to make, reading through the testimony, obviously we are really focused on State, local, territorial, tribal governments. We are concerned about enterprise, the critical infrastructure.

What is not really being covered, but I think the vast majority of Americans are concerned about, is their own cybersecurity. Ransomware attacks on individuals, I realize those are not going to be as profitable, because the fact that a big company can pay you millions, an individual maybe can only scratch up a couple hundred bucks.

But I do want to, as you are responding to these to her questions from other Senators, kind of keep in mind the individual, and I will just ask the question right now. We all use our devices. These things, if you are tied into Wi-Fi, you are plugged in. They automatically back up every couple weeks. They back up to the cloud. Is that adequate? Can ransomware, if attacked on a device, even though you have backed that thing up, is that an adequate backup or not?

So if you can just quickly drill down a little bit in terms of individual cybersecurity, what we are doing, what individuals need to know.

Mr. KREBS. The more pervasive ransomware crews right now are focused on Windows-based systems across enterprises. Are there malware capabilities across personal devices? Yes, but as long as you have a modern device and keep the software updated, then you are generally OK as long as you also do not click on bad links and email go to sketchy websites, click on random text messages from people you do not know. There are things that the individual can do.

The backup to the cloud is always a good idea, particularly, again, these enterprise clouds provided by the manufacturer.

Chairman JOHNSON. That is an effective backup. Once every 2 weeks, I mean, your photos, those things, your information is being backed up effectively, and even if you do suffer a ransomware attack, you should be able to recover.

Mr. KREBS. Generally speaking.

Chairman JOHNSON. Generally.

Mr. KREBS. Ransomware across individuals is not quite as—particularly in this iOS devices and the android devices, it is not quite as persistent or pervasive as you would see in the enterprise environment.

Chairman JOHNSON. OK. Appreciate that. Senator Peters?.

Senator PETERS. Thank you, Mr. Chairman.

Dr. Krebs, you mentioned in your opening comments, the list of foreign actors that are very sophisticated, that have been attacking us, including the Chinese attack on Equifax. Certainly, we are worrying about the election, potential interference again from the Russians.

But we just had a major incident that heightened everybody's awareness, and that was after the Iranian attack. There was a very higher threat level associated with, perhaps, Iranian retaliatory cyberattacks.

So can you give me an assessment of how the reaction—looking back now in an after-action? Because we went through that. Luckily, nothing happened, to our knowledge, but is there a gap that we need to be aware of in terms of our response from the Federal level and there is a way for this Committee to help you fill that gap?

Mr. KREBS. So the way I see it, the Department of Homeland Security in 2003 was established to do two things, at least my part of the organization, bring people together quickly and share information rapidly.

When I look back at what we did in the wake of the Soleimani strike on a Friday, we rapidly pulled together a broad group of stakeholders and shared information about what we knew about the event and how we were thinking about the next few weeks or two and then the things that organizations should do. We held three calls: Friday afterwards, the next Tuesday, and then the following Friday.

The first call, we had 1,700 connections on the line, and then the following Tuesday, we had 5,900 connections on the line. The following Friday, we had 5,400 connections.

In fact, I heard from an individual. I was down in Texas a couple weeks ago, and I heard that the CISO, the city of Dallas was on the line.

So these are the sorts of things that we know we can get out there and reach thousands, if not tens of thousands of people quickly, and share information and products.

I think some of the feedback we got is that the products we sent out, including one we sent out on Monday, that was a—used the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework of techniques that the adversary uses aligned against detections and mitigations that would be effective across a network. Those are the sorts of things that we want to continue to push out.

But, again, we pulled rapidly a broad group of stakeholders together, got them information that they could use.

Going forward, I have to have a better playbook in hand. So we have done an after-action process. We have developed that playbook. We also have to get more resources out in the field. I cannot be effective if I am sitting here in Washington, DC. I need more dedicated State and local resources.

The Cyber Coordinator Act, I think, would help us get along that way. One of the things I want to make sure I have is a State and local dedicated resource in every State Capitol. I am under-invested in cyber advisors. I have to get more resources out in the field, again, not hands on keyboard. We do not rebuild networks, but advising, helping build incident response plans, extracting best practices from Texas, from Louisiana, and then helping other States understand what they need to do as well.

Senator PETERS. Thank you.

I am going to ask our two other witnesses to give your assessment after hearing about the information going out after the Soleimani attack.

Mr. DeRusha, first off, did you get information quickly from the Federal Government? Was it adequate? What more would you have

liked to have seen, and what additional resources would you need to bring to bear in order to make it more effective? You can answer kind of broadly and then Ms. Crawford afterwards.

Mr. DERUSHA. Senator, we did get information right away. Chris actually hosted a call sort of immediately and got a lot of stakeholders together, and even though there was not a lot to share yet, even saying that and letting us know that they were on it, thinking about us out in the State and local critical infrastructure, it was very helpful. Then in the ensuing days, we would get updates on what was known, products from the past on known techniques and procedures that that adversary uses, so that we can ensure that we are protecting ourselves and make sure everybody had that information. So I think that DHS did everything that they could to move fast and share information.

I think one of the things we have been talking about here is we have discussed the Federal role, which is largely a support role. You have and run an operator network. You are responsible for it. What is interesting is across the Country, we are figuring out the State role. There are a lot of innovation going on.

We have a saying in our community, "If you have seen one State, you have seen one State," and we are trying to determine, within each State, how does that model work, which is why we need these DHS cybersecurity advisors dedicated to each State to help us tailor specific plans to our needs, which are quite varying.

The one thing I would say is that the local government and critical infrastructure, municipal-owned critical infrastructure particularly, they need enduring support.

As Chris said, DHS can come in and help respond to an incident, but to reconstitute a network and ensure those essential services continue to get delivered, that is where we are really focusing. I look forward to talking more about efforts that we have under way in our State today.

Senator PETERS. Great. Thank you. Ms. Crawford.

Ms. CRAWFORD. I would absolutely agree with Chris' assessment on the information that the States received relating to the Iranian event. It was extremely helpful. It was very timely. It was detailed.

In fact, I know in Texas, we participated in the calls, and we also—I mean, we could not have written a more informative document and shared it on our own website to get out to our customers at the State and local level on that.

If anything, really I would say that that was—and that is what I alluded to in my earlier comments about that ongoing dialogue and this—I do not want to say lessons learned as much. It is just this is a new space, and that although, as you mentioned, the cybersecurity issue, sir, is not new, it is becoming more prevalent. And if anything else, it is getting more attention. So leadership is becoming aware.

Because it is that new space, we are all adapting to it, and we are all evolving and trying to figure out what this new normal, unfortunately, looks like. So the information we received on that latest event was extremely helpful when it came to that.

Then as far as future resources, one of the things, again, it is that threat-sharing information, that it is timely, and that it is complete. One of the things that we look at—and I think the dedi-

cated resources that is tailored to each individual State would be very helpful. Texas is unique, and building on Chris' comment, everyone is going to have a different structure. Every State will have a different structure and different maturity. So having a resource that understands the constraints within those States as far as security would be helpful.

I think the other thing is trying to navigate, particularly in the midst of a crisis, what resources are available. Looking back to the August incident, really it was a matter of expectation-setting and understanding what exactly are the services that the Federal Government can offer, who offers them.

We had multiple Federal partners, and depending on the type of event, you may, in fact, reach out to maybe Secret Service. Maybe it is FBI. Maybe it is DHS. There are a lot of different players, and I say this, working in government and knowing that we are not always easy to understand and understand who does what and what agency handles everything. So I am speaking from experience that I know that on a State level, we work really hard to try to improve our communications to our constituents and our agency customers on what services we can offer.

So I think just that expectation-setting and understanding a clear playbook of what we can look for would be really helpful.

Senator PETERS. Great. Thank you.

Chairman JOHNSON. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you, Mr. Chair and Ranking Members Peters for having this hearing. Thank you, all three of you, for being here today and for your service.

I want to start, Director Krebs, with just following up on a little bit of the discussion we have already had. Your agency obviously has an enormously important and complex mission, and I want to thank you for all the hard work that you and your entire staff is doing.

As we have all heard today, cyberthreats against State and local entities are dramatically increasing. Across the Nation, cities and States have suffered from debilitating ransomware attacks that are carried out to extort public funds.

State and local governments, as our State witnesses have made clear today, often struggle both with a lack of available resources and with knowing where in the disjointed Federal bureaucracy to turn to for guidance and assistance.

You have talked a little bit about the Cybersecurity State Coordinator Act. I am glad we have been able to introduce that on a bipartisan basis. Maybe you can expand a little on why that is so important and also what your agency is doing to ensure that State and local entities have clarity as to where in the Federal Government to turn to for help and how are you seeking to improve the relationship.

Mr. KREBS. Yes, ma'am. Thank you for the question. We have already talked a little bit about FEMA and how incident response happens, which is a useful framing for the conversation, particularly when you think about how my agency, CISA, and the predecessor organization, National Protection and Programs Directorate

(NPPD)—I have thankfully forgotten what NPDD stands for. But you have to think about how the organization was built; first and foremost, Federal network security.

Senator HASSAN. Right.

Mr. KREBS. Second, significant cyber incidents. Significant cyber incidents are those that pose a significant national security threat or economic security threat.

We were not built and staffed and resourced to have significant support to the State and local governments. That just was not in the playing cards.

Over the last 18 months to 2 years, however, I have particularly with an increase of two things—first, ransomware, but probably, more obviously, election security. We have had to build out our ability to engage at the State and local level, and as Director Crawford mentioned, one of the most important aspects of all this is understanding that every State is different, that the laws are different. Home rule, for instance, makes it a challenge sometimes for engaging, but that is going to require me pushing force out from D.C. into the field again. So what we have to start with is additional resources out in the field, No. 1.

No. 2, I have a decade-plus of significant investment in Federal network security. What we have to do is put a little bit more on top of that to extract insights, best practices and lessons learned, that then we can shift and share with our State and local partners. When you think about the 99 Federal agencies that comprise the civilian Executive Branch, it is one of, effectively, the largest networks in the world.

Senator HASSAN. Right.

Mr. KREBS. The investments in security makes it one of the largest line items for IT security.

There is a lot of goodness that we can take out of there, and I have also pressed the team to think more about not just securing the networks, but what can we pull out of the efforts we put to secure the networks to share with State and local partners. So when we issue binding operational directives or emergency directives, we have to not just focus on the Federal networks, but developing implementation guidance and additional documentation that a State or local partner could immediately pick up and run with and down the road need to have concierge-like service to help them understand what we are doing and how they can do it as well.

Again, this takes time. We need to build out the force but also put the insights piece on top of existing investments.

Senator HASSAN. Well, thank you. That is helpful.

I also wanted to follow up with you on a letter that Senators Peters and Schumer and I sent concerning the Multi-State Information Sharing and Analysis Centers. They are an important tool for Federal, State, and local governments to share cybersecurity information with each other, and last fall, as you know, I sent you a letter along with Senators Schumer and Peters asking your agency to ensure that MS–ISACs have adequate funding.

I believe you have some good news to share regarding funding for the MS–ISAC, and can you shed some light on that for us?

Mr. KREBS. Yes, ma'am. So, first, yes, they are fully funded. I think in the fiscal year (FY) budget, we are talking about a base

of $11.5 million with an additional 10 on top. So we will be supporting the MS–ISAC.

The MS–ISAC, as you have already heard, is one of our key mechanisms for broadly engaging State and locals and also is the home of the Election Infrastructure Information Sharing and Analysis Center (EI–ISAC) as well.

But we are not stopping with the Albert sensors and the information-sharing mechanisms. We are also trying to understand what additional capabilities can we build out down the road. There are a number of pilots that we have ongoing; in particular, one that I am excited about, an endpoint detection response capability. So how can we help push out additional capabilities to the field to get the baseline of security up? A lot of what we talked about, the basics, we think we can buy. The Federal Government has significant advantage in terms of negotiation and contracting leverage. How can we bring that to the advantage of our State and local partners?

Senator HASSAN. Thank you very much for that, and thanks for making sure that the funding was there.

I want to turn to our State experts here. Ms. Crawford, much like Texas, New Hampshire entities have experienced ransomware attacks. Last year, Strafford County and the Sunapee School District were targets of malicious hackers. Luckily, in both cases, quick-thinking professionals spotted the attacks in progress and acted to limit their effects.

In Strafford County's case, despite a temporary inconvenience, the county was able to continue operations because they had trained and prepared for this type of emergency.

So if both of you can just touch on—I will start with you, Ms. Crawford. What kind of training exercise and resiliency plans would have helped cities and counties in Texas better prevent and respond to cyberattacks like the one you saw in August?

Ms. CRAWFORD. I think really, again, going back to the theme of awareness and education.

Senator HASSAN. Yes.

Ms. CRAWFORD. So one piece of State legislation that I am particularly excited about that passed last session in Texas is our House Bill 3834 that requires mandatory cybersecurity training on an annual basis for every public employee and official in the State, and to us, that is key. Cybersecurity is everyone's responsibility, which if we could have it tattooed on my forehead, then we certainly would.

But we want to make sure that people understand that and that they get that information out there. So those training exercises we are actually partnering with CISA on the Tabletop Exercise in a Box at our State Information Security Forum, where we pull State security professionals from around the State. It is coming up in March in Austin, and we will be doing that. So that is the key issue there, I think, is the education and training.

What we really see out there particularly with the local governments is we have extremely limited resources, and whether those resources are trained and skilled workers, whether it is funding, there are issues for the local governments that really put them at a disadvantage.

Senator HASSAN. Right.

Ms. CRAWFORD. And so they are frequently going out to managed service providers, where you may or may not be getting the best services that are out there and particularly in Texas when we are looking at when we are spread out over such a large geographical area. We have network issues, broadband-to-rural issues, all sorts of things that are very difficult, just it is a different threat landscape.

Senator HASSAN. OK. Thank you, and I realize I am well over time. So, Mr. DeRusha, I will follow up with you, but I was very interested in your reference to a Civilian Cyber Corps. And that is something that my office will follow up with you about because, again, I assume you agree with a lot of what Ms. Crawford just had to say but would love to learn more about what Michigan in particular is doing. Thank you.

Chairman JOHNSON. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you, Mr. Chairman, and thank you, all of you, for your testimony.

Our State's Chief Information Officer (CIO) and the folks that are in Oklahoma are doing a fantastic job. Thanks for engaging in this.

Chris, thanks for all your work at CISA. You have been a terrific asset to us, keeping us up to speed on things that you see and trying to help us. The information that you put online on the website has been very helpful. We have recommended it to quite a few folks after the Soleimani response that we had. We had excellent briefings from your team. I was able to take that information and to be able to do a large conference call in Oklahoma with State and local leaders, with businesses, infrastructure folks, be able to pass on that same information, and for them to be able to double that out. So it is not only the thousands of people you are talking with, but the people then multiple that message back out from there. It is very helpful. So we appreciate your engagement on those things.

Let me bring up a couple of things that we have talked about before. That is election security. It is a concern. It is a major focus of your office. Obviously, as we are focusing in on what is happening now, everyone is paying attention to Iowa and the debacle there or the apps and all those things there. That is not really the cyber election issue that we have. It is really an outward threat coming at us or someone internal being a threat to our systems as well.

So let me outline a couple of concerns that I have, and I would like to hear more of what you are doing.

In 2018, Congress passed $380 million in election security assistance grant money to the States. As of the end of last year, States have spent a total of $92 million of that $380 million allocated to them. About 24 percent of the money that we allocated in 2018, they still have not spent by the end of 2019. We just allocated another $425 million back to those States against, which certainly will not be out the door because they have not even gotten the money out the door from 2018 yet still.

So, with this, there is not a real change in hardware or software because the States are sitting on the money rather than actually

spending the money to improve their structure on election security. What is your office doing to be able to help us in the election security footprint right now?

Mr. KREBS. So specific to the Help America Vote Act (HAVA) funding, the 700-so-odd million, I would not focus too much on the percentages that were spent, particularly the 380 and the 425, and I think my partners here might be better witnesses to answer to that.

But what I understand is spending money at the State government level is really hard.

Senator LANKFORD. Right.

Mr. KREBS. It does not just flow out the door.

The additional thing is I would rather they spend the money right than just spend it.

Senator LANKFORD. I would agree.

Mr. KREBS. This is taxpayers' dollars, and it is multiyear money. So when you are talking about hiring in some cases, which we have incurred cyber navigators, I think some of the money is 5-year money. So they have to account and obligate salaries for multiple years.

Senator LANKFORD. Some of the States that I have talked to that have not spent the money out have said they are interacting with your office or with DHS specifically and said, "We are doing some background work with them," the Federal Government is, trying to be able to help them through the process. So walk me through what is happening.

Mr. KREBS. Specifically, what we are doing here, we have done a number of risk and vulnerability assessments, penetration testing, things of that nature, and we have discovered over—I think we have done 24 of these at the State and local level, and what we found is we approached 20 and then moved up to 21, 22, 23, 24, that we were getting 95 to about 98 percent of the same results for every vulnerability assessment.

So we were able to do two things. One is just pack out from those assessments, what the key risks, vulnerabilities, or other issues that need to be addressed. We then packaged that through the Government Coordinating Council (GCC), which we established a couple years ago for spending guidance, "If you are going to spend this money, here are the things you need to go spend it on," and also just pushed those results out to the balance of the States that we have not provided our Risk and Vulnerability Assessment (RVAs) for because we do not think we actually need to do hands-on assessments, because we can, again, with 95 percent certainty tell you what we are going to find. So we just roll those out to our partners.

But, again, we have developed guidance based on our experience over the last couple years, and we found that we will be updating that for this last tranche of money as well.

Senator LANKFORD. OK. So anything that you could say at this point that is missing from either resources you need or resources the States need to be able to prepare for the election in 2020?

Mr. KREBS. So for the 2020 election, I think the plans are in place, particularly from a procurement perspective for election

equipment. They are locked and loaded. They are not going to be able to, at scale, replace equipment.

Senator LANKFORD. Right.

Mr. KREBS. The things I would be thinking about for election security funding—and this is the decision that needs to be made—I really see three buckets of funding. One is addressing the immediate risks.

The way the HAVA formula works right now is it is based on the registered population of the 2010 Census. That will obviously get updated in 2020.

Florida Secretary Lee has done something interesting. Rather than allocate the Florida HAVA money to the biggest jurisdictions, they have actually taken a risk-based approach and getting it to the more rural communities that need that investment. I think that is probably a good approach for the national level. Let us go help New Jersey, for instance, transition off their direct recording equipment.

The second piece is sustainable funding. I do not care how much it is, but we just need certainty year over year over year.

The third thing is we want to encourage innovation. So how do we do that? I think that it makes sense to have a separate pot of money that could be dedicated to innovating around post-election audits, risk-limiting audits. These things take time for concepts, piloting, training, and rollout.

Senator LANKFORD. So one of the challenges I get from a lot of folks is the attribution and then the law enforcement side of it.

Famously, here in Washington, DC, we had two Romanians that hacked into security cameras right before the inauguration in 2017, and so when the parade route is preparing, two Romanians had actually hacked into the cameras along Pennsylvania Avenue and caused a major incident here in D.C.

When tracking it through, we found out it was just two folks that did not even know what they had hacked into with a ransomware piece, and they are living like the Kardashians in Romania off of stealing everybody's money around the world from this different threat.

We were able to identify those folks, arrest them, picked them up, but for individuals like that, the repetitive question is: How do we law enforcement? How do we handle attribution? How do we actually shut down some of these folks that are consistently doing thousands of people and doing ransomware attacks and such, whether it be companies or individuals?

Mr. KREBS. So, first and foremost, we have to continue to raise the security baseline so that they cannot be successful when they come after our networks.

The second piece we need to think through is how do we change the economic model. They are doing it because they are getting paid out. The business plan works. How do we change those mechanisms? I think there are some bigger policy questions in play here that we need to take a look out about paying ransom. I think the State of New York has a piece of legislation they have sponsored that says something along the lines of State and local governments cannot pay.

I am of the mind, do not pay. Do not pay. First off, you are doing a deal with a criminal. How do you know that they are going to pay out? And even if you do recover from what we understand, the recovery keys are only effective in 20 to 50 percent of the time, and then you still have to rebuild. That takes time as well.

Then the third thing is we are working with the FBI. I do understand that they are prioritizing enforcement, as they have for sometime now, but also how do we bring others into the fight? How do we have the intelligence community (IC) and other aspects of the Federal Government play ball here as well?

Senator LANKFORD. All right. Thanks, Chris.

Chairman JOHNSON. Just a real quick comment on election security, your final comment, encourage innovation. I guess it is the conservative in me. One of my favorite sayings is "All change is not progress. All movement is not forward."

I still use the optical scanners. That is how we have always done it. I think we are kind of going back to the future there. The innovation is tied to making sure that it is a more secure system as opposed to the whizbang computer and all of a sudden we find that is pretty vulnerable.

Mr. KREBS. If I may, specifically where I am focusing the innovation piece right now is on audits, auditing the process, post-election audits. Thirty-two States or something like that have an audit requirement right now. We need to help those other 18-plus get auditing in place, and that takes investment as well.

Senator LANKFORD. The only point I am making is we have been able to do elections for many years, and we started innovating and kind of screwed up. But regardless, Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thanks, Mr. Chairman.

To each of you, welcome. It is good to see you. Thanks for taking the time to visit with us and give us a little update and share with us some ideas of what we could all do by working together to be more successful.

As well, while we have 2020 elections coming up, New Hampshire today, and in the months leading up to Election Day, a whole host of primaries are going to be taking place across the country, hopefully no more caucuses like we experienced last week in the State of Iowa.

I will say this. I was out there, a little bit, helping Joe Biden when he ran in 1988, when he ran in 2008, and when he ran this time. For my money, those are some of the nicest people on the planet. They call them "Iowa nice." They are just lovely people.

Chairman JOHNSON. We call Wisconsin "nice." [Laughter.]

It is actually "Wisconsin even nicer."

Senator CARPER. I think we could all learn from them in that regard.

I like to tell people. People say, "What is Delaware's State motto?" I say, "Well, we are the first State to ratify the Constitution. So people call us the First State," and they say, "Well, what else? If you were not the First State, what would you use?" And we say, "Friendly, but you will get used to it." I like that one.

Our intelligence agencies agree that the foreign governments have already taken steps to attempt to interfere in our elections, and given that, we must ensure that our State and local governments are well equipped to address any potential threats to election security.

I have an old African saying I like to quote. It goes something like this, "If you want to go fast, go alone. If you want to go far, go together." In this case, it is important for us to do both, to go fast and to also go together in order to ensure that our State governments have the tools and resources available from the Federal Government, while ensuring that any vulnerabilities are adequately addressed well before this November.

I just want to start off by asking if you all can—this would be—Director Krebs, I think we will start with you on this one. But, if you could, please, just list some of the most promising and productive ways in which CISA has been working with State governments to address their election security concerns, and what are some of the common issues you are hearing?

Mr. KREBS. Sir, thank you for the question. I have to say I have shamelessly stolen from you in my confirmation hearing. You mentioned one of your sayings of "How are you doing? How am I doing? How can I help?" We have adopted that customer-centric mindset across the organization. I have also shamelessly stolen——

Senator CARPER. When you ask those questions, you tell people——

Mr. KREBS. Absolutely. It is the core and the ethos of what we are trying to do here at CISA. We are a customer service organization. We have to understand what our partners need, and that is going to take time.

Why does it take time? In Secretary Mattis' recent book, he quotes General Washington, President Washington, and his leadership philosophy has four key elements: listen, learn, help, lead. It is the same thing we are trying to do here. That is what we did in the election security community.

In 2016, we did not really know much of what was going on at all. So, as we worked up to 2018, we really listened. We listened to what our partners, what our secretaries of State needed, what our State election directors needed, what the local—and then we learned. We learned about the processes, who is who in the zoo, effectively, and then we helped.

We provided a number of resources establishing the election infrastructure, ISAC, providing a series of training and exercises. You have probably already heard about some of the training we provide to State and locals, but also holding three national-level—effectively national exercises on tabletop exercises—or election security, but again, getting information out, getting everybody together, and providing them the help they need.

The last thing, though, this is where we have to lead. We have to understand where the risks are, taking into account our unique perspective at the Federal Government. We launched an initiative last year that really took a look at this intersection of ransomware that we are talking about here, and what is the thing that we are most concerned about, frankly, where the risk really is in elections? It is highly networked. It is highly centralized. It is voter registra-

tion databases, so what would a ransomware infection of a voter registration database look like and how we can, A, prevent against that and, B, ensure that there is resilience in the system. So, if it does happen, it is not leading to a catastrophic failure across the election process.

Senator CARPER. All right. Thanks, and thank you for attributing. Usually, when I steal people's material, I do not attribute. So I especially appreciate that. [Laughter.]

I just want to again brief you, Director Krebs, if you will. In your testimony, I think you referenced a report—I believe it was from 2018—that lists China, Russia, and Iran as aggressive and capable collectors through their cyber capabilities of sensitive U.S. information and technologies.

I think your testimony goes on to say that our adversaries are using their cyber capabilities to undermine critical infrastructure, steal our national security, our national secrets, and threaten our democratic institutions.

Your testimony outlined some of the ways in which CISA has responded to evolving threats, including offering technical services, training programs, and incident management and response services.

Question. What is the participation rate amongst State and local governments seeking CISA assistance and assessing the cyber posture of their information technology systems as well as their election security infrastructure?

Mr. KREBS. So through the MS–ISAC and the Election Infrastructure ISAC, broadly State and local, every State is involved both in the MS–ISAC as well as the Election Infrastructure ISAC. On the Election Infrastructure ISAC, we have about 2,400 to 2,500 local jurisdictions that also participate, which is good, but there are 8,800 of them. So we still have to make the jump.

On the broader MS–ISAC, we have a significant amount of uptake, but that is, again, information sharing. That is getting this documentation out.

I think where we need to improve is working through, as we have already talked, incident response planning, roadmapping for effective security, and that is really the cornerstone for how all the other services and uptakes will be determined, whether they need them or not.

We offer a range of services. Organizations take what they need based on where they are, and it is not going to be everything. And taking a CISA service is not dispositive of a good cybersecurity posture. We have more work to do again on the roadmapping side, and I am looking forward to a couple of the internal initiatives that we have that are going to push that out in the next year.

Senator CARPER. OK. Last, just a quick one. How is CISA proactively reaching out to States locally—and you talked about this a little bit, State, local, tribal, and territorial governments—that have not requested assistance, that have not requested assistance but may be vulnerable?

Mr. KREBS. We will continue to push out information on the CISA through the ISACs and through our normal portals, but what you have touched on here at the end was if we are aware of a vul-

nerability out there, how do we engage a stakeholder? And this is bigger than State and local partners.

Through the Cyber Vulnerability Identification Notification Act that the Chairman has introduced along with Senator Hassan, that is a way that we can—when we understand that there are significant vulnerabilities, particularly in critical infrastructure, the industrial control system specifically, then we can reach out to an internet service provider (ISP), work with them to get the information on the customer identification, and then provide that customer the information they need to secure their networks. That is going to be a critical tool in our toolkit going forward.

Senator CARPER. Good. Thanks.

Mr. Chairman, do you think we might have another round of questions?

Chairman JOHNSON. Probably.

Senator CARPER. That would be great.

Chairman JOHNSON. Talk a little bit more about you are constrained right now by not having that subpoena power. I wanted to bring that up as long as you are on the topic. Just hammer home that point, how important that is.

Mr. KREBS. So there are a number of tools available. Shodan is one of them where you can get an understanding of what systems may be connected to the internet that have vulnerabilities that a bad guy could exploit.

So when you hear Director DeRusha talk about the 90 million hits or whatever it is against the firewall on a daily basis—and Texas, I am sure has a similar statistic—a lot of these are automated probes and scans that look for vulnerabilities, and when they see these vulnerabilities they then try a number of techniques to get into the system, and in some cases, this is what we are seeing through ransomware actors. They are automated processes.

So we can take a similar approach but to identify the vulnerabilities and then plug them, but if I identify a vulnerability, usually it is just tied to an Internet Protocol (IP) address and that is it. I do not know who the organization is. I cannot contact them.

So what we have to be able to do, then, is go to the internet service provider. The internet service provider, by law, cannot turn that information over to us absent an administrative subpoena.

They can go direct to the IP owner, but what we have seen in the past is some ISPs are also managed security service providers. So when they show up and say, "Hey, you have this vulnerability. You need to address it. You should do this," it looks like an upsell.

Plus, I am CISA. I am the Nation's civilian cybersecurity lead. I should be able to work with partners when we identify vulnerabilities, provide them guidance and remediations to patch their systems.

Chairman JOHNSON. This is power that other agencies have, and you do not. And it is a huge constraint on your ability to provide cybersecurity defense and information to the private sector so they can protect themselves, correct?

Mr. KREBS. Other agencies have a variety of this for different purposes, but ours is purely for defensive vulnerability mitigation purposes on critical infrastructure systems, not your average user,

not your home devices. This is the critical infrastructure systems that can have significant national consequences.

Chairman JOHNSON. Again, I know there are people concerned about this, but they really need to be concerned about the vulnerability because you do not have this capability. So, again, I am just trying to make sure that everybody at least on this Committee realizes this is something that has to be granted. Senator Portman.

OPENING STATEMENT OF SENATOR PORTMAN

Senator PORTMAN. Thank you. Thanks for having the hearing. This is really important and timely, given what is happening. I saw the two Government Accountability Office (GAO) reports. It sounds like you feel as though you have now done what you need to do in terms of the election security, recommendations they had in their report; is that correct?

Mr. KREBS. Yes, sir. We released our strategic plan on Friday, and if you take a look at it, by the way, it is a pretty clean polished document. This is not something I just rushed out. It was ready to go. This is the plan we have been operating against since next February. We have a very clear understanding internal to CISA and with out partners of what we are trying to accomplish, and we have had so for a year.

Senator PORTMAN. All right. In terms of what you talked about today, earlier you talked about some of the authorities you might be looking for. One that is out there already as legislation is to codify or formalize the relationship between you and the State Information Sharing Analysis Center, we have been talking about. That is 1846. It has passed the Senate already. I assume you would like to see that get passed.

Second is this legislation the Chairman just talked about to give you the subpoena power to be able to go to the internet service providers. It is very important.

On the State Coordinator Bill, are you openly supporting that? Is the administration supporting that? You have said you want to push more expertise down to the State and local level, and you would like to have somebody in every State Capitol.

Mr. KREBS. Yes, sir. That is definitely a capability that we could benefit from, additional resources out in the field. Yes, sir.

Senator PORTMAN. Again, that is when this is working through the system.

I want to talk for a second about hiring authorities. That is one that we have not gotten into much today. Actually, I am sitting next to Tom Carper who worked on this way back in the 2014 time period. We did pass legislation to help to provide you with additional hiring authority, "exceptional hiring authority," as it was called. My sense is that that is still not enough, that you are still having a difficult time attracting to government the kind of cybersecurity expertise that you need. By the way, the same is true in the private sector. What more can we do there? What more can we give you in terms of authorities to be able to ensure you have the right people in place at the right time to respond to these increasing cyberattacks?

Mr. KREBS. So I think stepping back a little bit, first off, whether it is the Boots on the Ground Act or the ability to direct higher au-

thority for certain positions, I think those are paving the way for us to be more successful.

I think we have some internal housekeeping to do in terms of the process from left to right, the entire hiring process. We have some internal roadblocks that we are working through right now that I am confident in the next 6 months, we will be able to make significant progress.

But more importantly, I think——

Senator PORTMAN. Let me just stay on that for a second, and I agree with you. And I am glad to hear you say that.

We passed this in 2014——

Mr. KREBS. Yes, sir.

Senator PORTMAN [continuing]. Excepted service. It is now 5 years later——

Mr. KREBS. Yes.

Senator PORTMAN [continuing]. And no hires have been made.

Mr. KREBS. That is the Cyber Talent Management System, and——

Senator PORTMAN. Why has it taken 5 years?

Mr. KREBS. So that is the Department of Homeland Security's Management Office that is taking point on that.

Senator PORTMAN. Right.

Mr. KREBS. My understanding is by fourth quarter this year, they will be fully hiring against those billets. It is a reimagining of the civil service, and so it is not an overnight process. And it took, I believe, some rulemaking and other aspects to get it where it needed to be.

But we are not waiting for that. We do have direct-hire authority. Plus, we have retention incentives up to 25 percent for employees, similar to what some of the intelligence community and Department of Defense (DOD) may have as well.

So we are taking full advantage of that, and we have seen our attrition rate go down over the last year or so. So we are excited by that.

But I have to buildup the base. So we are working with partners through the Scholarship for Service, through the Cyber Talent Initiative, where we can have the private sector play a role here.

One of the things I am really excited about is where the private sector can play a role—again, this is the Cyber Talent Initiative—where they can provide tuition assistance to students coming out of college as long as they serve 2-plus years or so in the Federal Government, and then they will have an opportunity to go out in the private sector.

For me, that is a good thing. So if I get somebody in and have them for 2 to 4 years and then they spin out in the private sector, that is not bad. That is good. That means I have been able to train people up. I now have an alumni network out in the private sector.

I am a small agency. I am a young agency, not like the FBI, big and old. Not old. They have just been around longer than us. Not old, been around longer. [Laughter.]

Senator PORTMAN. Agency, not then individual.

Mr. KREBS. Correct.

They have an alumni network. I do not. I have to be able to build this up. So when somebody goes out to the private sector, they

know how to work with us. They know what we can do. They know how to work with us. So I am really excited about some of these things that are coming down the pike.

Senator PORTMAN. And you have the authority to be able to do that loan forgiveness on the student debt?

Mr. KREBS. We also have tuition assistance.

The Cyber Talent Initiative is a different program, where the private sector takes over that piece.

But I think this is the cybersecurity workforce, and I think the gap has been built up a little bit. But this is truly one of those shared responsibilities where the private sector is going to benefit from supporting the Federal Government training, the first 4 years of someone's career, giving them the appropriate training and then spitting them out. I think it is a win-win for everybody.

Senator PORTMAN. Well, good.

On the directorate, DHS——

Senator CARPER. Excuse me. Would you yield for just a second?

Senator PORTMAN. Yes. Let me just finish this point.

I understand they are directing this effort to be able to use these cybersecurity accepted service authorities, but I hope you will push them on that. You say fourth quarters. I mean, it has been 5 years. Here we are.

Mr. KREBS. Yes, sir.

Senator PORTMAN. We have worked through the rulemaking. So I just hope that can happen soon.

Mr. KREBS. Yes, sir.

Senator CARPER. I would ask this to not count against Senator Portman's time.

You said build up the gap a little bit, and I am not sure I understood what you meant by that.

Mr. KREBS. I think that it is the cyber workforce hiring challenges. I think they are built up a little bit. I think, yes, there are significant open positions that we need to fill, but I think we also need to be looking further in the development cycle and getting better security practices into just design development, so that we are not always bolting security on at the end. DevSecOps is a great concept.

Again, it is including the K–12, through the higher education, making sure that security is a platform of any Science, Technology, Engineering, and Mathematics (STEM) education.

Senator CARPER. The thing that was confusing me, I always think we are trying to reduce the gap, not build up the gap. That is why.

Mr. KREBS. No, no, no, no, no. We are trying to reduce. Yes, sir.

Senator CARPER. Thank you for yielding.

Senator PORTMAN. No. Of course.

I would just say one final point. We have been talking a lot today about how to identify problems up front, and you have talked about some additional authorities you could use to be able to do that. And we talked about that today. I think this Committee has been responsive to that, and I think it will be responsive to every evolving threat out there.

But you mentioned Equifax. I mean, it is a great example. We worked with them, again, in our Permanent Subcommittee on In-

vestigations (PSI). We looked at what happened and why were they allowing these breaches to take place, which affected so many millions of Americans. But now we see it also affected our national security in very fundamental ways.

What we found was they failed to remediate vulnerabilities in a timely fashion. They operated outdated legacy systems. I am looking at our State partners here, some of whom have outdated legacy systems, not that Michigan would or any other particular State, like Texas. And they did not have a complete list of applications running on their networks.

So I think being proactive, being able to identify these problems up front, can save just an enormous amount of cost and hassle for individuals in terms of the consumers, and also, as we have seen here, even our national security can be directly affected.

So we want to help you in that, and you have to help us to provide you the authorities you need to be able to be proactive.

Thank you, Mr. Chairman. Senator Sinema.

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Thank you, Mr. Chairman, and thank you to our witnesses for participating today.

We live in an increasingly connected world, which brings both opportunities and risks. Arizona communities are exploring and using smart technologies to improve natural resource usage, advance health care delivery, and enhance public safety.

One great example of Arizona's innovation is our Smart Region Consortium. It is a collaborative of applied research and implementation partnership between public sector, academia, industry, and civic institutions with a vision to transform the Greater Phoenix Region into a model for Smart City technology.

Our State is also leading the way in advancing the development of autonomous vehicles, but like so many other States, Arizona has also experienced the risks of technology.

Just last year, we saw the downside to increase reliance on technology, both the Camp Verde and Flagstaff Unified School Districts suffered ransomware attacks in 2019.

Camp Verde was able to start their classes on time but could not use any of their computers, but Flagstaff was forced to delay the start of school by 2 days. The community hospital in Wickenburg, Arizona, also has suffered an attack. Fortunately, in these cases, fast-acting information technology teams worked quickly to contain the problems and minimize the damage, but these attacks demonstrate the risks our communities face and underscore how critical it is to focus on preparedness at the State, local, and for us, tribal levels.

So my first question is for Mr. Krebs today. Tribal representatives from Arizona who work on technology issues worry that while they have been welcomed in conversations about broadband and connectivity, they have not felt included in cybersecurity discussions.

The DHS 2018 Nationwide Cybersecurity Review also showed that Tribal Nations, while improving their cybersecurity maturity score from 2017 to 2018, still scored fairly low compared to State

and local entities in areas such as identification protection and response.

So what steps is DHS taking to better include tribal communities and assist them with cybersecurity challenges? And how can you help us improve this assistance?

Mr. KREBS. Yes, ma'am. I think some of the bills that we talked about today, including getting more personnel cyber advisors out into the field, can help bridge the gap with the tribal communities.

We are also taking a look internal to DHS of what are the available grant programs we have and how we can better purpose those grants toward cybersecurity purposes but also help jurisdictions, whether it is State, local, tribal, or territorial, write investment justifications for grant requests and then help shepherd those through the process. So it is about getting direct help and assistance advisory help as well as making resources available to them.

And then we have as always, our training, our education, our technical services that we can provide. It is just a matter of I have to start somewhere—and that is with direct engagement—and let them know where they are but also what resources are available to them from the Federal Government and completely recognize that, again, we have not put enough resources out in the field to make that happen in an effective manner.

Senator SINEMA. Thank you.

Following up on this topic with Ms. Crawford and Mr. DeRusha, from the State perspective, what recommendations do you have for ensuring that tribal communities are engaged in this process?

Ms. CRAWFORD. I think our perspective would be for tribal communities or any other entities that are out, particularly in our area and in rural parts of Texas, again, it is education and outreach. And whatever efforts we can do, we certainly work on community outreach through our education programs and our own office of the State Information Security Officer to try to reach all communities and again trying to encourage education in these issues from the very beginning, starting with elementary school making sure again that cybersecurity is an issue that people know about from the very beginning and building up that culture throughout the State and tribal communities of cybersecurity.

Mr. DERUSHA. So I think we find travel communities in very small municipalities similar challenges. There is really not even an awareness really of what cybersecurity is and what they should be doing. So we like to talk about thinking about these things in business risk, for mission risk. Cyberattacks can prevent them from delivering whatever services they deliver or just having normal operations and sort of helping them understand that there is a risk to them, and they do not need to necessarily have something of value. They could be just a target of opportunity.

So it is education, awareness, constant outreach. These are some of the things that been effective.

Senator SINEMA. Thank you.

My next question is back for Mr. Krebs. In the May 2019 interim report to DHS by the State, Local, Tribal, and Territorial Cybersecurity Subcommittee, the authors recommended that DHS create a dedicated grant program to States for cybersecurity. In Arizona,

we, of course, have seen the value that grants can provide firsthand.

The Arizona Department of Administration receives grant funding to offer anti-phishing and security awareness training for smaller and less-resourced Arizona government entities, but there are additional tools and training that Arizona would like to offer. But we do not have the funds to do so.

From DHS's perspective, what would be the benefit of the type of grant programs that the subcommittee has recommended?

Mr. KREBS. So, first and foremost, we do have training and exercise resources available free of charge through the Federal Virtual Training Environment (FedVTE) program. We have thousands of hours of training available.

We are also working right now on our existing Phishing Campaign Assessment tool, which is more manual. We are taking it to an automated version. That will allow for more scalable deployment, and those are the sorts of things, again, if we can help tribal organizations have increased access, it starts with awareness. Let them know that they are there, and then they can go use those services.

From a grant program, I think there are a couple different recommendations going out there and including from the Homeland Security Advisory Council subcommittee that touched on this as well as some legislation under consideration that would talk about $400 million in grants. I think that dedicated funding would help them have more repeatable ready access to resources.

But the other important aspect is it would also incentivize investment at the State level because it would require—I am not sure the specific matching amount right now, but it would also require a matching amount from the State or local jurisdiction, which again you can say, "You need to prioritize this. If you put in a little bit, you will get a lot more from the Federal Government." These are things that we continue looking forward to working with the Committee on and getting across the finish line.

Senator SINEMA. Thank you, Mr. Krebs.

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Chairman Johnson.

Thank you for being here, all of you, today for participating in this hearing.

I am proud to say that on Christmas Eve, my Building Blocks of STEM Act was signed into law. That is going to help building out the workforce. I have a few other bills in the pipeline, Cyber Ready Vets, Junior Reserve Officers' Training Corps (ROTC) Cyber Training Act and others that will help build workforce capabilities in the future.

None of these things are going to stop happening, like my colleagues said. Data breaches are occurring at a record pace. More than 4 billion records have been exposed in the first half of 2019 alone. Of course, we know the cost, the impacts it has on businesses, not to mention the reputational harm that is inflicted.

So one way to mitigate the impacts of cyberattacks on businesses is through the development of a comprehensive disaster recovery plan that will restore data, applications, even maybe save the hardware. And we know that such planning can help avoid the worst consequences of cyberattack.

In a prior life, I started my career as a computer programmer. I actually had to create lots of backout plans, do robust disaster recovery planning, offsite storage. You name it, we had to do it, and testing, testing, testing for some of those things, particularly help in the area of ransomware if you have offsite storage.

So despite this, we know large companies do this pretty well, but small companies, they really face a financial impact. Over 90 percent of businesses in Nevada are small business, and when they are targeted for a data breach, they may be doing cyber hygiene, but they may not be understanding how they can do robust—especially in the area of ransomware, which is particularly prevalent. How can we get out the word or training packages or templates for our small businesses to understand that you can overcome a breach in some ways to at least a particular point in time by having a good disaster plan in place? Can you talk to me how you are helping businesses do those things?

Mr. KREBS. Yes, ma'am.

So I think, again, it goes back to continuing to beat the drum on awareness, but also doing it in a way, as I mentioned in my opening, about demystifying this.

We pushed out in the fall, a Cyber Essentials document. It was probably more complicated than it needed to be, but it really comes down to six things that then roll up to three: leadership, security, culture. That is the baseline for——

Senator ROSEN. And I am talking about small businesses.

Mr. KREBS. Again, this is all part of it. It is about when you own a small business, you have to be thinking about delivering a service as well as ensuring the ability to continue to deliver that service. And it is not just——

Senator ROSEN. Are you able to give them some kind of templates——

Mr. KREBS. Yes, ma'am.

Senator ROSEN [continuing]. On your website about are you doing that?

Mr. KREBS. So we are working through a couple of different avenues right now.

We have had relationships in the past with the Small Business Administration (SBA), Small Business Development Centers (SBDC). That was part of Executive Order (EO) 13800 that requires an SBDC plan. So we are continuing to work through that process, working with the chambers of commerce, getting templates out there to understand what incident response planning looks like, what recovery looks like, but also just good old cyber hygiene plus using some of the resources that we have that are not supplanting anything in the marketplace, just offering free-of-charge services.

Senator ROSEN. Do you think that you have enough resources from us to be able to get this out there?

Mr. KREBS. Again, I need more people out in the field. I need more boots on the ground. I cannot be effective——

Senator ROSEN. Maybe we will get some more of my bills passed.
Mr. KREBS. Yes, ma'am.
Senator ROSEN. We may get some more boots on the ground.
Mr. KREBS. Yes, ma'am.
Senator ROSEN. I have a second question. Of course, in my home State of Nevada, over 250,000 Nevada residents live in rural areas, and of course, in Las Vegas, where we have lots of active chamber and bigger State and local government presence there, my smaller communities do not have that. So how can we again share—maybe you can speak about this. Especially in Michigan, lots of rural communities. You have the upper peninsula up there going on. How do we help them get the qualified staff or the qualified training to combat these cyberattacks?
Mr. DERUSHA. So, Senator, we think about this, both on the prepare and the response side of the equation.
From the preparedness side, it is a lot about developing communities of practice, advertising, making sure that they know they have State and Federal resources available to them, bringing these communities together so that they can do self-help and help each other and start to get to know one another.
We also have a very robust Cyber Civilian Response Corps that works in close coordination with our State police. So we can actually deploy people out. We have done so in rural communities, and what we find in the volunteer is that programs that we want, people who live locally to be a part of that. So we do try to recruit in some of those rural areas because we find that if you can go respond to an incident, return home at night, sleep in your own bed, come back the next day or maybe do some work and balance that, that that is working pretty well for us.
Senator ROSEN. And so building on that, what other efforts do you think we can do to increase these shared services, use the economy of scale through bulk technology services or using the same people to go out to rural areas? How do you think that we can best accentuate that?
Mr. DERUSHA. So, Senator, we need scalable models, and we need funding.
I think you can see there is a lot of innovation going across States. The National Association of State Chief Information Officers (NASCIO) put out a report highlighting 13 different States' local community initiatives last month. I think there is a ton of great innovation going on. We are starting to figure out what we need to do in each of our own States and how to solve these local problems.
But in the end, it needs to be in enduring help and assistance, and if you are going to procure a security vendor, managed security service, for example, to do net-flow monitoring, endpoint protection, email protection, that is a lot of money.
Senator ROSEN. Right.
Mr. DERUSHA. And that is part of the reason that some of the HAVA funds have not been spent yet, because getting those contracts together is a lengthy process.
But these things are very real protections. The market has a role to play. All levels of government have a role to play. It is just a collaboration.

Senator ROSEN. Thank you.

I yield back, unless somebody wants to say anything about this. Thank you, Amanda.

Ms. CRAWFORD. The only thing I would add, Senator, is, again, agreeing with Mr. DeRusha's comments, is one of the things we have done in Texas and that we are charged with is a cooperative contracts program for IT goods and services. So we have the prenegotiated contracts with State terms and conditions at low prices that helps the local governments be able to secure those and then our shared technology services program through managed security services, but also disaster recovery is a service and other elements to allow any level of government to participate in that, even the rural communities.

Senator ROSEN. Thank you. Appreciate it.

Chairman JOHNSON. Thank you, Senator Rosen.

I know a couple Senators talked to me about maybe having a second round. So for staff, if they want that, get them back here. Otherwise, when I am done, we are going to close it out.

Let me go back to the point I was talking about, about individuals, because I want to work back up to the larger enterprises, OK?

The basic question is, Does or why does not backup work? So, again, individuals, on an individual device, it just automatically backs up the cloud. Does that work, and if it does not work, what is preventing it?

Then go to a small business, where they have my era Peachtree or whatever accounting program. Pretty small database in the scheme of things. Pretty easy to back the entire thing up.

You go to the next size business, and I will bet you Senator Rosen could actually answer this question as well, having done all this testing.

Again, just kind of work our way up from the individual to a smaller enterprise to a little bit bigger, more complex, different divisions. What is the problem here?

Do you want to quickly chime in here?

Senator ROSEN. I would venture to just put this out there that a lot of people do not do offsite—like if you put something in the cloud, you are probably OK, but people do not have robust offsite backups. Everything is plugged to their computer, on their computer. So when your computer is locked up, essentially you cannot get——

Chairman JOHNSON. You need the air gap.

Senator ROSEN. If you move something away from the compromised system that you can then lay back on and begin to function from a starting point, but I will let them——

Chairman JOHNSON. Back ages ago when I had my International Business Machines Corporation Personal Computer (IBM PC), we just had these disk drives. You would plug them in. You back it up. You pull it out. And you had your entire system. If something ever happened, you would just plug it back in, and literally, as long as it takes to book up the computer and plug that data in, you were fine, again, smaller enterprise.

Answer that question. Scale it up from individual, small business, more complex, multiple division, multiple site, international.

Mr. KREBS. I think starting at the individual layer, if you can update or rather back up, you should. I do not think everybody does back up. It is not always enabled by default, and then it also, in some cases, depending on how many pictures you take—I know how many pictures my wife takes on her phone, and she has exceeded her iCloud storage in others. So we have to continue looking and buying for additional storage.

I have five kids. She takes a lot of pictures and videos and things like that. So you have to work through that.

Chairman JOHNSON. Again, I am technical imbecile. My phone just tells me, "You are going to back up" or "You have not backed up in 2 weeks. Make sure you are plugged in the Wi-Fi," and then it backs up. That works.

Mr. KREBS. I would also say you are probably in the minority. A lot of people just ignore that and click through. We have to continue increasing awareness on the importance of backups and telling people do not just click it away. Do not hit no. Do not ex out.

Chairman JOHNSON. So this goes into the overall message. Ninety-five percent of this can be prevented if you just do some basic things. Let your device back up because, if you do, you are pretty well protected.

Mr. KREBS. It takes time. Yes.

Chairman JOHNSON. OK. Now let us go to the small business, same type of thing. Is it just simply people are not doing it, or is there something more complex? Is it they have their software and they do not back up their software? They are just backing up the data?

Mr. DERUSHA. Senator, I think it is all of those things.

Again, the big theme here is we are trying to get education, understanding, and awareness, and that is a big piece of this.

One of the pieces of advice we give to a small entity is even if you leave, if it is an offsite and completely offline, a backup, it could be 3 weeks old, a month old. That is OK because you can at least roll back to something.

Whatever criticality level of the entity and skill capability level, these things are all going to matter on how often they are able to do it and whether or not they are doing it at all.

So we just try to say, "Hey, based on how critical you are, you really should be considering regular backups, ensuring offline redundancy."

Chairman JOHNSON. So, again, with modern technology, with modern software, why is not this stuff just pretty much automatic?

Mr. DERUSHA. It is fairly automatic particularly in the larger organization. At the State level, we have hundreds of critical applications running. Each of them have their own backups in place. A lot of them are backing up in the cloud. We have multiple data centers running. So we have a very sophisticated apparatus.

But the fact of the matter is the bad guys are always kind of a step ahead. Malware, particularly what they call "polymorphic malware," is constantly changing. So even if you are trying to defend against one old known type, we have seen in one day 35 different types of the same malware stream come through. It is just a very difficult thing to prevent because, if you are connected, there may be a way, if it is not perfectly configured, to defeat that, and

it is hard to perfectly configure systems because that is a very high skill level.

Chairman JOHNSON. So, again, if you have done the backup, I mean, you are not backing up continuously. So there is always going to be that gap.

I will go to Ms. Crawford. Is that the issue? In Texas, you may be backing these things up, and then you have to restore whatever activity occurred between the last backup and the present time.

Ms. CRAWFORD. Sure. I mean, continual backups is certainly a difficult challenge, but having backups that are regular and scheduled—and as you said, then there is only the small gap. And you decide based on a risk management perspective, what is that acceptable risk and what is that length of time for the gap and keeping those backups offline.

In ransomware, your data and information is held hostage, and you devalue your hostage when you have backups that you can then bring back up and restore. So that instantly helps to put a damper on any request for that ransom. So it is crucial and important.

I really think one of the issues, though, with the—and I am speaking again for the smaller government entities. It is those limited resources, and it is changing the dynamic and changing the conversation about cybersecurity. I think when you have smaller governments who are looking at their limited resources and are you going to spend a dollar on mission or a dollar on cybersecurity, for the longest time, they were looking at mission. Well, cybersecurity has to be part of the mission, and we have to do that and train on that through education and outreach and awareness.

You cannot issue marriage licenses, birth certificates, and titles and all of those other things that a local government does that is part of their daily business if your systems are down, and so it is just increasing that awareness to get folks to understand what it is they need to do.

Chairman JOHNSON. Mr. DeRusha, you had something?

Mr. DERUSHA. Senator, just to add, back to the individual layer, we are looking at some innovative and creative solutions to protect residents, potentially, by exploring mobile security applications that one could deploy out to residents for free download if they chose to download it. What this is doing is getting left of that attack, and any anomalies that are coming into the phone, it is detecting them. If you have downloaded a bad application, it is detecting that. If you go into a bad website, it is letting you know on the phone. If you are connecting to a bad Wi-Fi connection that is actually a rogue network, it is letting you know.

So these are some innovative solutions that we are looking at to try to get ahead of this and prevent that attack from occurring and needing the backups.

Chairman JOHNSON. I am looking for the private sector to handle those things. Director Krebs?.

Mr. KREBS. One of the things that you have already touched on is—you did not say it directly, but security cybersecurity is a cost center. You are not going to have significant resources plowed into cybersecurity of your networks, particularly in small businesses, medium-size businesses. So they are resource-strapped. They are

personnel-strapped, and even though we talk about these things, the basics you need to do, in a lot of cases, you are talking about existing legacy networks that have other problems that have to be addressed first.

Yes, you should always have a backup offline, and you should test it because they do not always work. But you have to start somewhere, and we are really pushing vulnerability management, asset management, identity management, and then good governance across the top.

Chris talked about all the different apps they have running. It is not just about you take an image of the entire network and then you have it somewhere. It is a series of backups.

I do not want it to be lost here that, yes, the basics, you need to do the basics, but the basics in a lot of cases are still really hard.

Chairman JOHNSON. Yes. I understand.

Senator Carper, did you have—I do not want to necessarily do full rounds. I have to close this out by 11:30.

Senator CARPER. OK. Thank you. Thanks, Mr. Chairman.

Let us go to Iran for just a little bit, if we could. Prior to our entering into the joint agreement between five countries and Iran on an effort to halt their nuclear weapon program. Prior to that, they were attacking our financial institutions using the internet, cyber attacks, unrelentingly. Within weeks following the signing of that agreement, those attacks dwindled significantly.

That reminded me at the time of root causes. The Chairman and I are two big proponents of not just addressing the symptoms of problems, but also the root causes of problems. That experience said to us maybe if we want Iran to back off, maybe having that kind of agreement and reward them for backing off would actually work.

I want to go from that timeframe from roughly 5 years ago to today and ask this question. It appears there is broad consensus, Mr. Krebs, among national security officials, including yourself, that Iran, far from being finished with retaliation from this attack that we took to take out Soleimani, but they are likely to pursue cyberattacks on U.S. targets, including State, local, and tribal governments. They might hit the pause button for a while but eventually come after us again.

What is more, we have known for sometime now that they are capable of doing a fair amount of damage through cyberattacks.

I believe, Mr. Krebs, you mentioned, I think, before I got here—I think you mentioned your interagency coordination after the strike on Soleimani, which is good. However, did the administration provide any warning to DHS, either through the Office of Intelligence and Analysis or to CISA specifically regarding an increased likelihood of cyberattack from Iran prior to carrying out the Soleimani strike?

Mr. KREBS. So we have been operating at an enhanced alert posture since probably early last summer. June 22, I issued an advisory that seemed to indicate there was an increase in activity, spear-phishing, credentials stuffing, password spraying, those sorts of account compromise technique that the Iranians used. We had seen that over the course of the last couple months. So we had

been already on heightened alert, and internal to the Department, we had a contingency plan for just this sort of thing.

I would have to defer to the Secretary and the Acting Secretary on the sorts of conversations they were having specific to this event with the rest of the administration, but we were already planning as if they were active. We had been sending out a significant amount of alerts and advisories.

So when news broke of the strike, we were in place ready to go. We snapped into place our engagement mechanisms. That is why we were able to get people on the line so quickly because we were ready for it.

There is a different aspect of this as well. The Soleimani strike was one of strategic surprise. The way that Iran in particular—but pretty much any other effective cyber actor—to get these sort of persistence and positioning that they want to launch their attacks against their strategic objectives takes time. It does not just happen overnight. That is what we saw last spring, where they were positioning for access.

So when the January 2 strike happened, they were either in position to do what they wanted to do or they were going to have to make a decision to work themselves into position. So we had a two-pronged approach of you may already be compromised and you need to be looking for the indicators of Iran comprise. Alternatively, if they increase their activity, you need to be on the lookout for these sorts of techniques, and that is part of what we pushed out with our alert.

Senator CARPER. Good. Thank you. Thanks very much.

I am going to stop picking on you, and then we will let these other folks answer a couple questions, if you would. I just want to ask the two of you, Ms. Crawford and Mr. DeRusha.

I want to give each of you—if you will just take a minute, to tell us what is working when it comes to your partnership with one another, including CISA. What is working?

Mr. DERUSHA. So one of the things that is working is we have really tried to integrate DHS CISA advisor into our monthly election security meetings, for example. We have regular threat information sharing briefings. They have ensured that the Secretary and both myself have been brought into classified prep briefings, which is really beneficial, particularly for officials who are not used to hearing the Intel. Actually, I would encourage that there could be more. It would be helpful to have more of that actually at the State legislature level as well as they are determining whether or not they can provide more funds for cybersecurity.

I would just say that the overall partnership is very streamlined and just reinsure that we are integrating and bring them along on every step of the way.

Senator CARPER. Ms. Crawford.

Ms. CRAWFORD. I would agree that we also have a great partnership along with our Secretary of State's office in receiving briefings on election security issue.

I mentioned a little bit before about we are taking advantage of the CISA's offering of a Tabletop Exercise to offer that on cybersecurity at our Information Security Forum in Texas.

I would also say just coming out of the August events, I have just been overwhelming impressed with CISA's efforts to reach out to us to make sure that the lines of communication were open.

They came down to visit after the August event. We came up and visited with their leadership as well to see how we could understand better what was offered, and they were very open with us about improving the communications line.

So we definitely feel that they hear us. I mean, we certainly would love a dedicated resource, but I know that we are not alone with that and that they are working toward that.

Senator CARPER. One last quick question, Mr. DeRusha, for you. As a former Senior Cybersecurity Advisor to President Obama and speaking from your current role as Chief Security Officer for the State of Michigan, how would you assess CISA's outreach to their State and local partners?

Mr. DERUSHA. The outreach of Homeland Security? So, as Director Krebs has mentioned a number of times, it is really about resources, and we see the intent every day of DHS trying to get everywhere across the State, particularly in the runup to the elections. I think it is just a matter of they need more boots on the ground, and again, they need to have a specific State representative so that they can get familiar with that State and understand how to plug in where they need help, where they have already got it covered, and what sort of tailored information for different groups is available and useful.

I really just think that DHS is doing everything it can with the resources it currently has, and we just need to work to get more funds and more resources.

Senator CARPER. Mr. Chairman, while you were running very successful businesses, I was trying to run the National Governors Association (NGA). They let me be a chairman for a while, and then—actually, they let me be the chairman of something called the NGA's Center for Best Practices. It is a clearinghouse for good ideas and which can be very helpful to Governors, to States in sharing information and best practices.

I suspect you are already well aware of that and taking advantage, but I would just bring it to your attention if you are not.

Thank you all very much for being here and for your work.

Chairman JOHNSON. Before I turn to Senator Peters, I just want to kind of reinforce that point. I really think CISA has the opportunity to really create a model versus an old agency. I would call it well-seasoned, the FBI. You have a new agency here. You can create the model of a clearinghouse, of a support system, without onerous over-regulations.

To me, the private sector will be ahead of us in many respects in terms of how to handle backups for individual devices, small enterprise, that type of thing.

I do not want to see CISA grow so big and have so many resources that, all of a sudden, now they are lording over State and local governments. I want them to be an effective resource. I want to see limited Federal Government but effective Federal Government.

So we want to get that balance. You have a perfect opportunity right now as you are standing up this agency, With the whole in-

terference in the 2016 election, I think the Federal Government has responded beautifully to that, quite honestly. Is it perfect? No. But I think CISA and both the Obama administration and Trump administration have done a pretty good job in, again, laying out that model, very similar to FEMA.

It really is the individual. It is about the enterprise. It is about State and local government are the first responders. They have to be responsible.

I do not want anybody to start looking at the Federal Government will take care of this for us, "Why did not you prevent this?" There is a lot we can do in terms of resources and vice and making people aware, but in the end, people have to take responsibility. So it is about getting that balance right.

Quite honestly, I am encouraged by the direction. I do not have a problem with additional resources so we can effect this thing, but I am going to always be very wary of too many and having CISA or Department of Homeland Security becoming "I am the Federal Government. We are here to help." I actually want that to be true as opposed to people rolling their eyes when the Federal Government comes here offering help. I do not want them controlling.

Senator CARPER. But, Mr. Chairman, Senator Portman was nice enough to reference some of the work that I had led when I was privileged to chair this Committee in the cyber world with some of you. My partner in that was Tom Coburn.

Some of you know Tom has battled cancer, I think, four times in his life and beat it, and he is in another battle today. Just keep him in thoughts and prayers.

Chairman JOHNSON. I agree. Keep Senator Coburn in your prayers.

Senator CARPER. You bet. Thanks.

Chairman JOHNSON. Senator Peters.

Senator PETERS. Thank you, Mr. Chairman.

Thanks again to our witnesses for all your great testimony today.

Chairman Johnson and I are on a bill called the DOTGOV Act, which will make it easier for State and local governments to transition to more secure and trusted dot-gov domains. When State and local websites can be mimicked, I think this is important protection.

Mr. DeRusha, could you talk a little bit about dot-gov use in Michigan and from your perspective why would transitioning to dot-gov really be beneficiary for both State and local governments?

Mr. DERUSHA. Absolutely, Senator. So to give just an example, if you look at about the top 10 counties in Michigan, they are pretty much using dot-com and dot-org, and those top 10 counties generally represent two-thirds of Michigan's 10 million population. So right there, we can just look and say we have got a challenge.

By moving to the dot-gov top-level domain, there is just inherently more security built in. They have protections in place to ensure that compromised passwords are not being reused, two-step authentication, and just the trust factor, it is really easy to spoof a dot-com or dot-org and pretend to be someone you are not and get someone to give you their personal information or credentials. So by having the dot-gov,—org in place, we would really be able to start stemming some of these very common attacks that we see.

Senator PETERS. Thank you. Director Krebs.

Mr. KREBS. So a couple things here. One is that we can preload a number of security services into a dot-gov Uniform Resource Locator (URL), and really what we are seeing more than anything right now is that local jurisdictions in particular are making decisions based on $400. And that is what it is costing them to sign up for a dot-gov account. We need to be able to solve that problem because you should not put security at stake over $400 at a local government level.

The second piece, as Chris just mentioned, is there is an aspect of countering disinformation baked in here as well. What we are encouraging organizations right now to do and individuals to do is go to your trusted sources for information. Do not just listen to the random dot-com or dot-org or whatever. Go to the trusted source; election officials, for instance. Go to the election official's website to find out registration information, where you are supposed to go vote. That should be a dot-gov. We need to shore up the dot-gov registration process to make sure people do not get there and have unauthorized access to dot-govs, but assuming we get there, this will help counter a lot of particularly election disinformation as well.

Senator PETERS. Great. Thank you.

Mr. DeRusha, you mentioned in your opening comments the partnership with the National Guard, both the Air and Army National Guard in Michigan. Could you elaborate on how that coordination is important and how we should be using those resources with State and local governments?

Mr. DERUSHA. Absolutely. So we are fortunate enough to have both Army and Air Force Reserve unit cybersecurity protection teams in the State. These are some of the best, most talented folks. They are highly skilled, trained, and well equipped. So they are a fantastic resource, as Texas showed us all when they leveraged them during their response, and so we have a very close partnership with them.

We exercise together. We recently did a live exercise, simulating a very large attack, and they were there along the way. Next month, we are actually going to be doing a training exercise on our State network where they will come in, and we will start to get more familiar with one another how to work together and then get more familiar with our team members and our network, so that if we need to go to them for support during a crisis, we will just be better prepared for that.

But I cannot emphasize enough that this is about all resources. It is DHS, plus State, plus Guard, plus FBI, plus vendors, plus, plus, plus, and I think that is just the key thing here. The threat is overwhelming, and we need to be using all available resources.

Senator PETERS. Great. Very good.

Director Krebs, a last question here. More and more critical infrastructure at the State and local government are relying on systems at data centers, which required, obviously, cybersecurity but also physical security. What efforts need to be made to ensure the physical security of our data centers?

Mr. KREBS. That is actually an interesting question, given the authorities of my agency. So we are not just the cyber agency. We

are the cyber and infrastructure security agency. We have five different disciplines, the way I see it: IT security, industrial control systems security, supply chain security, physical security, and insider threat. Those last two pieces—physical security, that is part of what we were able to do with our field force. I have a cadre of about 138 protective security advisors that focus on physical security, and you name it, whether it is data centers in northern New Jersey, out by Dulles Airport, we have done physical security assessments of these facilities to make sure that they get the appropriate security measures put in place. So this is absolutely critical.

The thing that I will kind of close out on here, though—and Director Crawford mentioned managed service providers early on. This is an area that, I think, bears some additional examination and coordination with our partners.

MSPs, whether it is the bigs or the medium sizes that provide resources at the State and local level, it is a community without peer. They do not have a natural aggregation point or an association here in D.C.

Moreover, we have really encouraged State and local governments, private sector, medium-size businesses to go to the cloud, to go to shared services and models like that, and that is the demand side.

On the flip side, the supply side, there has been a recognition that there is a market here, but we have not really established what good enough security looks like. I think that there is a lot of opportunity for my agency to work with managed service providers, help them understand what their challenges are. Again, their challenges are that they are a community without peer. There have been a lot of cases, large, complex, global networks and also a lot of risks baked in of contracts they may have signed years ago that they are not really sure how to manage that risk long term.

So I think this is one of those areas that over the next 18 months, you will see my agency lean in a little bit more to really understand the areas of focus that we can manage that is an unknown risk right now.

Senator PETERS. All right. Thank you so much.

Chairman JOHNSON. Senator Peters, just real quick on MSPs, I assume—and I know how dangerous it is to assume, but I have always assumed that there is plenty redundancy built into the cloud, storage, and that type of thing.

So if you did have, let us say, a service center attacked and go down, you have redundancy, correct?

Mr. KREBS. It depends. I think with the hyperscale cloud providers, you have a significant amount of redundancy involved, but again, we have not really defined what best practices, what standards look like for MSP. So you might see some MSPs with a shared back end, where you could lose it all in one fell swoop, others that will have virtualization across the platform. But, again, we have not collectively defined what good enough looks like, and I think that is an area that we need to lean into.

Chairman JOHNSON. I think it is just a basic consumer protection. Again, I am a limited government kind of guy, but to me, this is the kind of regulation that I think the Federal Government should be supporting, so I am happy to work with you on that.

Before I close this thing, we did hit election security. So I just want to go to Director Krebs a little bit.

You have heard me kind of lay out my definition in terms of what you have to worry about. Vote tallies, voter files, and then the whole social media disinformation. Can you just kind of go through the vulnerability of those three? Voter tallies. What is our vulnerability there? What is the likelihood?

Again, I know some voting machines have Wi-Fi, but it should not be hooked up during the voting. That should be very limited use. Then voter files which personally, I think, when it comes to CISA is your primary area of concern, certainly my area of concern, and then social media disinformation, the burden falls there on consumers. We need to be discerning consumers of information and how we use it, but can you just kind of go through those three?

Mr. KREBS. I want to approach this maybe from a different perspective, but we have done a significant amount of research lately in the last year or so working a risk assessment across the system of systems that makes up election security. And what we found was the greatest opportunity for impact at scale. It is where things are highly centralized and highly networked, and to your point of the voter files, the voter registration data bases, that is precisely where if you wanted to create havoc at scale, catastrophically, that is where the adversary would hit.

Last summer, we launched our Voter Registration Database Ransomware Initiative, just with this concept in mind. So I think, again, that is where a significant amount of the risk is.

On the voter tallies, I interpret that as the voting machines that are not necessarily networked. They are highly decentralized. So to get an effect at scale is going to be really difficult, particularly in an undetected way.

This lays then into your third piece of voter disinformation. You have to question the strategic objectives of the adversary. The adversary may not be looking to achieve an outcome at scale and in an undetected manner. The outcome may be that they want to be detected in one key district in a swing State and throw the entire thing into question.

So I have said this before, but we have some time now between November and today that we can continue working through these threat scenarios and just let the public know, hey, these are the techniques that you may see them do. They may try to question or put into doubt the sanctity of these systems. Are there vulnerabilities throughout? Yes. Are they easy to exploit if you got your hands on? Yes. But there are measures that can be put in place, paper backups and audit the process, absolutely critical security measures in place.

So, again, our objective is not 100 percent security. It is resilience, and the voting public plays a part here too.

The third pillar of our strategic plan is to engage the American public and let them know what their rights are. You have to have a plan for voting. You have to know where you are registered to vote. You have to know if there are any voter ID requirements. You need to know what your provisional ballot rights are, so that if something happens and the e-Poll book is acting up—because let us be honest. Things happen on Election Day that do not have to

be Russian-related. They just happen. You know what your plan is. You know how to vote.

And, last, have a little patience. Election night reporting is unofficial results. If it does not get there by nine o'clock, it is OK. They have time to validate the system.

Chairman JOHNSON. Almost $800 million of spending, again, I have been using optically scanned, just fill in the dot. I have always thought that was pretty secure. Is there a more secure system? And in terms of State and local spending of that, of those Federal dollars, I would think that would be a good place to start. If you did decide to electronic, maybe you ought to, again, go back to the future and do something that is auditable because you have a paper ballot filled out by a voter that is optically scanned. It is pretty easy to go back and recount in that as well.

Mr. KREBS. So the market itself, I think, is going away from these direct recording equipment machines that do not have any sort of paper ballot backup.

There is one instance over the summer that I am aware of. The manufacturers themselves are not prioritizing them in their production runs. That is not, I think, a longer-term concern. The concern is, Do you have a paper ballot backup, and do you have a post-election audit process in place? Those are the things that we need to prioritize, and I think the numbers actually show that, I think, in 2016, it was on the order of 82 percent.

Now you should be seeing about 90 to 92 percent of votes cast in the United States will be associated with a paper ballot, and that includes all the historically known swing States. There are scatterings throughout the country of areas where there is paper, but the trendlines are in the right way.

Chairman JOHNSON. Have you just done a quick analysis of what it would cost to have everybody convert to optically scanned paper ballots?

Mr. KREBS. So optically scanned paper ballots is one way of doing it. There are other machines.

Chairman JOHNSON. What percent of the vote is tallied that way?

Mr. KREBS. So with a Scantron and then an optical scan, off the top of my head, I am not sure. We will have to come back with you, but there is about an 8 percent set of systems that do not have any paper ballot. And that is what we should ruthlessly look to phase-out over the next several years.

Chairman JOHNSON. Again, my understanding is that DHS has done a pretty darn good job—and I will ask the two State and local government representatives—of reaching out and making sure people are aware of the voter file situation and raising the awareness and doing everything they can to be a resource. If State and local governments are willing to access their capabilities, is that true, Ms. Crawford?

Ms. CRAWFORD. I know that in Texas, working with the Secretary of State's office, they were very appreciative of the HAVA money to do these election security assessments. Those chose to go, rather than through DHS, but actually through a program through DIR to use those funds to do the assessments.

Just speaking to that and the value of those assessments, we had one of our 254 counties who did an assessment and did remediation based on what they saw in that assessment. They were and should have been a victim of that August ransomware event, and that did not happen. I think part of that speaks to the value that is truly there once you have these assessments and the funding going in looking at these county systems as a whole. So that is a positive test case for that.

Getting 254 counties in a State like Texas to all agree to do this and have folks come in has not been without its challenges, but I think we have all but three signed up to undergo those assessments now. So we are encouraged by that.

Chairman JOHNSON. So in terms of what Director Krebs was talking about, the greatest vulnerabilities of voter files in Texas, again, there is no guarantees, but you are pretty, fairly confident that you are obviously fully aware of this and taking the steps that you are pretty confident that we should not have any problems in 2020?

Ms. CRAWFORD. I would defer that to our Secretary of State's office since they handle that, and we are really just essentially the IT provider to do those services. But I am confident in the relationship that our Secretary of State's office has with DHS in working to address those issues.

Chairman JOHNSON. Mr. DeRusha, in terms of Michigan—and, again, assessment with the other 50 States? Because you are talking amongst each other.

Mr. DERUSHA. Yes. So we collaborate closely with our Secretary of State, Bureau of Elections, Michigan State Police. We have DHS. We all have a different role and responsibility. There is a lot of activity going on.

So, for example, we are trying to put two-factor authentication on all of the county clerks that are going got access our registration system, something that the State just needs to do.

But DHS is doing briefings. We are trying to do educational briefings, and what we are doing is we are just planning together, tailoring those, making sure that there is good content for the audience, and then sending one coordinated message out and just pulling out in the field together so that we bring all resources to bear at once, because otherwise it would be overwhelming for them, frankly.

They also have to make sure the elections work. So we want to make sure that we are working together to just make these resources available and easy to use.

Chairman JOHNSON. OK. Again, I want to thank you all for taking the time for your testimony. I cannot tell you how many Senators walked by me and said, "Hey, this is a great hearing. We really appreciate this," and that was really because you did a great job in preparing your written testimony and answering the questions in a relevant manner. So thank you very much.

The hearing record will remain open for 15 days until February 26, 5 o'clock p.m., for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 11:41 a.m., the Committee was adjourned.]

APPENDIX

"What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"
Opening Statement of Chairman Ron Johnson
February 11, 2020

As prepared for delivery:

The purpose of today's hearing is to examine how state and local governments and critical infrastructure owners/operators and other businesses can mitigate, and protect against, persistent cyber threats.

The protection of mission-critical systems for state, local, tribal, and territorial (SLTT) governments is an essential component of our nation's cybersecurity. Last year alone, cybercriminals used ransomware attacks to cripple municipal entities with near impunity. An estimated 966 government, education, and healthcare entities were victims of ransomware attacks in 2019 that cost an estimated $7.5 billion in operational and financial damages.

In addition to the increased frequency of ransomware attacks, heightened tensions between the U.S. and Iran have raised concerns about the extent to which state and local governments, and critical infrastructure owners and operators, are prepared to respond to cyberattacks by state or state-sponsored actors. Earlier this year, DHS issued multiple alert bulletins referencing potential Iranian cyberattacks against our critical infrastructure in retaliation for the U.S.'s lethal strike against Qassem Soleimani, then head of Iran's Islamic Revolutionary Guard Corps, a designated Foreign Terrorist Organization. One bulletin referenced Iran's "willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks."

Fortunately, according to Leidos, a defense, science, and information technology research company, "[a] handful of hygiene measures can stop up to 95 percent of targeted cyber intrusions." In other words, simple, cost-effective actions can make a tremendous difference. In addition to practicing good cyber hygiene, SLTT governments, and critical infrastructure owners and operators can also leverage Department of Homeland Security resources to help further protect their cybersecurity systems and assets. DHS, specifically the Cybersecurity and Critical Infrastructure Security Agency, plays a key role in sharing cyber threat information and cyber hygiene practices. The Department also offers assistance to help these entities better protect their mission-critical systems, such as penetration testing, and it also offers recovery assistance if an incident does occur.

State and local governments and the private sector are on the front lines and grappling with these cyber threats every day. For example, this past August, Texas was hit by a coordinated ransomware attack. The ransom was not paid, but the response effort still cost the state hundreds of thousands of dollars. DHS assisted in the response through reverse engineering the malware, but according to state officials, additional improvements are needed. We can learn a great deal from the experiences of individual states and businesses, and identify areas for improvement.

I want to thank all of the witnesses for being here today, and I look forward to your testimony.

U.S. Senate Committee on Homeland Security and Governmental Affairs "What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"

OPENING STATEMENT OF RANKING MEMBER GARY C. PETERS
February 11, 2020
AS PREPARED FOR DELIVERY

"Thank you, Mr. Chairman, and thank you to all of our witnesses here today.

"I'm especially pleased that we have Chris DeRusha with us today. He is the Chief Security Officer for the State of Michigan, and an important partner in combatting cyber-attacks in our home state. Chris, I want to congratulate you on welcoming a baby boy last month and thank your family for allowing you to come to Washington while you are on paternity leave to share your expertise with us.

"The cyber threats facing our nation are becoming increasingly sophisticated and we are all at risk – families, government agencies, schools, small businesses, and critical infrastructure.

"In today's digital world, state and local governments are responsible for safeguarding everything from election systems to sensitive personal data, including social security numbers, credit card information and even medical records. State and local governments don't always have the tools to defend against cyber-attacks. Financial constraints, workforce challenges, and outdated equipment are all serious challenges for states and cities.

"Attackers always look for the "weakest link" and that's why we must ensure that everyone from small businesses to our state and local governments have the tools to prevent, detect and respond to cyber-attacks. That's why I have introduced commonsense, bipartisan legislation with my colleagues on this committee to help bolster our cyber security defenses at all levels of government.

"I introduced the bipartisan DOTGOV Act with Chairman Johnson and Senator Lankford to help state and local governments transition to the more trusted and secure dot-gov domain.

"I also introduced the State and Local Government Cybersecurity Act with Senator Portman. This will help DHS share timely information, deliver training and resources, and provide technical assistance on cybersecurity threats, vulnerabilities, and breaches with states and localities.

"In 2016 – in my home state of Michigan, hackers used a ransomware attack on the Lansing Board of Water and Light, forcing taxpayers to pay a $25,000 ransom to unlock the targeted computer systems. My bill would give cities and states the tools to prevent and respond to these kinds of attacks more effectively.

"Recently, Richmond Community Schools in Michigan were closed for a week due to a similar attack demanding a $10,000 payment. Luckily, their data was not compromised. But this attack exposes a dangerous vulnerability as schools maintain a considerable amount of sensitive records related to their students and employees – including family records, medical histories, and employment information.

"I introduced the K-12 Cybersecurity Act with Senator Scott to protect students and their data by providing better cybersecurity resources and information to K through 12 schools in Michigan and across the country.

"It is clear that these kinds of attacks are only growing and they pose a serious risk. I will continue working to ensure that all of our state and local governments have the resources, information and expertise they need to safeguard Americans.

"I will keep working with my colleagues on this important issue, and look forward to hearing from today's experts on what else the federal government can do to prevent cyber-attacks."

Testimony

Christopher Krebs
Director
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"

BEFORE THE
UNITED STATES SENATE

Homeland Security and Governmental Affairs Committee

February 11, 2020

Washington, DC

Chairman Johnson, Ranking Member Peters, and members of the committee, thank you for the opportunity to testify regarding the Cybersecurity and Infrastructure Security Agency's (CISA) support to state, local, tribal, and territorial (SLTT) and the private sector to mitigate cyber threats. Our mission is to defend against the threats of today and secure against the evolving risks of tomorrow. We work with partners across all levels of government and in the private sector to– "Defend Today, Secure Tomorrow."

CISA leads the Nation's efforts to ensure the security and resilience of our cyber and physical infrastructure. We assist agencies with the protection of civilian federal networks, and coordinate with other federal agencies, SLTT governments, and the private sector to defend our Nation's critical infrastructure from malicious cyber activity. By bringing together all levels of government, the private sector, international partners, and the public, DHS protects against cybersecurity risks, improves our whole-of-government incident response capabilities, enhances information sharing of best practices and cyber threats, and strengthens resilience of our Nation's critical infrastructure and protects our way of life.

Cyber Threats

Cyber threats remain one of the most significant strategic risks for the United States, threatening our national security, economic prosperity, and public health and safety. Advanced persistent threat actors, hackers, cyber criminals, and nation-states, have increased the frequency and sophistication of their attacks. In a 2018 report, *Foreign Economic Espionage in Cyberspace,* the U.S.'s National Counterintelligence and Security Center stated, "We anticipate that China, Russia, and Iran will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace." Our adversaries are developing and using advanced cyber capabilities in attempts to undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions.

Just last month, in response to increased geopolitical tensions and threats with Iran, CISA released a *CISA Insights Resource*[1] to inform our private sector and SLTT partners about enhanced risk and appropriate security postures. CISA also actively shared information with thousands of public and private sector stakeholders across the critical infrastructure community through regular, coordinated teleconferences. This is dynamic, two-way communication in real time. CISA provides information and stakeholders have a forum to share their experiences, ask questions and get answers. Additionally, CISA coordinated closely with other federal partners and the intelligence community to ensure a coordinated response to the potential threats. These activities will be replicated as the cyber threat landscape continues to evolve.

Cybersecurity threats are all around us, but Ransomware is a specific type of cyber threat that has been in the news a great deal lately. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected

[1] *CISA Insights: Ransomware Outbreak.* Cybersecurity and Infrastructure Security Agency. August 21, 2019. Accessed at: https://www.us-cert.gov/sites/default/files/2019-08/CISA_Insights-Ransomware_Outbreak_S508C.pdf

website. In a typical ransomware attack, hackers have the ability to take over a system, locking out owners and operators and potentially disabling the system functions or holding the system information hostage until a ransom is paid. Ransomware can be devastating to an individual or an organization in the form of critical public safety services suspended, personal information at risk and potentially millions in financial loss possible. Anyone with important data stored on their computer or network is at risk.[2] In 2017, WannaCry was a global example of ransomware that opened our eyes to the potential breadth and depth of the harm that such attacks could cause. Ransomware continues to be a major threat facing US critical infrastructure, SLTT, and the private sector.

Ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our nation's networks. Unfortunately, ransomware seems to be a business model that works, and victims are paying higher and higher ransoms.[3] According to a recent report from EMSISOFT, in 2019 ransomware attacks impacted at least 966 government agencies, educational establishments and healthcare providers at a potential cost of $7.5 billion. A further breakdown shows 113 state and municipal governments and agencies, 764 healthcare providers, and 89 universities, colleges, or school districts were impacted by ransomware.[4]

Between 2018 and 2019, several of the largest US cities fell victim to this type of cyber attack. In 2018, ransomware impacted the city of Atlanta, including its city services and programs.[5] In November of 2018, the Justice Department announced criminal charges against two Iranian citizens in a series of ransomware attacks against Atlanta, Newark, New Jersey, Port of San Diego, the Colorado Department of Transportation, a university, and multiple hospitals using the SamSam Ransomware.[6] In 2019, ransomware infected Baltimore city government computers, demanding a payment of thousands of dollars to free systems.[7] This past December, New Orleans declared a state of emergency due to a ransomware attack, prompting a shutdown of digital services.[8] This represents only a few of the reported ransomware attacks on state and local governments. It's important to note that all statistics we discuss today are based on the landscape of known or reported attacks. A significant concern with ransomware attacks is that we do not know how many incidents go unreported.

CISA Services

In an effort to protect against and respond to evolving cyber threats, CISA offers technical services ranging from proactive vulnerability scanning to malware analysis. CISA leverages technical expertise during cyber incidents providing mitigation recommendations and ensuring that threats are widely known. CISA provides exercises and training programs to

---

[2] https://www.us-cert.gov/Ransomware
[3] Catalin Cimpanu. "The average ransom demand for a REvil ransomware infection is a whopping $260,000." *ZDNet*. January 28, 2020. Accessed here: https://www.zdnet.com/article/the-average-ransom-demand-for-a-revil-ransomware-infection-is-a-whopping-260000/
[4] "The State of Ransomware in the US: Report and Statistics 2019," ENSISOFT Malware Lab. December 12, 2019. Accessed at: https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/
[5] Benjamin Freed. Atlanta was not prepared to respond to a ransomware attack. *StateScoop*. April 24, 2018. Accessed at: https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/
[6] Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses. Press Release. Department of Justice. November 28, 2018.
[7]Ian Duncan and Colin Campbell. "Baltimore city government computer network hit by ransomware attack." *The Baltimore Sun*. May 7, 2019. Accessed at: https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html
[8] Kristen Korosec. "New Orleans declares state of emergency following ransomware attack." *TechCrunch*. December 14, 2019. Accessed at: https://techcrunch.com/2019/12/14/new-orleans-declares-state-of-emergency-following-ransomware-attack/

critical infrastructure partners around the nation. We help build awareness of an evolving threat as well as increase understanding of what steps to take to mitigate these threats. CISA offers incident management and response capabilities through sharing, and analysis. We also offer response to cyber threats--such as sending experts to Ukraine to assist in the aftermath of the 2015 attack on Ukraine's electric grid.

During the global ransomware attacks in 2017, then NPPD, now CISA, collaborated domestically and internationally to protect critical infrastructure and federal networks. (For example, we conducted malware analysis on multiple samples of the suspected threat vector and collaborated with commercial service providers to discover and share indicators related to the ransomware.) Additionally, CISA issues technical information for network defenders around the globe , enabling them to reduce their exposure to mitigate the consequences of an attack. When the RobbinHood ransomware attack occurred, CISA, in conjunction with the FBI, promptly shared our analysis of the vulnerabilities that the malicious cyber actors were able to exploit.

In July 2019, CISA released a joint statement with our partners at the Multi-State Sharing and Analysis Center, (MS-ISAC), the National Governor's Association (NGA) and the National Association of State Chief Information Officers (NASCIO) with three simple, actionable steps to increase state and local resilience against ransomware. These steps included, Back Up Your System; Reinforce Basic Cybersecurity Awareness and Education; and Revisit and Refine Cyber Incident Response Plans.

In the fall of 2019, CISA released several resources aimed at assisting its stakeholders in raise the level of their cybersecurity practices. These resources include:

- ***CISA Insights - Ransomware Outbreak*:** The Insights document focuses on Ransomware and building a better understanding of how attacks are taking place and what actions can be done to mitigate such attacks. The document includes elements like: backing-up data, system images, and configurations and keep the backups offline; updating and patching systems; reviewing and exercising incident response plans; and asking for help from CISA, the FBI, or the Secret Service.

- ***CISA's Cyber Essentials***: The Essentials document is a guide for leaders of small and medium businesses as well as leaders of state, local, tribal and territorial government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.

- ***Ransomware Cyber Tabletop Exercise Package:*** Commonly referred to as "exercise in a box," the Exercise Package is as a resource for state, local, and private sector partners that includes template exercise objectives, scenario, and discussion questions, as well as a collection of ransomware and cybersecurity references and resources. Partners can use the exercise package to initiate discussions within their organizations about their ability to address the threat of ransomware, which is impacting the community with increasing frequency.

CISA Insights, Cyber Essentials and other materials, including a webinar on Ransomware, viewed over 4,000 times, are available online at www.us-cert.gov/ransomware to assist state and local governments, and small and medium-sized businesses.

At CISA, we believe that there are six key attributes of a successful cyber program. Two strategic attributes are leadership engagement and a culture of security. Two technical attributes are knowing what is on your network and knowing who is on your network. Finally, the two tactical attributes are being able to recover after an incident, utilizing backups that have been tested and having a plan in place that includes outreach to employees, public, etc. CISA actively coordinates with our state and local stakeholders to better understand the support they need to defend their systems from a ransomware attack. CISA utilizes a layered approach to supporting SLTTs through direct assistance, indirect assistance, and self-service capabilities to raise their level of cyber resilience. CISA funds the MS-ISAC, that not only provides a range of free services, but also serves as a network where SLTT agencies can share best practices and lessons learned with each other. Additionally, our partnerships with the private sector are essential. Private sector companies are regularly called in to help victims rebuild systems. We need partnerships and input from them as we continue to build out and strengthen our incident efforts.

CISA will continue to raise awareness of the threat, sharing key actions that make organizations harder, more resilient targets. Additionally, we have come together with our other interagency partners to build-up a ransomware campaign working through the FBI's National Cyber Investigative Joint Task Force (NCIJTF).

CISA Cybersecurity Operations

CISA provides entities with information, technical assistance, and guidance that they can use to secure their networks, systems, assets, information, and data by reducing vulnerabilities, ensuring resilience to cyber incidents, and supporting their holistic risk management priorities. CISA also does allied tasks in the physical critical infrastructure and communications coordination mission areas. CISA operates at the intersection of the Federal Government, state and local governments, the private sector, international partners, law enforcement, intelligence, and defense communities. The *Cybersecurity Act of 2015* (P.L. 114-113) established DHS as the Federal Government's central hub for the sharing of cyber threat indicators and defensive measures. By focusing on rapid sharing of the technical features that permit network defenders to identify and respond to threats while minimizing the receipt of personally identifiable information, CISA's automated indicator sharing capability allows the Federal Government and private sector network defenders to share technical information at machine speed. This sharing provides greater situational awareness for all sectors and entities across an ever-evolving threat landscapes.

CISA, our government partners, and the private sector are all engaging in a more strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity. In May of 2018, the Department published the *DHS Cybersecurity Strategy*, outlining a strategic framework to execute our cybersecurity responsibilities during the next five years. The *National Cyber Strategy*, released in September 2018, reiterates the criticality of collaboration and strengthens the government's commitment to work in partnership with industry

to combat cyber threats and secure our critical infrastructure. Together, the *National Cyber Strategy* and *DHS Cybersecurity Strategy* guide CISA's efforts.

The National Cybersecurity Incident Response Plan (NCIRP), required by Presidential Policy Directive 41, outlines how the US government will respond to a significant cyber incident. The plan addresses the various roles of the private sector, state and local governments, as well as multiple federal agencies. DHS, acting through CISA, is the lead for asset response during a significant cyber incident. CISA's asset response activities include providing technical instance to affected entities, mitigating vulnerabilities and impacts of a cyber incident. CISA is also responsible for identifying additional entities that may be affected and assessing risks of cascading impacts. Lastly, CISA is responsible for facilitating information sharing and operational coordination.[9]

Conclusion

In the face of increasingly sophisticated threats, CISA employees stand on the front lines of the Federal Government's efforts to defend our Nation's federal networks and critical infrastructure. The threat environment is complex and dynamic with interdependencies that add to the challenge. As new risks emerge, we must better integrate cyber and physical risk in order to effectively secure the Nation. CISA contributes unique expertise and capabilities around cyber-physical risk and cross-sector critical infrastructure interdependencies.

I recognize and appreciate the committees strong support and diligence as it works to understand this emerging risk and identify additional authorities and resources needed to address it head on. We at CISA are committed to working with Congress to ensure our efforts cultivate a safer, more secure, and resilient Homeland through our efforts to defend today and secure tomorrow.

Thank you for the opportunity to appear before the Committee today, and I look forward to your questions.

[9] National Cyber Incident Response Plan, Department of Homeland Security, December 2016.

Statement Before the United States Senate Committee on Homeland Security and Governmental Affairs

"What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity."

Testimony of Amanda Crawford

Executive Director

Texas Department of Information Resources

February 11, 2020

Chairman Johnson, Ranking Member Peters, and members of the committee,

My name is Amanda Crawford, and I serve as the Executive Director for the Texas Department of information Resources ("DIR"). Thank you for inviting me to testify today. The mission of DIR is to serve Texas government by leading the state's technology strategy, protecting state technology infrastructure, and offering innovative and cost-effective solutions for all levels of government. We achieve this mission through a variety of ways including a robust Shared Technology Services – or managed IT-as-a-Service – program that allows entities at all levels of Texas government to focus their limited resources on mission rather than managing technology, and a multi-billion dollar cooperative contracts program that harnesses the buying power of the State of Texas to provide eligible government customers throughout the country with IT goods and services at aggressive discounts without a lengthy procurement process. DIR also sets the technology strategy for the State of Texas and, as you'll hear later in my testimony, plays a significant role in helping secure Texas from cyberattacks.

I would like to provide the committee with an overview of the August 2019 ransomware attack that impacted 23 local governments in Texas, focusing on the federal and state response and recommendations for the future. I will also discuss how Texas leverages cyber threat information from the Department of Homeland Security ("DHS") to protect its mission critical systems and assets. Finally, I will discuss the voluntary assistance provided by DHS-CISA to help Texas identify and address vulnerabilities, as well as avenues to make that assistance more robust.

State preparation and cooperation were the keys to the successful Texas response to the August 2019 Ransomware Incident.

As the State of Texas' technology agency, DIR is charged with many duties by statute. One of our primary missions, and the one I am here to speak with you about today, is cybersecurity. Our role in this space is two-fold. First, we serve as the internet service provider and network security operations center for many Texas state agencies. In that role, we detect and block malicious traffic over our networks. Second, the Office of the Chief Information Security Officer of Texas is a part of DIR. That office provides statewide information security program guidance to state agencies, institutions of higher education, and other governmental entities. Led by the

State of Texas Chief Information Security Officer, Nancy Rainosek, the team works to set state information security policies and standards, publish guidance on best practices, improve incident response preparedness, monitor and analyze incidents, coordinate security services, and promote information sharing throughout the public sector cybersecurity community. It was this second role, through the Office of the Chief Information Security Officer, that DIR was called into action to assist the 23 local government entities who were simultaneously attacked in the same ransomware event last August.

The attack began early in the morning on Friday, August 16, 2019. As public servants across the state came to work and discovered that their systems had been compromised and held hostage by ransomware, reports began filing into us at DIR. DIR was notified at 8:36 AM that eight local government entities across the state had been attacked. Over the next two hours, eleven more reports came in, and at approximately 10:30 AM it was reported that one of the impacted municipality's Supervisory Control and Data Acquisition ("SCADA") system had been rendered inoperable in the attack. This SCADA system controlled the monitoring and distribution of the entire local community's water supply. Given the number of entities impacted and the very real public health and safety threat, I notified the Office of the Governor to discuss the need to issue a disaster declaration.

Shortly after 11:00 AM, Governor Abbott issued the State of Texas' first statewide disaster declaration for a cyber event. With the Governor's disaster declaration, the Cybersecurity Annex to the Texas Emergency Management Plan was put into action. The disaster declaration also activated the Texas Division of Emergency Management's ("TDEM") State Operations Center ("SOC") to Level Two – meaning 24/7 operations. By noon, the SOC was fully active with state and federal incident responders reporting to the SOC. Leveraging the well-practiced logistics expertise of TDEM, Texas was able to have the first coordination call with all potentially impacted entities at 2:30 PM. Over the course of the incident, 23 impacted entities would be identified. The makeup of the victim pool was a representative sample of local governments across Texas.

By noon the following day, Saturday, August 17, 2019, Texas incident responders had identified and prioritized all impacted entities. By end of day Sunday, August 18, 2019, incident responders had made in-person visits to all impacted entities across Texas. And by the end of the day Friday, August

23, 2019 – one week after the incident began – all impacted entities had been remediated to the point that state support was no longer required.

While by no means perfect, the Texas response to this cyber event was a successful one. No ransom was paid in this event. While we are still collecting total costs to rebuild from the impacted entities, the current total cost for the state response is approximately one-tenth of the $2.5 million ransom demanded by the criminals responsible for this attack. The ability to bring these entities back online and into the rebuilding phase within one week can be attributed to extensive preparation and cooperation between the responders. In preparation for an event such as this, Texas took the following steps:

- **Senate Bill 64 (2019):** This legislation amended the definition of a disaster to include a cybersecurity event. Additionally, the bill allows the Governor to order the Texas National Guard to assist with defending Texas' cyber operations.
- **Cybersecurity Annex to the Texas State Emergency Management Plan**: In 2017, House Bill 8 called for DIR to create a statewide cybersecurity incident response plan. DIR coordinated the plan's development with the Texas Division of Emergency Management, the Texas Department of Public Safety, and the Texas Military Department. DIR held incident handling training and incident response exercises with response partners to ensure the ability to quickly operationalize the cybersecurity annex.
- **Managed Security Services Contract**: Through DIR's Shared Technology Services program, state and local governments can utilize a pre-negotiated cyber incident response contract with a managed security services vendor with no retainer fee. All contractors under this service are background-checked in advance so they are ready to assist on demand. Through the DIR contract, we have established competitive pricing as well as service level agreements for guaranteed response times and service quality and delivery.
- **State Operations Center**: Utilization of TDEM's State Operations Center was a key driver in our success. TDEM is prepared for communicating with the local entities through its district disaster coordinators and has critical tools to communicate with field teams. Additionally, local governments are accustomed to the communication channels from TDEM.

The other key to the Texas success in this event was the collaboration and cooperation of state and federal partners. Per the State of Texas Cybersecurity Annex, DIR led the incident response effort. Other state responders included:

- Texas Military Department (field incident response)
- Texas Division of Emergency Management (State Operations Center and logistics support)
- Texas A&M University System's Security Operations Center/Critical Incident Response Team (malware reversal, field support, and impact analysis)
- Texas Department of Public Safety (image capture)
- Public Utility Commission of Texas (consultative work)
- Texas Water Development Board (consultative work)
- Private sector vendors – both paid and volunteer – (field incident response)

Federal responders included:

- Federal Bureau of Investigation (criminal investigation)
- Department of Homeland Security (observation and malware reversal)
- Federal Emergency Management Agency (observation)

Texas greatly appreciates the participation of its federal partners in this event. The FBI teams worked well with the Texas responders and quickly assimilated with the other responders on this joint effort. They provided clear and timely information to us and were excellent partners on the forensic side of this mission. DHS-CISA also provided reverse engineering of the malware. However, early in the August event, there were miscommunications between DHS-CISA and state responders. These miscommunications primarily resulted from role confusion and a lack of clarity concerning what resources DHS-CISA could provide to help Texas. We have worked jointly to put plans in place to avoid the same missteps in the future. DHS-CISA has since initiated multiple meetings with DIR to address our concerns and propose solutions. Our communications with DHS-CISA have improved as a result of the August event.

Recommendations for improving federal participation include:

- **Better sharing of classified information with state government:** Currently, our receipt of timely and complete classified information about cyber threats facing our systems is sporadic.
- **Increasing DHS-CISA resources per region:** Having a dedicated resource to work with the Chief Information Security Officer of each state would help to drive incident response planning and preparedness and would better integrate federal resources into each state.
- **Clearly communicating what federal resources are available to state and local governments and how to receive those services:** Because these large-scale cyber incidents are a relatively recent development, clear delineations of roles and responsibilities have not been sufficiently communicated from the federal government to the state and local level. Multiple federal agencies provide cyber assistance of some sort and it can be challenging and inefficient, particularly in the middle of a cyber event, to know what help is available and who to call. A single federal point of contact who can then coordinate with other potential federal resources would be helpful.
- **Balancing the law enforcement need to protect investigations with the ability to share information about active threats:** It is critical to be able to share information with the cybersecurity community to prevent the same attack from occurring elsewhere. While we understand law enforcement's goal of catching the criminals responsible for these attacks, the ability to release more specific information would be helpful for the information security community who protects critical assets.

The interagency cooperation that occurred during this event is a testament to how government agencies at the federal, state, and local level can effectively work together to respond to critical events. No single agency could have responded successfully to the August ransomware incident. Absent these incident responders, the 23 local entities would have had great difficulty responding to the event without either paying the ransom or spending considerable time and resources trying to handle the situation on their own. While the August event was the first statewide cyber disaster declared in Texas, it will likely not be the last. We must prepare, as a state, for the next event, building and improving on our existing plan and anticipating what the next generation of cyber warfare will look like. Unfortunately, cyberattacks on state and local governments have become our new normal.

For example, DIR knows of 57 ransomware events that impacted state and local governments in Texas in 2019. This information comes from various sources including self-reporting, news articles, and partner notifications, as there is currently no statutory requirement for local government to report these events to DIR.

Organization Type	Number of Incidents
Cities	24
Counties	8
School Districts	15
Other Local Entities	6
State Agencies/Universities	4

Table 1: Ransomware Events Affecting Texas Governmental Entities in 2019

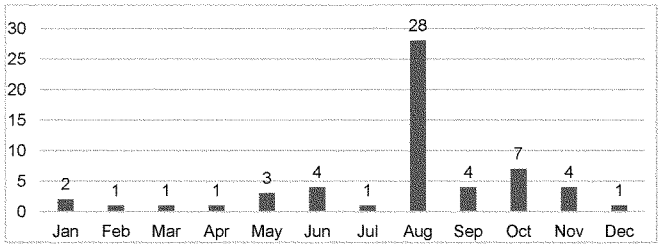


Chart 1: 2019 Texas Ransomware Incidents by Month

As Texas continues to face these events in 2020, MS-ISAC and DHS-CISA can be a valuable source for ransomware information, particularly at the local government level. Tracking trends and patterns can improve our education and outreach efforts and our ability to stop the next incident from occurring. Coordinated ransomware information sharing would be beneficial at both the state and national level.

Information received from DHS-CISA is one of the many valuable tools Texas uses to protect its critical assets and infrastructure. Additionally, DIR has a large Texas state and local government network for sharing information received from DHS-CISA.

Most of the federal information that Texas receives to improve the state's cybersecurity posture comes from the Multi-State Information Sharing and Analysis Center ("MS-ISAC"). This information consists of alerts from the Albert intrusion detection sensors and threat intelligence feeds with valuable indicators of compromise. Additionally, we benefit from their Vulnerability Management Program which provides website compromises, malware alerts, and notifications of compromised credentials.

The Albert sensors are a valuable addition to other intrusion detection capabilities at the state's Network Security Operations Center ("NSOC"), which is operated by DIR. These Albert sensors monitor inbound and outbound internet traffic and provide ransomware alerts to our NSOC. These alerts are actionable and have a low false-positive rate, which allows the DIR NSOC to take immediate steps to mitigate these cyber events.

The state also receives monthly reports from the MS-ISAC Vulnerability Management Program. This report notifies the state on outdated software that could pose a threat to state and local government systems. Using this report, DIR identifies and shares this information with our agency customers that own or maintain a vulnerable system. Because this is a comprehensive view of vulnerabilities across state and local entities in Texas, the report is voluminous and takes considerable time to review, assess, and then ultimately inform the potentially impacted entities. If this information could be shared in a more easily accessible format, it would enable states to send this information out to their vulnerable government entities more quickly.

Additionally, MS-ISAC is the state's main source of information regarding website defacements, particularly at the local government level. In fact, in

2020 alone, we have been informed of more than a dozen website defacements throughout Texas.

DIR also participates in pilot programs funded by DHS-CISA. Through these programs, Texas gains valuable information on strategies and new technologies to enhance the state's cybersecurity posture. For example, Texas is one of three states participating in a Johns Hopkins Security Orchestration and Automated Response ("SOAR") pilot funded by DHS-CISA. This will enable an automated update of indicators of compromise to decrease the time between discovery and mitigation of risk. Currently, DIR's NSOC cannot receive, and therefore cannot benefit from, automated updates from the Albert sensors because there are federally classified filters on these sensors. After the pilot is complete, if successful, Texas will still have to invest in orchestration tools at the state's expense.

DIR maintains a large mailing list of state and local government cybersecurity personnel to share all information received from various federal agencies, including DHS-CISA, MS-ISAC, and the FBI. We provide actionable and immediate alerts when necessary, and produce a weekly update consolidating other alerts. In addition, DIR hosts a monthly meeting during which we update the Texas cybersecurity community on significant issues and provide tabletop exercises, some of which are provided by MS-ISAC. Further, DIR is in the process of establishing the Texas Information Sharing and Analysis Organization for sharing threat and vulnerability information with both the public and private sector in Texas. This will tie together the federal and state information sharing efforts. Texas stands ready to share all timely and complete cybersecurity information that DHS-CISA can provide.

While the Department of Homeland Security offers many voluntary services, the wait times for receiving such services make them ineffective for securing Texas systems and critical assets.

DHS-CISA services that have been leveraged by Texas have been very valuable. Of note, the Texas Secretary of State had an election security assessment and penetration test provided by DHS-CISA which included testing of the State of Texas' consolidated data centers. That assessment provided good insight and actionable feedback on steps Texas could take to further improve the security posture of its systems. However, most of these voluntary services are not readily available for state and local governments.

If these services had more immediate availability, they could help state and local governments drive continuous improvement in cybersecurity. As it stands today, the wait times on some of these services can be a minimum of eighteen months. In cybersecurity, the entire threat landscape can change quite rapidly; and in technology eighteen months represents a full generation of change and advancement. Assessment and testing are only valuable if they are timely.

However, we are seeing improvements in communications and finding new ways to work with our DHS-CISA partners. One such novel engagement will occur in March at DIR's 20th annual Texas Information Security Forum ("ISF"), where over 400 state and local government security personnel gather to gain current cybersecurity education. This Forum is hosted by the State of Texas and free for any government security employee in the state to attend. DHS-CISA is working with DIR to provide an incident management workshop at the ISF. This workshop will consist of an overview of the process of detecting, analyzing, responding to disruptive events with the goal of mitigating the impact of a disruptive event and improving systems and processes to avoid future incidents.

As mentioned above, MS-ISAC is a valuable partner for Texas' cybersecurity program. They provide critical information sharing services and, when the partnership is working, it works well. Of course, no partnership is without room to improve. One area needing improvement is in event notification. Frequently, MS-ISAC will not inform the state when an incident has occurred at a local government entity somewhere in the state. This puts both the state and the local government entity at a significant disadvantage. In these cases, the state is unable to provide any assistance that would normally be available to the local government during their incident. Additionally, the states cannot collect data on attack trends or conduct pattern analysis to better protect state interests. States cannot respond if they are not notified.

In summary, DHS-CISA and the MS-ISAC provide valuable information and services to Texas when it comes to protecting its critical assets and information. While improvements can be made, we are engaged in continuing dialogue with both organizations to evolve the services and information we receive. Texas stands ready to assist in the continuing effort to enhance the security of our nation's assets and provide input when needed.

On behalf the state of Texas, I want to thank the Committee for addressing this important issue and inviting me to share our perspective with you. Thank you for your time and attention. I look forward to answering your questions.

WRITTEN TESTIMONY

OF

CHRIS DERUSHA
CHIEF SECURITY OFFICER
STATE OF MICHIGAN

FOR A HEARING ON

"WHAT STATES, LOCALS, AND THE BUSINESS COMMUNITY SHOULD KNOW AND DO: A ROADMAP FOR EFFECTIVE CYBERSECURITY"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Tuesday, February 11, 2020
Washington, D.C.

Thank you to Chairman Johnson and Senator Peters for inviting me to speak today on the subject of cybersecurity among states, localities, territories, and tribal governments. As the Chief Security Officer for the State of Michigan, this is a fantastic opportunity for me to highlight the steps we are taking to better secure our state and discuss some of the challenges we face.

It is no surprise to the members of this committee that the threat environment we face is daunting. Attacks on government organizations at all levels continue to increase and demonstrate the ever-expanding capacity of our adversaries. State of Michigan firewalls repel over 90 million potentially malicious probes and actions every day, and we are not unique. To defend our networks and the data entrusted to us by our residents, state and local cybersecurity leaders are taking proactive steps to improve protections. States are often hailed as the "laboratories of democracy." In the face of determined and well-resourced opponents, states are proving all across the country that we are test beds for cybersecurity innovation as well.

Cybersecurity in the State of Michigan

In the State of Michigan, the state government's information technology (IT) and cybersecurity are centralized under the Department of Technology, Management, and Budget (DTMB). Centralization enables the state to enforce common security policies, standards, and controls across state agencies and leverage economies of scale when procuring new technology. Benefits include a robust risk assessment and security accreditation process for all new systems and applications, the ability to apply governance and enforce security policies, standardized cyber awareness training and phishing exercises, and a common operating picture of threats facing the entire state government enterprise. In Michigan, several organizations have cybersecurity-related responsibilities, but all have different missions:

- Michigan Cyber Security (MCS): Information security for the State of Michigan is managed by MCS within DTMB. The Michigan Security Operations Center hosts advanced security capabilities such as threat hunting, incident response, digital forensics, and vulnerability management.
- Michigan Cyber Command Center (MC3): The Michigan State Police's MC3 coordinates cybersecurity-related activities as they relate to emergencies and computer-based crimes. Whereas MCS is focused on the state government's information assets, MC3's purview extends to all of Michigan.
- National Guard: Michigan is fortunate to have both Air and Army National Guard Units with cybersecurity capabilities. The State of Michigan is working closely with our colleagues in the Guard to formalize how we can operate together in times of emergency, and next month will mark the first National Guard assessment of one of a state agency's cybersecurity capabilities.
- Michigan Cyber Civilian Corps (MiC3): Designed to leverage Michigan's cybersecurity talent, the MiC3 program allows qualified cyber professionals from across all industries to volunteer their services to respond to cybersecurity events on behalf of the state.

In 2015, the state developed the Michigan Cyber Disruption Response Plan (CDRP) to delineate roles and responsibilities between MCS, MC3, and the National Guard, who all work closely together to prevent and respond to cyber events. The CDRP clearly sets forth chains of command, delineation of responsibilities, and processes for escalation, decreasing the chaos that often accompanies major security incidents. However, as I recently told a group of local officials, the value of a response plan can be significantly reduced if it is not tested. It is for this reason that the State of Michigan conducted a functional exercise this past November that simulated major compromises at two large state agencies and involved numerous senior decision makers. Armed with the results of the exercise, we are currently

updating our processes to ensure we are using best practices that reflect the realities of both our adversaries and our defenses.

Federal Assistance to the State

While the close working relationship between DTMB, Michigan State Police, and the National Guard is essential to defending the state's public and private networks, another key relationship is the one we share with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). As a former DHS cybersecurity official, I understand the tremendous resources DHS can bring to bear as well as its eagerness to do so. Michigan is fortunate to have a CISA cybersecurity liaison who helps us coordinate with our national-level partners, saving us from navigating the Federal bureaucracy on our own. By having a direct line to DHS, we are able to incorporate a Federal perspective into our decisions and better understand the resources available to us. Providing such resources to every state, as described in **S. 3207, the *Cybersecurity State Coordinator Act***, would be a major asset to state and national cybersecurity efforts by ensuring greater continuity between the efforts of states and the Federal Government. It would also provide a stronger state voice within CISA, helping them to better tailor their assistance to states and localities.

Similarly, **S. 1846, the *State and Local Government Cybersecurity Act*** would help states like Michigan access resources, tools, and expertise developed by our Federal partners and national cybersecurity experts. This includes making available to state and local governments the experts at DHS's National Cybersecurity and Communications Integration Center for training and consulting. It would also afford these organizations with greater access to security tools, policies, and procedures to help drive vital improvements.

I want to sincerely thank the Chairman, Ranking Member, and numerous members of this Committee for their bipartisan leadership on this legislation and support all efforts to see both bills be enacted into law.

Beyond the State: Securing the Digital Ecosystem

The Federal Government and most state governments operate largely decentralized models in which every department and agency must provide for itself. Under this system, some agencies build mature cybersecurity operations while others have little to no ability to defend themselves. Agencies also end up competing against each other for scarce cybersecurity professionals. The interconnected nature of the digital age means securing a system or network can no longer be achieved by simply protecting oneself. Governments at the Federal, state, and local levels interact with each other digitally every day, and improving the security of any of these levels of government require enhanced security capabilities for the others.

However, as difficult as the current environment is for states, it is even more perilous for counties and localities. As much as state IT and cybersecurity programs face shortages of human and financial resources, these are even more scarce for smaller units of government. For instance, of Michigan's 83 counties, which are home to approximately 10 million people, only three have uniquely designated Chief Information Security Officers with dedicated time and authority to address cybersecurity for their organizations. Even their websites face legitimacy challenges as few use the .gov domain, opting instead for the easier to obtain .com. .net, or .org domains. To give a sense of scale, Michigan has over 2,000 local government-affiliated entities: counties, cities, villages, townships, K-12 and higher education institutions, transit and utility authorities. In fact, there are only approximately 8.5 percent of all eligible

local governments across the country on the .gov domain, according the General Services Administration (GSA).

Understanding these challenges, I am pleased to see steps are being taken at both the state and Federal levels to help these county and local governments. S. 2749, the DOTGOV Act seeks to ease the process for these governments to obtain .gov domain names, providing the sites themselves with greater security and offering greater assurances to residents that they are, in fact, looking at a government website. The bill also charges DHS with providing information to make the transition to the .gov domain easier and provides the Director of CISA with greater authority to waive associate fees if he or she deems it necessary. Passage of S. 2749 would certainly go a long way in providing greater security assurance for local and county government websites.

The State of Michigan has also been proactive in developing new ways to provide support to county and local government systems and networks. One of these efforts was dubbed the "CISO-as-a-Service" initiative, which leveraged a centralized pool of cybersecurity experts to advise a pilot group of counties and cities on their security posture. While the results were positive for 13 communities, the model proved to be unscalable when targeting the 2,000+ local entities across the state. However, leaning on the experience gained from the pilot, we created the Cyber Partners Program. This program pulls together the IT and cybersecurity leadership of county and local governments across the state and provides a forum for combatting current challenges and disseminating best practices and information. Cyber Partners is currently piloting a new initiative that would utilize a framework of priority security controls that county and local government could use to better understand the state of their security protections, develop prioritized plans to improve their posture, and potentially, seek additional consultative assistance. While securing county and local IT is an important end unto itself, our efforts in this area have also been essential as the State of Michigan, and the country at large, prepare for the upcoming 2020 elections.

In addition to helping counties and localities improve their defensive postures, Michigan has also taken steps to help them respond to incidents when they occur. As previously noted, the MiC3 is an organization of qualified cybersecurity professionals who have volunteered their skills should an incident occur at critical infrastructure, county or local government organizations. Currently approximately 100 members strong, the group has helped numerous organizations respond to significant compromises of their systems, including ransomware attacks, and helped them reestablish operations. With members from across the state, MiC3 significantly expands Michigan's ability to secure its information landscape.

While the security of government entities, be they state, local, or otherwise, is important, our digital ecosystem is ultimately made up of individuals. Every year, the theft of personal information from Americans, including Michiganders, costs our economy billions of dollars. To combat this dangerous trend, the State of Michigan is exploring options to provide greater protections for our residents. This could include a free mobile app that would help residents secure their mobile devices from cyber criminals, reducing the potential of fraud. The app is designed not only for security, but for privacy, collecting no identifying information and even receiving the approval of the ACLU. By helping our residents become more secure, we help all levels of government become more secure as well.

Our country's state and local governments are on the frontlines of today's digital conflict, attacked daily by highly resourced advanced persistent threats, and there remains a great deal of work in order to secure the networks we rely on to provide essential services to the public. The State of Michigan greatly

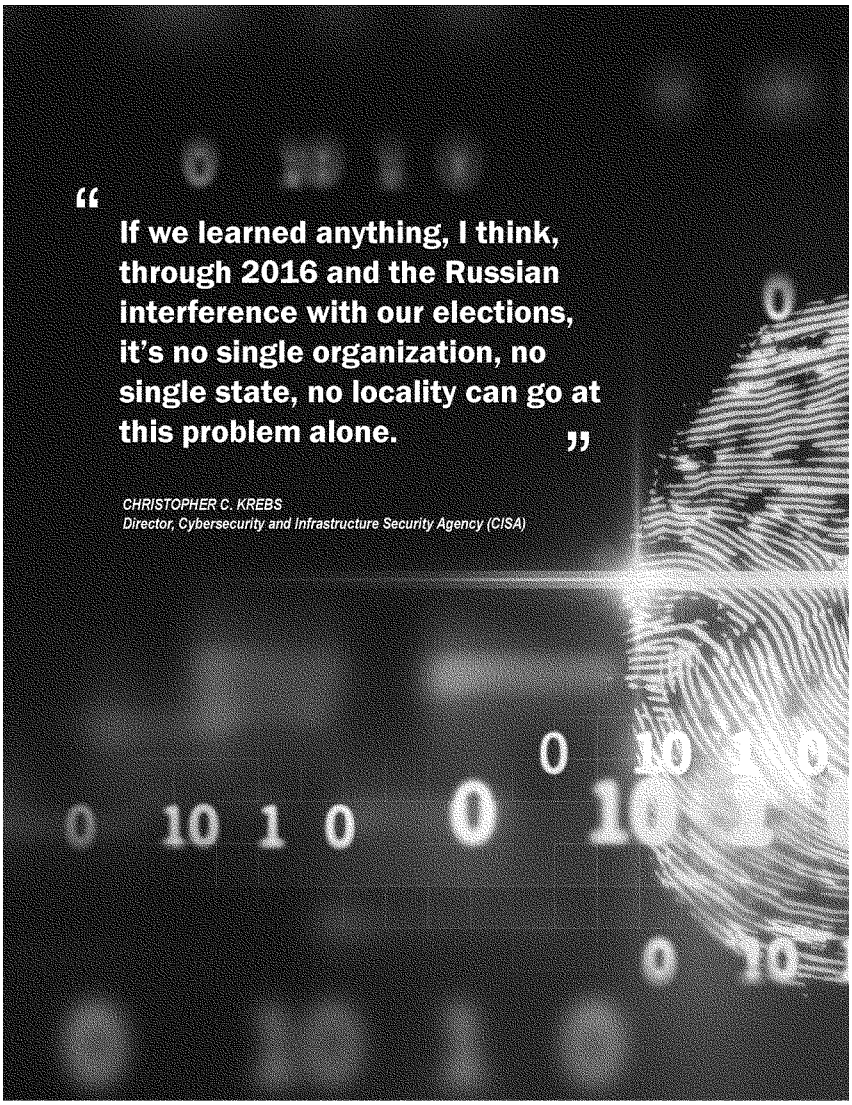
appreciates the attention paid to this issue by the members of this committee and we look forward to continuing to work with you all to secure our critical infrastructure and protect our residents.

CISA
CYBER+INFRASTRUCTURE

#Protect2020 Strategic Plan

FEBRUARY2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency


“
If we learned anything, I think, through 2016 and the Russian interference with our elections, it’s no single organization, no single state, no locality can go at this problem alone.
”
CHRISTOPHER C. KREBS
Director, Cybersecurity and Infrastructure Security Agency (CISA)

CONTENTS

02

Message From the Director

CHRISTOPHER C. KREBS
Director, Cybersecurity and Infrastructure Security Agency (CISA)

Election security is a top priority for the U.S. Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). As the lead federal agency responsible for securing the Nation's elections infrastructure, CISA works closely with the intelligence community, law enforcement officials, private sector partners, and others across the Federal Government to ensure we are doing everything possible to defend our electoral systems. But this needs to be a whole of nation effort. State and local election officials are on the front lines, and the role of the Federal Government is to make sure that they are prepared.

Ultimately, CISA's efforts depend on the trust and cooperation of state and local officials. Those relationships are strong and growing stronger. CISA's #Protect2020 initiative will engage officials from all fifty states, District of Columbia, and partisan organizations. We are working to make it harder for adversaries to compromise our systems and to enhance our resilience so that Americans know their votes will count—and will be counted correctly.

Guiding Principles

Customer Oriented
Emphasizing stakeholder needs and delivering rapid solutions

Resilient
Building stakeholder capabilities to resist malicious actors and recover rapidly from attacks

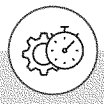
Adaptive
Developing creative solutions to a rapidly evolving threat landscape

Strategic Planning Overview

03

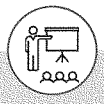
> **There's no question that our election process is more resilient and secure than it was in 2016, and heading into 2020 it will certainly be more secure than it was in 2018.**

Matt Masterson
Election Security Initiative, Senior Cybersecurity Advisor



Vigilant
Continuously monitoring threat trends and forecasting future vulnerabilities to provide timely services and information

Trustworthy
Safeguarding the trust and information of our partners and the American public



Transparent
Sharing information quickly and effectively

Background & Authority

In January 2017, DHS designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country. It gave federal agencies authority to assist in election security, but strictly in a supporting role. Under the Constitution, the responsibility for carrying out elections rests with state and local officials.

The President directed DHS to lead federal efforts to protect election infrastructure. DHS provides voluntary assistance and support to state and local officials in the form of advice, intelligence, technical support, and incident response planning—with the ultimate goal of building a more resilient, redundant, and secure election enterprise.

During the 2018 midterm Election cycle, DHS established the Election Task Force (ETF) and the Countering Foreign Influence Task Force (CFITF) to coordinate federal support to the election community. ETF and CFITF have now been institutionalized as the Election Security Initiative (ESI) within CISA. CISA works in coordination with various federal partners, such as DHS' Office of Intelligence and Analysis (I&A) and the Federal Bureau of Investigation (FBI), as well as non-federal election stakeholders.

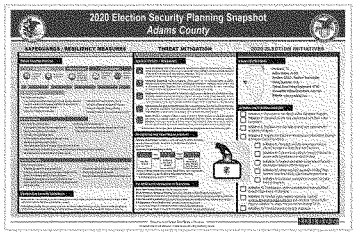
Through #Protect2020, CISA leverages a wide range of offerings and services to build outreach programs and engage local election officials in the over 8,000 election jurisdictions across the country. CISA builds these crucial relationships within the election community by supporting election officials in their efforts to identify and plan for potential vulnerabilities to elections infrastructure ahead of and during the 2020 election cycle. CISA engages political campaigns by supporting the development of non-partisan informational products and conducting voluntary assessments, partners with the private sector to collaborate on best practices and vendor security, and works towards raising public awareness about foreign interference efforts.

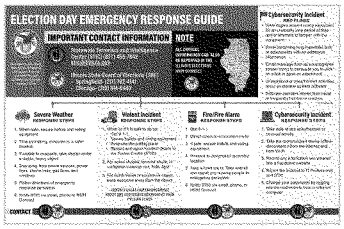
An example of a successful direct engagement with state officials is CISA's Last Mile Project, featured on the following page. Launched in 2018, the Last Mile effort creates and distributes election security products to various stakeholders, tailoring the products to stakeholder needs and priorities. Fifteen states have worked with CISA to complete customized Last Mile products that have been distributed to over 1,000 jurisdictions. Officials from 20 additional states have already expressed interest in Last Mile products for the 2020 elections.

05

CISA #Protect2020 "The Last Mile" Products

Thousands of local jurisdictions, vendors, and political campaigns make up the majority of the U.S. elections stakeholder community, and together represent the biggest opportunities and vulnerabilities for election security. The independence and resource disparity among these entities create significant challenges to information sharing and implementation of best practices. Engaging these local stakeholders and the voters they serve represents the "Last Mile" in reducing risks to election security. CISA's Last Mile products are scalable, customizable tools that local stakeholders can use immediately to improve security and awareness of additional services available. These products aim to strengthen the relationships among national, state, and local partners, which are essential for effective information sharing and continual engagement on critical election security issues.





See Appendix A for samples of Last Mile Products and other election security deliverables

SPOTLIGHT:
ELECTION SECURITY PLANNING SNAPSHOT POSTER

The Election Security Planning Snapshot posters highlight the measures state and local election authorities are taking and plan to implement to strengthen the security of their election systems. CISA collaborates with state election officials to customize the Snapshot posters for each state and locality. The Snapshot posters promote election security initiatives and bolster confidence among voters, lawmakers, and election personnel in the security of their jurisdiction's elections. The Snapshot posters help cover the Last Mile by demonstrating to localities that election security is a top priority for state governments and CISA, and by encouraging localities to leverage the free resources CISA offers.

SPOTLIGHT:
ELECTION DAY EMERGENCY RESPONSE GUIDE POSTER

CISA has identified incident response and reporting as a capability gap among state and local election authorities. CISA also recognizes that polling places, election offices, and storage facilities are vulnerable to a variety of threats. The Election Day Emergency Response Guide posters address this capability gap by providing local election personnel with a simple yet eye-catching tool for determining what steps to take when an incident occurs and who to report the incident to. CISA works with state election officials to determine which response steps and contacts are most appropriate for their jurisdictions.

06

Who We Support

The election community is made up of a variety of independent actors. CISA must constantly work to ensure stakeholder buy-in and to build trust within the community. Without each of these groups' voluntary engagement, CISA could not work to promote election security.

SPOTLIGHT: COORDINATING BODIES

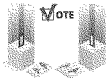
The Government Coordinating Council (GCC) & Sector Coordinating Council (SCC)

The GCC and SCC are made up of state and local election officials and private sector election stakeholders, respectively. They are the primary coordinating bodies through which their respective stakeholder groups and the Federal Government collaborate to address the entire range of security and resilience efforts and policies in the subsector.

State and Local Election Authorities

State and Local Authorities: Elections are organized and executed by citizens at all levels of government from a State's Chief Election Official to precinct poll workers. These are the operators on the front lines of drafting election security policies and overseeing their implementation.

Coordinating Bodies: Stakeholders in the election community often voluntarily come together in formal organizations to share information and best practices and to serve as a central communication point between the Federal Government and individual actors.



Election Technology Vendors

Elections take place on technology and infrastructure developed, deployed, and sometimes operated by private sector companies. These companies play a critical role in ensuring the overall security of the election system.

Campaigns and Political Infrastructure

Campaigns: The security practices of candidates and staffers can affect how easily an adversary can penetrate their networks and attempt to disrupt U.S. elections through leaked materials.

National Political Party Committees: Partisan organizations are potential targets for adversaries searching for sensitive political information. They also provide resources to assist campaigns in strengthening their cybersecurity posture.

American Electorate

Voting citizens are the lifeblood of the election system and the ultimate targets of any attempts to interfere in the elections process.

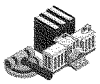
Who We Partner With

SPOTLIGHT:
EI-ISAC

Elections Infrastructure ISAC

The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

The EI-ISAC facilitates the sharing of cyber and critical election infrastructure data among members and others as appropriate, in order to promote communication regarding election-related disinformation and cyber and election infrastructure readiness and response efforts.



Federal Partners

Federal Partners: A number of federal agencies play a role in election security. Some have a direct election-related mandate while others have adapted from their traditional roles to support election security efforts. Through coordination across the federal interagency, election security stakeholders are provided the best possible intelligence, information, and security services.

Non-Governmental Organizations (NGOs)

NGOs work with stakeholders at all levels to increase the election community's resilience to disruption.

Think Tanks & Academia

Academic institutions, think tanks, and private researchers play a pivotal role in creating and promoting best practices for election security.

Media & Social Media Companies

Traditional media outlets and social media platforms are critical nodes for reporting on elections and can be abused by malign actors to manipulate or erode confidence in the electoral system.

Cybersecurity Firms

Private sector firms are often responsible for providing election officials with risk consultations, threat monitoring services, and incident response teams.

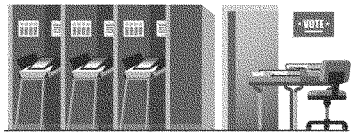
08

CISA Lines of Effort

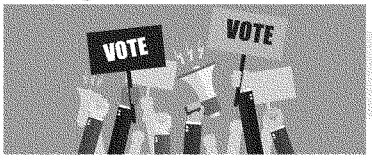
CISA's #Protect2020 campaign supports the election infrastructure community, campaigns, political infrastructure stakeholders, and the American electorate, with a combination of technical expertise and relationship building to ensure they have a solid understanding of the risks they face and access to the resources they need to manage them. To aid this effort, CISA engages with public and private sector threat intelligence sources to identify risks to the election community. CISA's #Protect2020 lines of effort work toward making the 2020 elections the safest and most secure in our Nation's history and toward building a sturdy and sustainable framework for defending all future elections.

This Strategic Plan is organized by the lines of effort shown above. For each line of effort, CISA has defined associated objectives, key actions, and measures of success.

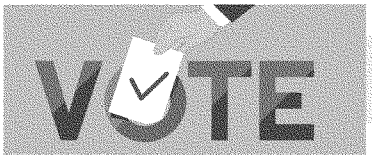
Elections Infrastructure



Campaigns & Political Infrastructure



The American Electorate



Warning and Response

SAFE & SECURE ELECTIONS

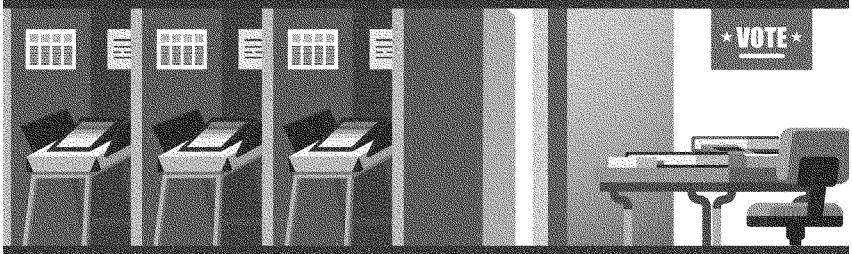
#PROTECT2020 / CISA LINES OF EFFORT

09

Line of Effort 1:

Election Infrastructure

Ensuring state and local election officials and private sector partners have the information they need to assess and manage risks to their networks. CISA assists with efforts to secure election infrastructure, which includes storage facilities, polling places, and centralized vote tabulation locations used to support the election process. Additionally, CISA assists with information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and to report and display results on behalf of state and local governments.



Objectives

1 Build Stakeholder Capacity

1.1 Promote security practices among key audiences
1.2 Advise and coordinate the creation of incident response & communications plans
1.3 Train stakeholders and exercise security practices

2 Provide Assessments and Services

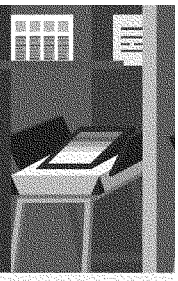
2.1 Coordinate interactions between deployed cyber and physical advisors, and election stakeholders
2.2 Promote the use of CISA's no-cost, voluntary security services & assessments
2.3 Provide Incident Response capabilities, as necessary, by request

3 Facilitate Information Sharing

3.1 Convene and interface with stakeholder bodies
3.2 Expand reach among election community
3.3 Promote situational awareness among stakeholders

10 *Line of Effort 1*

Election Infrastructure



Objectives

1. Build Stakeholder Capacity

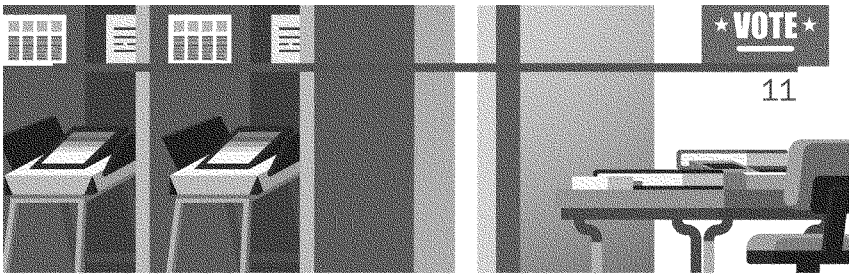
CISA focuses on making sure that election infrastructure stakeholders have the skills and information necessary to assess and manage the risks they face. State and local officials, volunteer poll workers, and election system vendors are responsible for administering safe and secure elections. However, they face threats from foreign nation-states and criminal organizations. CISA serves to provide them the resources and support necessary to build their capacity to deal with these outside adversaries.

KEY ACTIONS

- **1.1 Promote security practices among key audiences**
  CISA partners with state and local election officials and their private sector partners to create and distribute customized products that aim to close the disparity in resources and capabilities among election infrastructure stakeholders.
- **1.2 Advise and coordinate the creation of incident response and communications plans**
  CISA works to produce standardized incident response and crisis communications plans and encourages states to adopt and practice them prior to election day.
- **1.3 Train stakeholders and exercise security practices**
  CISA offers trainings and facilitates exercises at the local, state, and national levels for the election community. The exercises simulate likely election scenarios, such as disinformation campaigns and cyber events, while highlighting best practices and allowing actors to develop and practice their response plans. The exercises serve to reinforce existing communication channels and forge new ones to be used in the event of a crisis.

SPOTLIGHT:
ELECTION INFRASTRUCTURE SUBSECTOR COORDINATING COUNCIL (EISCC) ELECTION SECURITY GUIDE

Election system vendors and their third-party providers establish the technological foundation of American democracy and are therefore integral to CISA's efforts to secure election infrastructure. However, many private sector companies that EISCC members partner with lack the resources and the know-how to meet the security standards expected by the voting public. The *EISCC Election Security Guide* provides election technology providers a tool for promoting the measures they take to secure their products, services, and infrastructure, as well as for providing guidance to their third-party providers for contributing to those efforts. The Guide also details incident response and reporting steps for their own employees and third-party providers to follow, as well as CISA resources they should leverage.



2. Provide Assessments and Services

CISA engages with election infrastructure stakeholders continually to give them the technical assistance necessary to monitor and secure their networks and provides them with federal support as they confront cyber threats.

KEY ACTIONS

- **2.1 Coordinate interactions between deployed cyber and physical advisors, and election stakeholders**

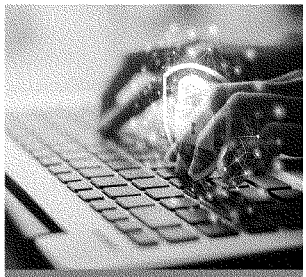
  CISA deploys cybersecurity advisors (CSAs) and protective security advisors (PSAs) to all regions of the country. These advisors engage stakeholders and assist with creating their risk profiles, using federal resources, and implementing best security practices.

- **2.2 Promote the use of CISA's no-cost, voluntary security services & assessments**

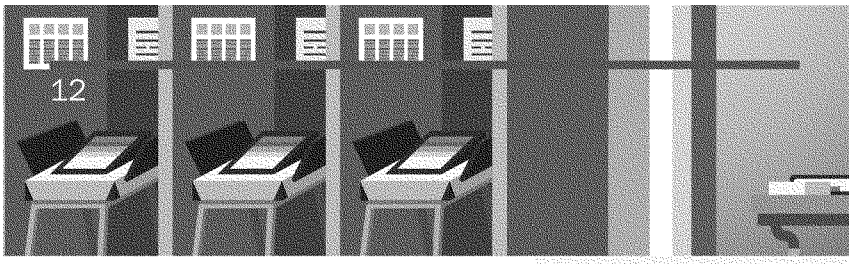
  CISA maintains a full catalog of no-cost physical and cybersecurity services. These services inform CISA's understanding of risk to different communities. CISA has specifically promoted services such as vulnerability scanning, physical security assessments, remote penetration testing, and Phishing Campaign Assessments for the election community. Through these services, CISA helps stakeholders assess their risk profile and works with them to develop individualized plans for increasing security.

- **2.3 Provide incident response capabilities, as necessary, by request**

  When cyber incidents occur, CISA offers assistance by request to potentially impacted entities, analyzes the impact across critical infrastructure, and coordinates the national response to significant cyber incidents. CISA works in close coordination with other agencies with complementary cyber missions, as well as private sector and other non-federal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents.



> "As the threat environment evolves, DHS will continue to work with federal agencies, state and local partners, and private sector entities to enhance our understanding of the threat; and to make essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency."
>
> *Bob Kolasky*
> *Director of National Risk Management Center*



3. Facilitate Information Sharing

The election infrastructure community relies on up-to-date threat reporting and best practice sharing to secure America's elections. CISA facilitates this two-way process by coordinating up-to-date intelligence sharing between the Federal Government and private and local partners.

KEY ACTIONS

- **3.1 Convene and interface with stakeholder bodies**
  CISA is the sector-specific agency for the election infrastructure subsector and takes the lead in managing to guide priorities across the subsector and promote effective communication among state and local officials, industry experts, and the Federal Government.
- **3.2 Expand reach among the election community**
  CISA funds the EI-ISAC to enable rapid communication, information sharing, and situational awareness across the community. CISA has prioritized encouraging localities to sign up for the EI-ISAC.
- **3.3 Promote situational awareness among stakeholders**
  CISA and the EI-ISAC provide a variety of situational awareness capabilities, including hosting a platform prior to, during, and after state and national elections for election stakeholders to swiftly identify, react to, and share real-time events and intelligence.

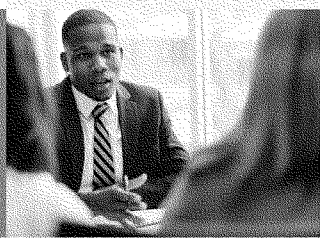
SUCCESS INDICATORS

- Advance election technology security from voter registration databases to vote casting devices and ballot tabulation processes.
- Prepare election infrastructure stakeholders to perform their duties securely and manage incident response scenarios.
- Encourage more secure publicly facing platforms that display voting information and report election night results.

SPOTLIGHT: GCC "READY FOR 2020" PRIORITIES

The Election Infrastructure Government Coordinating Council (EI-GCC) identified 5 priorities to support the Election Infrastructure Sector Specific Plan ahead of the 2020 elections:

- Increase engagement and support to local-level election officials.
- Increase awareness of risks associated with inconsistent and insufficient resources.
- Mature risk initiatives with Sector-Specific Agencies (SSAs) through coordination with Sector Coordinating Councils.
- Apply lessons learned from 2018 to review and refine the communications mechanisms and content supporting the subsector.
- Drive improved security practices in future election infrastructure.

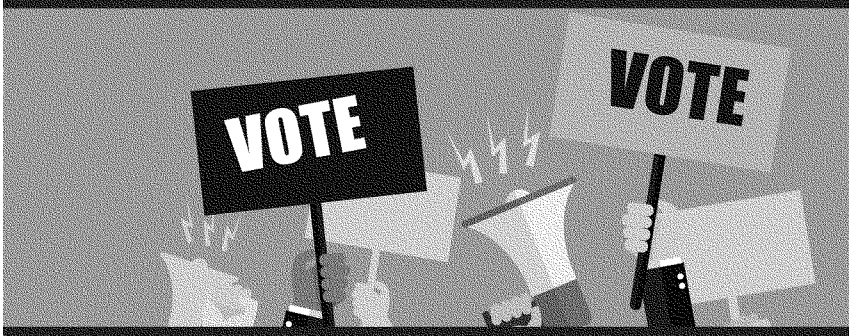


13

Line of Effort 2:

Campaigns & Political Infrastructure

To provide political campaigns and partisan organizations with access to the information they need to assess and manage risks. CISA assists efforts to secure political infrastructure and critical communications systems.



Objectives

4 Build Partisan Stakeholder Capacity

4.1 Foster the creation of an engaged stakeholder community

5 Provide Assessments and Services to Partisan Stakeholders

5.1 Offer CISA no-cost, voluntary services & assessments

6 Facilitate Information Sharing with Partisan Stakeholders

6.1 Brief campaigns on the latest threat intelligence

6.2 Meet with national-level campaigns and party committees

14 *Line of Effort 2*

Campaigns & Political Infrastructure

Objectives

4. Build Partisan Stakeholder Capacity

Traditionally, campaigns and national political parties are hyper focused on raising money, amplifying political messages, and turning out voters, but 2016 showed that they are vulnerable stakeholders in the election community. CISA works with them to build their capacities and increase their resilience.

KEY ACTIONS

- **4.1 Foster the creation of an engaged stakeholder community**

  CISA works with political infrastructure stakeholders to create a culture of active information sharing and collaborative best practice sharing.

5. Provide Assessments and Services to Partisan Stakeholders

Campaigns and political parties host sensitive voter information, private communications, and privileged policy proposals on a wide array of networks and devices. CISA works with them to identify and mitigate vulnerabilities within these information technology systems.

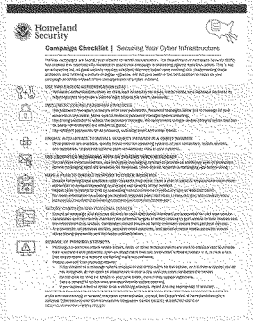
KEY ACTIONS

- **5.1 Offer CISA no-cost, voluntary services and assessments**

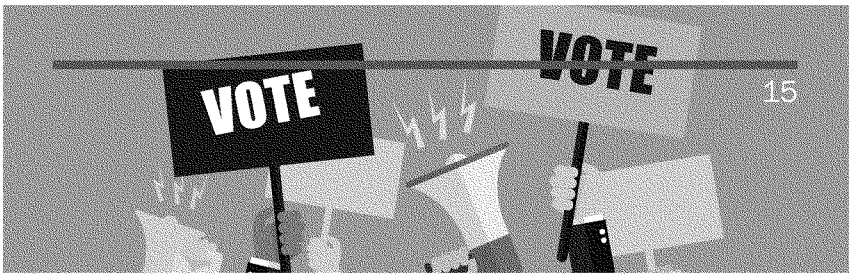
  CISA offers campaign staff, candidates, and national party committees the same services and assessments available to election infrastructure stakeholders. However, due to its critical infrastructure status, any services or assessments requested by election infrastructure stakeholders would receive priority over campaigns and political infrastructure requests. CISA also provides incident response capabilities, by request.

SPOTLIGHT: CAMPAIGN CHECKLIST

In 2018, CISA built a campaign checklist to circulate to candidates and their staff to assist them in implementing cybersecurity best practices in order to protect them against malicious actors.


Homeland Security

Campaign Checklist | Securing Your Cyber Infrastructure

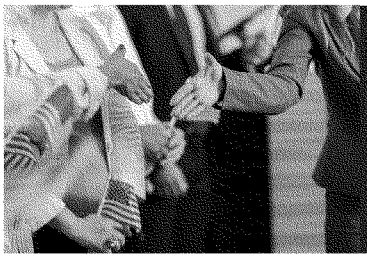


6. Facilitate Information Sharing with Partisan Stakeholders

In a heated political contest, information sharing between partisan entities is difficult. CISA works with campaigns and political parties to provide them real-time threat and vulnerability information from the Federal Government. Even though campaign and partisan actors are not designated as elections infrastructure, CISA offers cybersecurity assistance to these entities, ensuring that the same assistance is offered to all similarly-situated entities and is not offered for the purpose of conferring any political advantage or disadvantage on those entities.

KEY ACTIONS

- **6.1 Brief campaigns on the latest threat intelligence**
  CISA collaborates with the FBI and the intelligence community to offer campaigns joint briefings on potential threats to their systems or active hostile campaigns.
- **6.2 Meet with national-level campaigns and party committees**
  CISA holds introductory meetings with national-level political campaigns and partisan organizations to provide information on CISA services and points of contact for incident response and other needs.



SUCCESS INDICATORS

- Increase engagement between partisan actors and the Federal Government.
- Promote a greater emphasis on cybersecurity and risk mitigation throughout the political infrastructure community.

16

"We recognize the fundamental link between public trust in our election infrastructure and the confidence the American public places in basic democratic functions. Ensuring the security of our electoral process is a vital national interest and one of our highest priorities at DHS."

Bob Kolasky
Director of National Risk Management Center

SPOTLIGHT:
COUNTERING FOREIGN INFLUENCE TASK FORCE (CFITF)

In early 2018, former Secretary Kirstjen Nielsen established a Countering Foreign Influence Task Force (CFITF) within the Department of Homeland Security. The Task Force is now formally a part of CISA. It works in close coordination with the FBI Foreign Influence Task Force, the government lead on foreign interference.

CFITF is charged with helping CISA's leadership understand the scope and scale of this challenge; identifying the policy options available to the government; and working with social media companies, academia, international partners and across the executive branch on a variety of projects to build resilience against foreign influence operations.

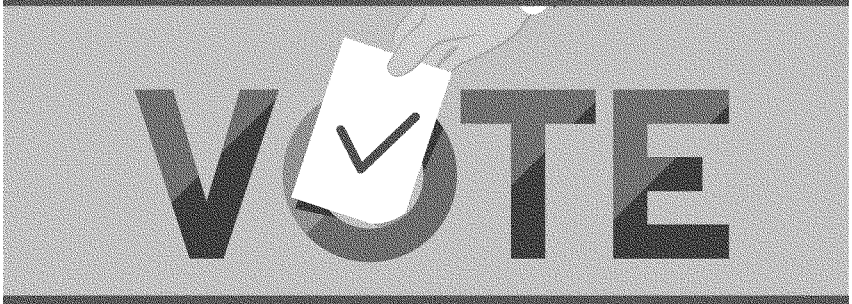
Based on its governing authorities, CISA plays a significant role in enabling stakeholders to make effective risk management decisions. Applying that role to the foreign influence context, the Task Force supports election stakeholders by helping them to understand the scope and scale of the challenge and by enabling them to take actions they deem appropriate. CFITF and the FBI Foreign Influence Task Force coordinate closely on public outreach and education efforts.

17

Line of Effort 3:

The American Electorate

Americans regularly believe, engage with, and share content online and through their personal networks, that has been designed by foreign adversaries to undermine U.S. democratic institutions, disrupt U.S. markets, and sow societal discord. CISA aims to build societal resilience to the persuasion and dissuasion created or amplified by foreign influence activities, including disinformation and misinformation, to ensure the integrity and autonomy of the American electorate.



Objectives

7 Understand and Evaluate the Threat
- 7.1 Partner With Subject Matter Experts
- 7.2 Partner With Federal Counterparts

8 Build Public Awareness & Educate the Public on Best Practices
- 8.1 Develop Informational Products
- 8.2 Engage Trusted Voices

9 Facilitate Information Sharing
- 9.1 Expand the Reporting Community
- 9.2 Host Domestic and International Disinformation Switchboard

#PROTECT2020 / LINE OF EFFORT 3: THE AMERICAN ELECTORATE

18 *Line of Effort 3*

The American Electorate

Objectives

7. Understand and Evaluate the Threat

In order to come up with policy recommendations and adequately support stakeholder populations, CISA needs to understand the nature and scope of the threat and common tactics used in foreign influence operations. Rather than starting from the drawing board, CISA engages the expertise of external and federal partners who have studied or tracked information operations beyond the election sphere, as well as regional and national security experts familiar with the tactics of U.S. adversaries active in the disinformation space.

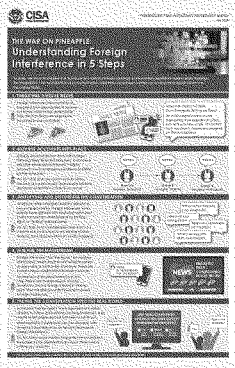
KEY ACTIONS

- **7.1 Partner with Subject Matter Experts (SMEs)**
  CISA engages with SMEs, including researchers, academics, think tanks, and marketing experts, to better understand the threat and how to develop messaging to mitigate the impact of foreign influence operations.
- **7.2 Partner with federal counterparts**
  CISA works in close collaboration with the FBI's Foreign Influence Task Force, the State Department's Global Engagement Center, the Department of Defense, and intelligence community to recognize, understand, and help manage the threat of foreign influence on the American people.

> **"One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections."**
>
> *CHRISTOPHER C. KREBS*
> *Director, Cybersecurity and Infrastructure Security Agency (CISA)*

SPOTLIGHT:
THE WAR ON PINEAPPLE

In 2019, CISA launched a public awareness campaign to educate the electorate about ways foreign actors may try to interfere with democratic processes by sowing discord and pitting American against American. The first product of this initiative was an infographic taking an innocuous example — whether pineapple belongs on pizza — and showing a potential strategy a foreign actor could use to spread divisiveness on the issue.



8. Build Public Awareness & Educate the Public on Best Practices

Findings from academics and researchers show that much of the manipulative power of disinformation can be undermined through awareness. As the public becomes more aware of the tactics and procedures used to covertly manipulate their opinion forming, they become more resistant to them. For this reason, CISA prioritized building public awareness and providing educational materials on best practices as a key strategy in its efforts to foster public resilience to disinformation.

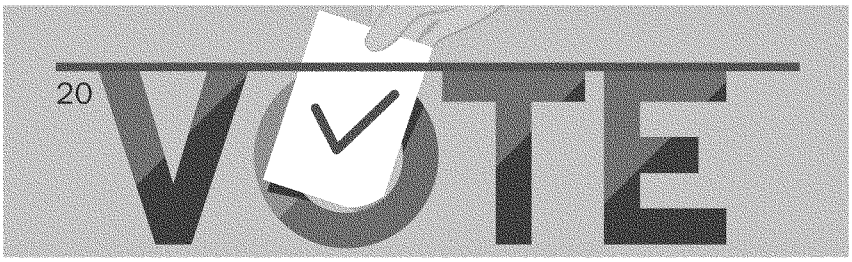
KEY ACTIONS

- **8.1 Develop informational products**

  CISA is developing a number of products to share with the public and influencer organizations. These products aim to build public awareness about the disinformation threat and educate the public on ways to mitigate it. In addition, CISA promotes third-party products that align with its mission statement.

- **8.2 Engage trusted voices**

  CISA engages "trusted voices," influential groups such as the American Association of Retired Persons (AARP) and the National Association for the Advancement of Colored People (NAACP), to amplify resilience messaging and reach a broader stakeholder base.



9. Facilitate Information Sharing

CISA coordinates the sharing of information between the Federal Government, private sector, and state election officials to make sure that the American electorate has access to accurate and up-to-date information on all aspects of the election process.

SUCCESS INDICATORS

- Limit electorate's exposure to foreign disinformation on social media platforms.
- Mitigate the effect of foreign disinformation on targeted audiences.

KEY ACTIONS

- **9.1 Expand the Reporting Community**
  CISA will build upon 2018 midterm Election Information Sharing efforts by expanding the number of entities that can report incidents to CISA and expanding the number of platforms with agreements to receive reporting from CISA.
- **9.2 Host Domestic and International Disinformation Switchboard**
  Following its success in the 2018 U.S. midterm elections, CISA again plans to operate as a switchboard for routing disinformation concerns of state and local election officials to appropriate social media platforms and law enforcement agencies. Additionally, CISA plans to share information and best practices with international partners who are experiencing similar concerns within their own elections.

> **"We can patch cyber vulnerabilities and defend our databases, but if we don't also prepare the American people for the onslaught of foreign interference they face daily, then we will have failed."**
>
> *BRIAN SCULLY*
> *Countering Foreign Influence Lead, Election Security Initiative*

21

Line of Effort 4:

Warning and Response

Warning and response reinforces CISA's three previous lines of effort, capacity building and support for election officials, campaigns, and the American electorate. It aims to provide accurate and actionable threat intelligence to the election community.

Objectives

10 **Partner with the Private Sector**

10.1 Improve warning and response by facilitating cooperation between vendors, election officials, and private sector experts

10.2 Engage the cybersecurity community

11 **Cooperate Across the Federal Interagency**

11.1 Foster a sense of community and support common understanding across the federal interagency on election threats

11.2 Coordinate with the intelligence community and law enforcement to enrich their understanding of cybersecurity incidents and identify trends impacting election infrastructure

12 **Monitor Threat Activity**

12.1 Identify emerging threats using CISA, EI-ISAC, and federal partner & private sector capabilities

12.2 Synchronize information from a variety of sources to understand the full threat picture

13 **Facilitate Rapid Information Sharing with Elections Infrastructure Stakeholders**

13.1 Share cyber threat intelligence, context on cyber incident trends, and mitigation advice with elections infrastructure owners, operators, and vendors in a rapid, actionable manner

13.2 Facilitate provision of feedback on shared threat information to improve the intelligence cycle and ensure mitigation advice is actionable

22 *Line of Effort 4*

Warning and Response

Objectives

10. Partner with the Private Sector

Many private sector firms conduct research and perform assessments relevant to election security. In order to have access to the most up-to-date information and avoid duplicating efforts, CISA partners with recognized security experts from across the private sector to understand the threats and provide warning and mitigation actions to election stakeholders.

KEY ACTIONS

- **10.1 Improve warning and response by facilitating cooperation between vendors, election officials, and private sector experts**

  CISA coordinates between election technology vendors, state and local officials, and private cyber threat intelligence firms to develop indicators and warnings.

- **10.2 Engage the cybersecurity community**

  CISA works with cybersecurity communities to identify ongoing attacks and coordinate response measures.

11. Cooperate Across the Federal Interagency

As with previous lines of effort, to develop a warning and response protocol requires cooperation with federal counterparts and information sharing across the intelligence community to stay up-to-date on the most urgent threats and vulnerabilities across the election community.

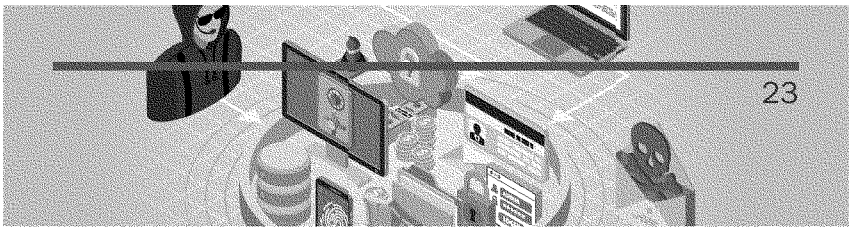
KEY ACTIONS

- **11.1 Foster a sense of community and support common understanding across the federal interagency on election threats**

  CISA advocates creating a joint Sense of the Community Memorandum to consolidate and highlight current knowledge on election threat intelligence.

- **11.2 Coordinate with the intelligence community and law enforcement to enrich their understanding of cybersecurity incidents and identify trends impacting election infrastructure**

  CISA works closely with interagency partners to ensure the government has an accurate and complete picture of the threat landscape from which to engage the election community.



12. Monitor Threat Activity

CISA relies heavily on partner capabilities, including the intelligence community and EI-ISAC, to track and monitor emerging threats to elections.

KEY ACTIONS

- **12.1 Identify emerging threats using CISA, EI-ISAC, and federal partner & private sector capabilities**
  CISA uses passive measures to monitor relevant networks to spot malign activity and reveal key trends.
- **12.2 Synchronize information from a variety of sources to understand the full threat picture**
  CISA reviews and analyzes third-party vendor information, unclassified open source reporting, and threat information received from stakeholders to understand the scope of malicious cyber activity and foreign influence activities targeting elections.

13. Facilitate Rapid Information Sharing with Elections Infrastructure Stakeholders

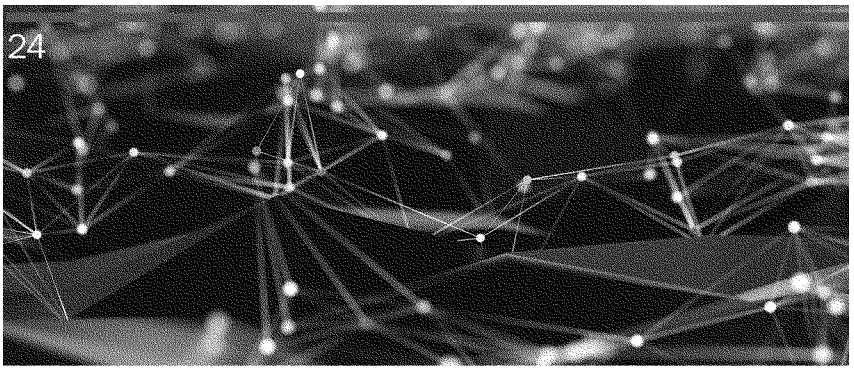
CISA analyzes various information sources to develop a continuously updated picture of the threats to election infrastructure and provides information to elections stakeholders in order to facilitate risk mitigation activities.

KEY ACTIONS

- **13.1 Share cyber threat intelligence, context on cyber incident trends, and mitigation advice with elections infrastructure owners, operators, and vendors in a rapid, actionable manner**
  CISA works to ensure relevant and actionable threat information is declassified when necessary and shared with the appropriate network owners and operators for cyber defense purposes. CISA also develops and publishes mitigation advice when appropriate and shares it with elections stakeholders as rapidly as possible.
- **13.2 Facilitate provision of feedback on shared threat information to improve the intelligence cycle and ensure mitigation advice is actionable**
  CISA will ensure that feedback from election infrastructure stakeholders is shared with interagency partners to facilitate improvements for network defense purposes.

SUCCESS INDICATORS

- Identify potential and realized threats to the election community.
- Improve sharing of timely and actionable threat information with election community.
- Improve processes and mechanisms for information sharing across federal entities.



Measuring and Achieving Results

The Federal Government has made significant improvements in its efforts to promote safe and secure elections since the Secretary of Homeland Security designated elections infrastructure as a critical infrastructure subsector on January 6, 2017. Initially, there was much confusion over what the designation meant, and stakeholders criticized DHS for not involving them in this decision, for not explaining it effectively, and for continuing to describe threats to election infrastructure without engaging the states. CISA recognized a need to better serve this community and surged resources to establish the Election Task Force and build critical infrastructure governance bodies.

CISA's mission for the 2018 midterm elections focused on proactively building trust with the election community, elevating security of election infrastructure, and facilitating information sharing across stakeholders, including social media and technology companies, law enforcement and intelligence, and state and local election officials. In the lead up to the 2020 elections, CISA will continue the prioritization of support to election administrators and vendors and will continue to build relationships to support and advise partisan organizations. It aims to enhance awareness of and participation by the public and to partner with third-party organizations and subject matter experts to help develop and amplify effective public messaging. Additionally, CISA will work to enhance federal, private, and ISAC operational alliance to improve rapid bi-directional information sharing and expand engagements with threat intelligence firms and the intelligence community to ensure that the election community has access to accurate and actionable threat analysis.

25

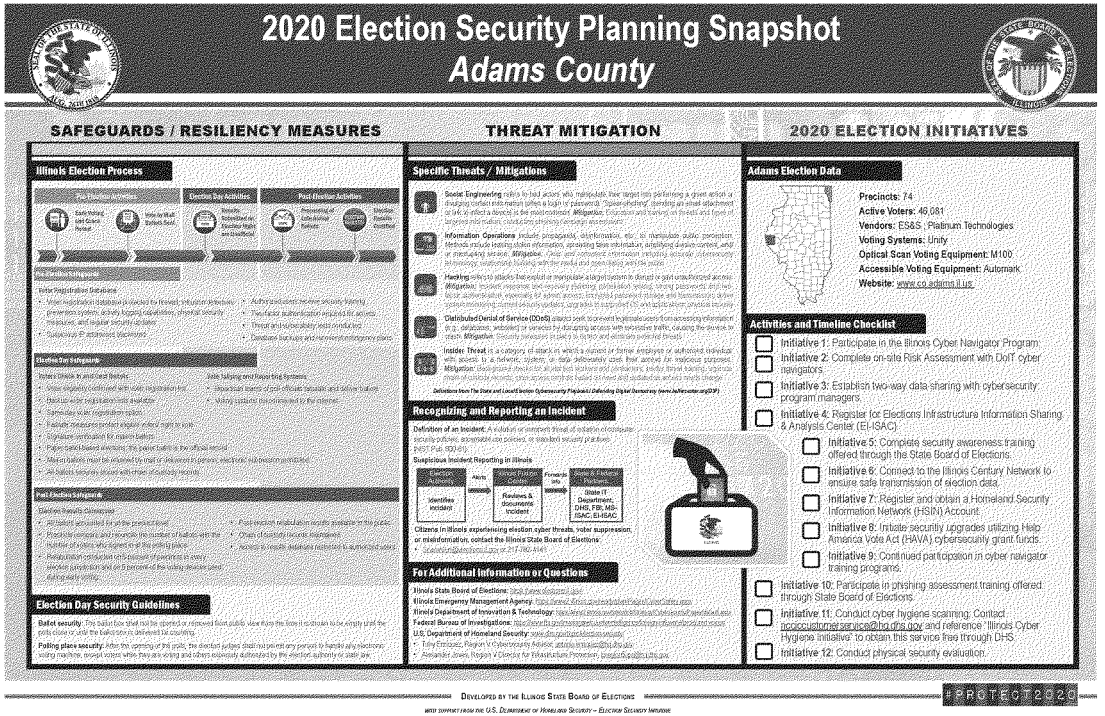
Conclusion

#Protect2020 is more than just a slogan; it is a pledge among election security stakeholders—including the Federal cybersecurity community, state and local election officials, vendors, political campaigns, and others—to work together towards a common vision of a safe and secure election trusted by all Americans in 2020. This is an ambitious undertaking. The threat landscape is constantly evolving, and dedicated, malicious actors with virtually unlimited resources will always be able to penetrate some aspect of American networks or to spread disinformation. In the field of election security, it is not possible to identify all system vulnerabilities and defend them in all scenarios. However, it is CISA's mission to elevate the security posture of our Nation's election systems to make these intrusions more difficult, identify them when they occur, and ensure that they do not affect the overall outcome of the election. CISA cannot do this alone.

Ultimately, the security of America's elections rests with the state and local officials who administer them, the private sector vendors who create the technology that makes them possible, the candidates and campaigns who participate in them, and ultimately the electorate who show up to the polls on election day. Securing American elections requires hard work, resources, and persistence among all of these critical actors, and no one entity can do it alone. To this end, CISA's #Protect2020 strategy is all about building strong, resilient, and interconnected stakeholder communities, outfitted with the required capacities, technical assistance, and information necessary to resist adversaries while trusting that the DHS CISA organization will be there to support them in every way that they can.

Appendix A: Election Security Deliverables

Election Security Planning Snapshot – "The Last Mile" Poster



Election Day Emergency Response Guide– "EDERG" Poster

ELECTION DAY EMERGENCY RESPONSE GUIDE

Developed by the Illinois State Board of Elections with support from the Cybersecurity and Infrastructure Security Agency (CISA)

IMPORTANT CONTACT INFORMATION

Statewide Terrorism and Intelligence Center (STIC) (877) 455-7842
stic@illinois.gov

Illinois State Board of Elections (SBE)
- Springfield- (217) 782-4141
- Chicago- (312) 814-6440

NOTE

ALL CRITICAL INFORMATION CAN ALSO BE REPORTED IN THE ILLINOIS ELECTIONS HSIN CONNECT

Severe Weather RESPONSE STEPS

1. When safe, secure ballots and voting equipment
2. Time permitting, evacuate to a safer location
3. If unable to evacuate, take shelter under a stable, heavy object
4. Stay away from power sources, power lines, phone lines, gas lines, and windows
5. Follow directions of emergency response personnel
6. Notify STIC via email, phone or HSIN Connect

Violent Incident RESPONSE STEPS

1. When or if it is safe to do so:
   - Call 9-1-1
   - Secure ballots and voting equipment
   - Evacuate the polling place
   - Record and report incident details to the Fusion Center (STIC)
2. For active shooter, terrorist attack, or workplace violence: run, hide, fight
3. For bomb threat or suspicious object: keep everyone away from the object

CONTACT LOCAL LAW ENFORCEMENT ABOUT ANY SUSPICIOUS BEHAVIOR AT YOUR POLLING PLACE

Fire/Fire Alarm RESPONSE STEPS

1. Dial 9-1-1
2. Direct voters to evacuation route
3. If safe, secure ballots and voting equipment
4. Proceed to designated assembly location
5. Take a head count. Take note of and report any missing people to emergency personnel
6. Notify STIC via email, phone, or HSIN Connect

Cybersecurity Incident RESPONSE STEPS

1. Take note of any unauthorized or unusual activity
2. Take the compromised device offline- disconnect it from the internet and from Wi-Fi
3. Record any information you entered into a fraudulent website
4. Report the incident to IT Professional and STIC
5. Change your passwords by logging into the real website from a different computer

Cybersecurity Incident RED FLAGS*

- Voter lingers around voting equipment for an unusually long period of time and/or attempts to tamper with the equipment
- Email containing long hyperlinks and/or attachments with no additional information
- Email message from an unrecognized sender trying to persuade you to click on a link or open an attachment
- Unexplained or unauthorized activities occur on election system software
- Software operates slower than usual or frequently freezes or crashes

*Limited scope

CONTACT

#PROTECT2020/APPENDIX A

Campaign Checklist

Homeland Security

Campaign Checklist | Securing Your Cyber Infrastructure

Political campaigns are facing cyber-attacks of varied sophistication. The Department of Homeland Security (DHS) has created this cybersecurity checklist to assist your campaign in protecting against malicious actors. This is not an exhaustive list, as good security requires constant attention based upon evolving risk. Implementing these protocols, and instilling a culture of digital vigilance, will put your team in the best position to focus on your campaign priorities instead of the consequences of a cyber incident.

USE TWO-FACTOR AUTHENTICATION (2FA)

- Two-factor authentication allows an extra layer of security for email, social media, and database accounts by requiring users to provide a second login beyond the user's password.

IMPLEMENT STRONG PASSWORD PRACTICES

- Use password managers to secure all of your passwords. Password managers allow you to manage all your accounts in one place. Make sure to review a password manager before selecting.
- Use a long password to access the password manager. We recommend using a unique string of words that can be easily remembered, but difficult to guess.
- Use different passwords for all accounts, including email and social media.

ENABLE AUTO-UPDATE TO INSTALL SECURITY PATCHES IN A TIMELY MANNER

- Once patches are available, quickly install onto the operating systems of your computers, mobile devices, and databases. Unpatched systems pose unnecessary risks to your systems.

USE ENCRYPTED MESSAGING APPS OR SYSTEMS WHEN NECESSARY

- For sensitive communications, use encrypted messaging services to provide an additional layer of protection.
- Secure messaging apps are available for download. Users should research a messaging app before using.

HAVE A PLAN TO QUICKLY RESPOND TO CYBER INCIDENTS

- Despite following these practices, cyber incidents may occur. Have a plan in place to respond and know which authorities to contact depending on the type and severity of the incident.
- Report cyber incidents to DHS by contacting ncciccustomerservice@hq.dhs.gov or 888-282-0870.
- For more information on creating an incident response plan, visit https://www.dhs.gov/sites/default/files/publications/Incident%20Handling%20Elections%20Final%20508.pdf.

SECURE CAMPAIGN AND PERSONAL DEVICES

- Ensure all campaign and personal devices for staff **AND** family members are accounted for and kept secure.
- Candidates and their family members are potential targets of actors looking to gain access to their devices and the information they contain. Candidates should ensure all family members secure their personal devices.
- At a minimum, all personal devices, personal email accounts, and personal social media accounts should utilize strong passwords and two-factor authentication.

BEWARE OF PHISHING ATTEMPTS

- Phishing is a common attack where emails, texts, or other communication are sent to entice a user to provide their username and password, open an attachment that has destructive software hidden in it, or click a link that directs them to a website containing malicious software.
- Protect yourself from phishing attacks:
  - If the content of a message seems unusual or out of the norm for the sender, or it is from a sender you do not recognize, do not open an attachment or click a link until you have contacted the sender.
  - Do not click on links for emails in your junk folder, even if they appear legitimate.
  - Take a second to review links and attachments before opening.
  - If you suspect a text or email to be a phishing attempt, report it to the appropriate IT provider.

If you are experiencing or suspect malicious cyber behavior, contact the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870 or NCCICCustomerService@hq.dhs.gov.

29 The War on Pineapple Infographic

CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
July 2019

THE WAR ON PINEAPPLE: Understanding Foreign Interference in 5 Steps

To date, we have no evidence of Russia (or any nation) actively carrying out information operations against pizza toppings. This infographic is an ILLUSTRATION of how information operations have been carried out in the past to exploit divisions in the United States.

1. TARGETING DIVISIVE ISSUES

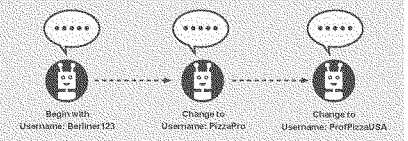
Foreign influencers are constantly on the lookout for opportunities to inflame hot button issues in the United States. **They don't do this to win arguments; they want to see us divided.**

American Opinion is Split: Does Pineapple Belong on Pizza?
An A-list celebrity announced their dislike of pineapples on pizza, prompting a new survey. No matter how you slice it, Americans disagree on the fruit topping.

2. MOVING ACCOUNTS INTO PLACE

Building social media accounts with a large following takes time and resources, so accounts are often renamed and reused. Multiple accounts in a conversation are often controlled by the same user.

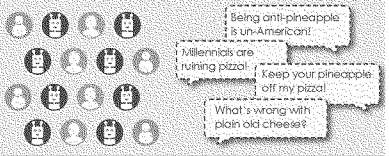
Pro Tip: Look at an account's activity history. **Genuine accounts usually have several interests and post content from a variety of sources.**



3. AMPLIFYING AND DISTORTING THE CONVERSATION

Americans often engage in healthy debate on any number of topics. Foreign influencers try to pollute those debates with bad information and make our positions more extreme by picking fights, or "trolling" people online.

Pro Tip: Trolls try to make people mad, that's it. **If it seems like an account is only aiming to raise tensions, think about whether it's worth engaging.**



4. MAKING THE MAINSTREAM

Foreign influencers "fan the flames" by creating controversy, amplifying the most extreme version of arguments on both sides of an issue. These are shared online as legitimate information sources.

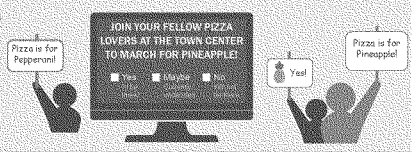
Sometimes controversies make it into the mainstream and create division among Americans. **This is a foreign influencer striking gold! Their meddling is legitimized and carried to larger audiences.**

5. TAKING THE CONVERSATION INTO THE REAL WORLD

In the past, Kremlin agents have organized or funded protests to further stoke divisions among Americans. They create event pages and ask followers to come out.

What started in cyberspace can turn very real, with Americans shouting down Americans because of foreign interference.

Pro Tip: Many social media companies have increased transparency for organization accounts. **Know who is inviting you and why.**



For more information, please see the #Protect2020 website at https://www.dhs.gov/cisa/protect2020

Post-Hearing Questions for the Record
Submitted to Hon. Christopher Krebs
From Senator Josh Hawley

"What States, Locals, and the Business Community Should Know and Do:
A Roadmap for Effective Cybersecurity"
February 11, 2020

Question#:	1
Topic:	Secure Now
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: We learned yesterday that four members of China's People's Liberation Army (PLA) hacked the data of millions of Americans during the Equifax breach in 2017. Are we any more secure now than we were then from attacks by our adversaries, particularly China, on our infrastructure?

Response: The Equifax breach in 2017 was eye opening for critical infrastructure owners and operators in terms of the speed of hackers targeting publicly facing portals with recently known vulnerabilities and then immediately taking advantage of a lack of network and system segmentation to compromise a corporate network. Since this incident, more companies have made the decision to quickly test and implement patches as they come out, so that systems can be updated quickly to eliminate known vulnerabilities. Organizations are prioritizing outside portal patching, since there are often trust relationships between these portals and backend systems, while also ensuring appropriate segmentation is in place to prevent further misuse if a hacker uses a vulnerability which was previously known or unknown. These changes in cybersecurity practices are significant in reducing risk. Additionally, more organizations have ensured it is a reportable condition if a security tool or certificate will be expiring in the near-future, to prevent the experience which Equifax had of not knowing about data being exfiltrated for months, due to a renewal mistake. Companies have continued to improve their cybersecurity methods, including through more effective security, orchestration, automation, and response techniques.

To address the risk posed by foreign malign actors to United States telecommunications and information networks, the President issued the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" and the "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector." The implementation of these Executive Orders will help prevent certain companies associated with or answering to the intelligence and security apparatus

Question#:	1
Topic:	Secure Now
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

of foreign adversaries from, for example, readily accessing the private and sensitive information of the United States Government, the United States private sector, and individual Americans. To ensure protection of our information worldwide, including sensitive military and intelligence data, the United States is actively engaging with our allies and partners, including in multilateral fora, to promote a set of common standards for secure, resilient, and trusted communications platforms that underpin the global information economy. To compel Beijing to adhere to norms of responsible state behavior, the United States is working with allies and like-minded partners to attribute and otherwise deter malicious cyber activities.

Question#:	2
Topic:	Collaborating with China
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: When we consider the threats from China more broadly, at what point would it be constructive to begin a conversation about decoupling some of our technology from China?

Response: The Chinese government has a long-track record of intellectual property theft and coercive behavior, particularly when it comes to strategic technologies that are the subject of industrial policy and indigenization efforts. Chinese laws and policies can be used to force companies to comply with intelligence activities and national security interests and can negatively impact private company operations. The Chinese government has financial stakes in many Chinese companies, which could increase the risk of influence and coercion.

The risks of doing business in China, particularly for companies working in strategic sectors, are becoming clearer, and U.S. agencies and companies are actively engaging on options for mitigating supply chain risks. CISA is building tools to make it simpler for public and private partners to assess their information and communications technology supply chain risks. This supply chain risk analysis is not focused exclusively on technology coming from Chinese sources, but all sources.

In his 2018 Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, the United States Trade Representative (USTR) determined that numerous acts, policies, and practices of the People's Republic of China (PRC) government were unreasonable or discriminatory, and burden or restrict United States commerce. Based on a rigorous investigation, USTR found that the PRC: (1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies' ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States companies' networks to access sensitive information and trade secrets.

As outlined in the recently released *United States Strategic Approach to The People's Republic of China*, the PRC's attempts to dominate the global information and communications technology industry through unfair practices is reflected in discriminatory regulations like the PRC National Cyber Security Law, which requires companies to comply with Chinese data localization measures that enable Chinese Communist Party (CCP) access to foreign data. Other PRC laws compel companies like Huawei and ZTE to cooperate with Chinese security services, even when they do business abroad, creating security vulnerabilities for foreign countries and enterprises utilizing Chinese vendors' equipment and services.

Question#:	2
Topic:	Collaborating with China
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Related to that, could you describe the risks American companies face in collaborating with China? Apple is storing encryption keys in China, for example.

Response: The Cybersecurity and Infrastructure Security Agency (CISA) is aware of and working with federal partners to better understand the risk faced by American companies doing business with China. CISA's contributions to the Committee on Foreign Investment in the United States (CFIUS) and efforts to improve information and communications technology supply chain risk management allow us to make strides for reducing risk from such foreign dependencies. Our participation in the interagency response to the calls to action in "A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals" also helps us engage in managing risks that our critical infrastructure partners may find supply chains disrupted through a variety of reasons.

CISA has been working with federal and private sector partners through its Information and Communications Technology (ICT) Supply Chain Risk Management Task Force to better understand risks and share best practices for addressing those risks. The agency is committed to working with government and industry partners to enhance the security and resilience of the global ICT supply chain and to integrate SCRM into CISA's cybersecurity efforts. On May 5, 2020, CISA publicly released an ICT Supply Chain Essentials Guide, which contains actionable steps on how to start implementing organizational Supply Chain Risk Management (SCRM) practices to improve overall security resilience.It can be found on CISA's website at https://www.cisa.gov/publication/cisa-scrm-essentials [1].

Supply chain risk is amplified by adversaries' attempts to exploit ICT technologies and their related supply chains for purposes of espionage, sabotage, and foreign interference activity. Vulnerabilities in supply chains—either developed with malicious intent or unintentionally through poor security practices—can enable data and intellectual property theft, loss of confidence in the integrity of the system, or exploitation to cause system or network failure. Increasingly, adversaries, including nation-state adversaries such as Russia, China, North Korea, and Iran, are looking at these vulnerabilities as a principal attack vector.

Compounding the risk associated with supply chains is that vulnerabilities may be introduced during any phase of the ICT life cycle: design, development and production, distribution, acquisition, deployment, maintenance, and disposal. These vulnerabilities include malicious software and hardware; counterfeit components; and poor product designs, manufacturing processes, and maintenance procedures. Coordination between the public and private sector

[1] ICT Supply Chain Risk Management Essentials: https://www.cisa.gov/blog/2020/05/05/building-collective-resilience-ict-supply-chain

Question#:	2
Topic:	Collaborating with China
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

helps with the understanding of these vulnerabilities and sharing of expertise for developing solutions to global supply chain risk

CISA continues to work every day to protect the Homeland from nefarious technology, supply chain vendors, and foreign investors, whether they come from China or elsewhere. Additional information on CISA's efforts can be found here: https://www.cisa.gov/supply-chain.

Question#:	3
Topic:	Coordination with Europe
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Josh Hawley
Committee:	HOMELAND SECURITY (SENATE)

Question: Last month, the EU announced that it would allow member states to decide on the place of Huawei in their local infrastructure. Can you describe the state of coordination with your European counterparts on our common cybersecurity when it comes to 5G and protecting our networks from China's influence and exploitation?

Response: Current efforts include encouraging all countries, including EU member states, to adopt a risk-based security framework for the rollout of 5G networks. We urge nations to conduct a careful evaluation of potential hardware and software equipment, vendors, and the supply chain. It is imperative that the international community renews its efforts to incentivize security, as well as cost, in the marketplace and ensure it is a primary consideration in product development, manufacture, acquisition, and procurement. In 2019, the global community made great strides at the Prague 5G Security Conference, where officials from nearly 40 countries met to discuss a set of principles on how best to design, construct, and administer secure 5G infrastructure, known as the Prague Proposal. Additionally, the European Commission and European Union (EU) member states released their coordinated EU risk assessment of 5G security. The assessment clearly identified the vulnerability of 5G vendors or suppliers that could be subject to pressure or control by a third country, especially countries without legislative or democratic checks and balances. The assessment also highlighted the corporate ownership structure of 5G suppliers as a potential risk factor, which aligns with the U.S. assessment and the Prague Proposals' call for transparency. Establishing international cybersecurity norms, like we did in Prague, must continue with our international partners. We must continue to encourage responsible behavior and oppose those who would seek to disrupt networks and systems.

Post-Hearing Questions for the Record
Submitted to Hon. Christopher Krebs
From Senator Kyrsten Sinema

"What States, Locals, and the Business Community Should Know and Do:
A Roadmap for Effective Cybersecurity"
February 11, 2020

Question#:	4
Topic:	CETAP Grants
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: The State, Local, Tribal, and Territorial Cybersecurity Coordinating Council for CISA recommended providing grants to NGOs and other organizations to build cybersecurity educational programs for "younger people." Educators in Arizona have told me that while they appreciate the efforts of CISA to support the development of cybersecurity-integrated high school curricula through the Cybersecurity Education and Training Assistance Program (CETAP), they often face barriers in accessing these resources due to the rigors of their schedule, their need to seek out education opportunities that will provide them with continuing education credits (CEUs), and a general sense of feeling overwhelmed and ill-equipped to integrate cybersecurity curricula. Arizona's university and K-12 educators have expressed an interest in creating partnerships to create provide K-12 educators on the ground programming and support from cybersecurity experts to help them integrate cybersecurity education in their classroom while also awarding CEUs. This is an extension of the natural mission of CISA to coordinate and collaborate among a broad spectrum organizations and is a natural extension of the CETAP grants.

Does CISA have the authority now to establish such a grant program that support collaborative partnerships between universities and K-12 institutions to educate, support, and reward educators for learning and integrating cybersecurity curricula into their classrooms? If not, what authorities would CISA need to establish such a program?

Response: CISA is strengthening training and education mission areas through various initiatives, including targeted K-12 campaigns and outreach.

CISA does not have general grant issuing authorities to develop collaborative partnerships between colleges and universities, community cybersecurity educators, or K-12 institutions to contribute to the cyber education of the next generation of cybersecurity professionals. CISA is

Question#:	4
Topic:	CETAP Grants
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

working with federal partners to explore partnerships with existing federal programs that do allow for stronger coordination. CISA's multipronged strategy to address national cybersecurity needs is working to implement the most cost-effective yet impactful methods for enhancing the entire cybersecurity education and training pipeline. The most effective enhancements, based on national and federal needs, are being prioritized.

Question: What additional infrastructure would CISA need to establish such a program, or does the infrastructure already exist?

Response: CISA would need to better understand the scope of any proposed partnerships to determine the infrastructure and authorities necessary. CISA also will continue to explore partnerships with other federal partners that have such authorities.

Question: What funding would CISA need?

Response: In Fiscal Year (FY) 2020, Congress appropriated $4.3 million for the Cybersecurity Education and Training Assistance Program that provides teacher resources for K-12 classroom instruction on cybersecurity. CISA is exploring opportunities to partner with other federal agencies to achieve this vision.

Question#:	5
Topic:	Smart City Initiatives
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: How is CISA engaging with SLTT entities that are deploying smart cities to help them plan, evaluate, and mitigate potential risks that smart city initiatives might pose?

Response: CISA is engaging with State, Local, Tribal, and Territorial (SLTT) entities that are deploying smart cities to help them plan, evaluate, and manage potential risks that smart city initiatives pose by coordinating the flow of timely information through various channels to planners and users. Released on June 10, *Trust in Smart Cities Systems: Characteristics and Key Considerations*, was initiated and led by CISA and developed by the Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS-owned Federally Funded Research and Development Center (FFRDC), recognizes smart cities systems as those that integrate information technology with the management and operation of civic functions. The report is intended to help managers of smart city projects be better prepared to address the risks associated with such projects, thereby resulting in a more secure and robust national infrastructure.

On January 30th, 2020, CISA conducted a webinar on Smart Cities, in partnership with the Regional Consortium Coordinating Council, and the SLTT Government Coordinating Council. 424 attendees (including 82 SLTT officials) heard directly from city government and industry leaders about the opportunities and vulnerabilities related to Smart Cities technologies – and how everyone can best participate in cities of the future.

Question#:	6
Topic:	Tracking Use of Resources
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: CISA has develop a number of resources for State, Local, Tribal, and Territorial entities to help inform how they can best protect themselves. How is CISA tracking the use of these resources and their effectiveness from stakeholders ranging from the local government, small business, tribal entities etc.? What metrics is CISA using to evaluate them, what outcomes are you seeing, and how is this information being used to continually improve development and distribution of these resources to the various entities that require them?

Response: CISA utilizes a layered approach to supporting small businesses and SLTT entities to raise their level of cyber resilience. Examples include the Vulnerability Scanning Program, Automated Indicator Sharing, and a suite of assessments conducted by regionally based Cybersecurity Advisors (CSA). CSAs conducted cybersecurity risk assessments in FY 2019, consisting of 68 Cyber Resilience Reviews, 68 Cyber Infrastructure Surveys, and 41 External Dependency Management Assessments. These assessments allowed the CSA, in coordination with the entity, to evaluate the cybersecurity posture of the organizations and to assist them in making crucial risk-informed decisions and improvements to security programs. The assessments utilize the NIST Cybersecurity Framework and considers cybersecurity programs through ten domains, or distinct areas of focus, such as Asset Management, Controls Management, and External Dependency Management. The assessments also allow an entity to look at their results against those of all entities for a comparison of cybersecurity maturity. These assessments are tracked in a secure repository, with follow-up discussions, asking if changes were made to their security program based on the assessment.

CISA also issues a variety of alerts, bulletins, and other products, in addition to the thousands of hours of training available to SLTT partners through the Federal Virtual Training Environment (FedVTE). CISA funds the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Centers (EI-ISAC). Both the MS and EI ISAC provide a range of services to members free of charge, but also serve as a network where SLTT agencies can share best practices and lessons learned with each other. MS and EI-ISAC analysts are embedded within CISA's operational teams to ensure shared awareness on threats facing SLTT governments and that resources are assigned to support their needs. The MS-ISAC also conducts the Nationwide Cyber Security Review (NCSR) on behalf of CISA. This is a cyber risk management self-assessment aligned to the NIST Framework. CISA collaborated with FEMA to make completion of this assessment a requirement for all FEMA Homeland Security Grant Program recipients. CISA encourages recipients to cite identified risk management gaps in their investment justifications with technical assistance provided by CISA. In this way, CISA is helping to align funding to where risk management gaps may exist. Self-

Question#:	6
Topic:	Tracking Use of Resources
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

service resources include best practices and campaigns, such as the Cyber Essentials, which specifically provides small businesses and governments with a path to building cyber readiness.

In terms of effectively using the data from services and assessments, CISA will proactively warn SLTT governments when critical vulnerabilities are detected on their public-facing information systems via our Vulnerability Scanning Program. For the most critical vulnerabilities, CISA provides tailored information and patching or mitigation recommendations to SLTT partners, broadly speaking, and emphasizes and reinforces information they already receive via weekly scanning reports.

The tracking and associated metrics for these activities vary, given the depth and breadth of resource types. CISA uses various mechanisms. CISA takes a continuing evaluation approach to each service, starting with setting priorities, tracking service delivery against those priorities, updating content and approaches based on stakeholder Feedback. CISA also receives feedback from the feedback from Government and Sector Coordinating Council structure and relationships with strategic partners, feedback forms on individual products, informal feedback collected from deployed personnel, and a host of other mechanisms to collect requirements and feedback. Feedback is then used to enhance and shape the future development of resources. As previously mentioned, the development of the Cyber Essentials campaign is a good example of an activity in response to feedback. In the wake of an uptick in ransomware attacks, small businesses and smaller government agencies indicated that they did not know where to start in building a cybersecurity program, regardless of the wealth of resources provided by CISA and non-governmental entities. Working with partners across the federal government and with experts across the cybersecurity field, CISA developed the Cyber Essentials. Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices. For a deeper look and greater insight, check out the Cyber Essentials Toolkits, a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. It includes six key attributes of a successful cyber program. Two strategic attributes are leadership engagement and a culture of security. Two technical attributes are knowing what is on your network and knowing who is on your network. Finally, the two tactical attributes are being able to recover after an incident, utilizing backups that have been tested and having a plan in place that includes outreach to employees, public, etc. Additional information can be found at: https://www.cisa.gov/cyber-essentials.

Question#:	7
Topic:	Information Sharing
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Question: SLTT entities continue to request that DHS share threat information, such as indicators of compromise (IOC), in a more timely way. What are the challenges in sharing this information when they are more relevant (versus months old)?

Is there an option to share IOCs in a more easily consumable way, such as a spreadsheet either lieu of or in addition to a PDF?

Response: To provide timely and actionable cyber threat information, the MS-ISAC and EI-ISAC currently leverage its threat intelligence platform to disseminate MS-ISAC and CISA-derived indicators of compromise (IOC) to membership and other partners in a machine-readable format. ISAC members have access to an unlimited number of analyst-level accounts, which they can use to upload indicators for MS-ISAC and EI-ISAC review and action. The MS-ISAC and EI-ISAC also receive member-submitted IPs and Domains through the MS-ISAC Security Operations Center, which are reviewed by analysts and included in weekly and monthly IOC lists sent out via email and also uploaded, which shares the information with ISAC members and CISA.

Moving forward, the MS- and EI-ISACs, in coordination with CISA, are working with John Hopkins University Applied Physics Lab to stand up a full-fledged Structured Threat Information eXpression (STIX)/ Trusted Automated Exchange of Indicator Information (TAXII) server, which will enable the ISACs to host additional machine readable and analyst content specific to SLTT governments. The current plan is to add approximately four separate feeds, via STIX/TAXII, for ISAC members These new STIX IOC feeds are: (1) A Weekly Malware IPs and Domains List, (2) A Monthly Scanning IPs and Domains List, (3) An unclassified version of a list of high-confidence IOCs from the Federal Government, and (4) Near-real-time IOCs pulled from critical Albert (intrusion detection) events.

In addition, CISA releases information sharing products and reports (e.g., Activity Alert, Malware Analysis Report, and Indicator Bulletin) that emphasize priority threats and critical vulnerabilities with partners, including the state and local community. This includes recent threats like Iranian and North Korean malicious cyber activity, as well as vulnerabilities like those in SSL VPN software, Microsoft products, Citrix, and other products. These strategic network defense information products often include a machine-readable STIX file containing Indicators (IOCs) and context discussed in the reports. These IOCs are also shared via CISA's Automated Indicator Sharing program, including to the MS-ISAC and EI-ISAC for sharing with members. This enables relevant IOCs to more easily be applied by the receiving entity for network defense purposes.

Question#:	7
Topic:	Information Sharing
Hearing:	What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity
Primary:	The Honorable Kyrsten Sinema
Committee:	HOMELAND SECURITY (SENATE)

Finally, CISA will proactively warn SLTT governments and other partners when high or critical vulnerabilities are detected on their public-facing information systems, via our Vulnerability Scanning Program. For the most critical vulnerabilities, CISA provides additional, tailored information and patching or mitigation recommendations to SLTT partners, and also emphasizes specific relevant information they already receive via weekly scanning reports.

One challenge at the state and local government level is the need for the technical sophistication to ingest and apply the previous mentioned data for network defense purposes, even when shared in machine readable formats, in a timely manner. This involves SLTT partners vetting what is shared and understanding its applicability for the defense of their specific network and system environments. It is also dependent on existing security solutions and tools the entity has in place. Receiving the information is one challenge, while having the expertise, tools, and resources to apply the information for network defense purposes in a timely manner is a separate, but related challenge.

Post-Hearing Questions for the Record
Submitted to Amanda Crawford
From Senator Maggie Hassan

"What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"

February 11, 2020

1. **State and local entities often simply do not have the funding to address their cybersecurity needs. In your opinion, does the state Homeland Security Grant Program and other DHS grant programs provide enough federal funding for improving the cybersecurity of your state and local communities? If not, then what are the limitations of those programs and what would you propose as a solution?**

   The Texas Department of Information Resources (DIR) currently receives $350,000 in grant funding for cybersecurity in Texas. This provides training for state and local cybersecurity professionals in incident handling, and staff for training and information sharing. We were only able to receive this funding when the State Homeland Security Program (SHSP) was modified to include funding cybersecurity as a requirement.

   The fiscal year 2020 grant allocation for Texas is between $15,839,200 and $19,799,000, which will require allocation of five percent, or between approximately $800,000 and $1 million, for cybersecurity programs. A way to drive investment in cybersecurity would be to increase the percentage of cybersecurity funding from five percent to a larger portion of the funding available to the state. Additional grant funding is available to three urban areas in Texas, namely Houston, San Antonio, and the Dallas/Fort Worth metroplex. This Urban Area Security Initiative (UASI) funding is allocated at between $36 and $45 million; however due to the five percent allocation this results in only $1.8 to $2.25 million in cybersecurity grant funding available to these three cities.

   On April 19, 2019, the Cybersecurity and Infrastructure Security Agency (CISA) issued supplemental guidance to inform the development of the required cybersecurity investment justification. This introduced the Nationwide Cybersecurity Review (NCSR) as a required assessment, starting with the Fiscal Year (FY) 2019 SHSP and the UASI. After working with local governments and school districts over the past year, DIR has become aware of the lack of cybersecurity resources at the local level, to the point where placing a restriction of this kind on an organization's ability to receive grant funding will severely limit them. Many times, when we contact an organization to assist, we are speaking with the local sheriff or city manager. Simply put, many local governments are not well-versed enough on technology or cybersecurity to be able to complete the detailed NCSR. Put off by the complexities and not understanding the requirements of the NCSR, they do not apply for grant funding for cybersecurity.

2. **As you know, communities across the country are actively searching for any and all cybersecurity expertise they can get to help address their cybersecurity needs before an attack occurs. Many states' National Guards are growing their cybersecurity capabilities and expertise. What can we do to help leverage the experience of the National Guard for the cybersecurity needs of state and local entities? What impediments do you see for state and local entities to access this expertise for preventative measures?**

   The National Guard (NG) has been a tremendous asset to Texas in assisting with cybersecurity incidents. Texas currently has 97 authorized guard forces of the approximately 3,270 NG cyber forces available to protect all states. During the August ransomware incident, there were 50 such forces deployed to assist, which at the time was their maximum capacity.

   One issue is the varying authorized forces by state. Texas has 97, where Virginia, Kansas, Maryland and Washington have between 250 and 350 authorized forces. Increasing the authorized forces for each state would be beneficial for Texas, should an even larger incident occur.

   In Texas, because we have a state guard, we have not determined a way to leverage the NG without a disaster declaration to activate the State Operations Center. Consideration for an easier way to leverage NG forces would be beneficial for events that do not rise to the level of disaster scale.

3. **In your testimony, you mentioned the role of academic institutions and the private sector in helping Texas investigate and recover from the August 2019 ransomware incident that impacted twenty-three municipalities. In your view, what can the federal government do to help incentivize these kinds of private-public partnerships?**

   DIR is proposing the establishment of regionally dispersed security operations centers located at Texas universities to aid local governments during a crisis such as the August 2019 ransomware event. This initiative is intended to:

   - provide cybersecurity logging and event management to local governments and school districts;
   - establish "boots on the ground" across Texas so that when a local government needs assistance, in person response can happen in hours versus a day or more; and
   - establish a training program for university students to fulfill future needs for an experienced cybersecurity workforce.

   The initial cost of this program is $58 million for funding the startup of seven regional centers. Adding Endpoint Detection and Response software to the local government computers would add another $168 million per year.

   There are several ways the federal government can incentivize private-public partnerships:
   - Establishing tax credits for private sector partners who assist SLTT governments with their cybersecurity needs.

- Extending the CyberCorps®: Scholarship for Service to state and local government employment in return for financial support. Currently this only applies to the US government. Establishing a similar program where the private sector could fund scholarships in exchange for employment at their businesses would be another way to fulfill future cybersecurity workforce needs.

Post-Hearing Questions for the Record
Submitted to Christopher DeRusha
From Senator Maggie Hassan

"What States, Locals, and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity"

February 11, 2020

1. State and local entities often simply do not have the funding to address their cybersecurity needs. In your opinion, does the state Homeland Security Grant Program and other DHS grant programs provide enough federal funding for improving the cybersecurity of your state and local communities? If not, then what are the limitations of those programs and what would you propose as a solution?

   Response: Limited funding will likely always be a limiting factor in state government's ability to defend against well-resourced malicious actors, and this is even more true for local governments. The more money that is available to states and localities, the more we will be able to invest in necessary security assessments, tools, and personnel that will enhance our security. Another factor is the availability of trained professionals. Often times, and particularly for counties and localities, the availability or ability to afford dedicated cyber professionals simply is not feasible. In those cases, we turn to contractors or outside vendors. This may not "build capacity" in the traditional sense, but it does build capacity for units of government to defend themselves. We simply ask that this be kept in mind as projects are considered. Additionally, we believe the resources that would be made available to both us and our local partners under the State and Local Government Cybersecurity Act would further enhance our ability to safeguard our systems and information.

2. As you know, communities across the country are actively searching for any and all cybersecurity expertise they can get to help address their cybersecurity needs before an attack occurs. Many states' National Guards are growing their cybersecurity capabilities and expertise. What can we do to help leverage the experience of the National Guard for the cybersecurity needs of state and local entities? What impediments do you see for state and local entities to access this expertise for preventative measures?

   Response: The National Guard is a tremendous asset for addressing national security threats at the state and local level. The State of Michigan is lucky to have cybersecurity protection teams (CPTs) within both its Army and Air National Guard units, and Michigan Cyber Security is proud of the strong relationship with our National Guard colleagues. Historically, this has been primarily based on coordination, preparedness, and sharing of best practices, but we are working to better integrate our work and professionals. For instance, we are currently working on a joint exercise in which National Guard cybersecurity specialists will assess the digital defenses of State of Michigan critical infrastructure systems.

   However, the biggest impediment to greater collaboration is a lack of legal guidance. I have leaned on the experience of other state cybersecurity officials to structure our own legal

frameworks for National Guard interaction, including the memorandums of understanding other states have used to authorize activity. However, what we would really like to see is national-level guidance come from the National Guard Bureau on the best ways to leverage National Guard resources, streamlined paperwork and processes, , and clear implementation guidance and examples. These inconsistencies and lack of clear authorities and process may be the biggest challenge for better leveraging National Guard in support of state and local government resources.

3. In your testimony, you spoke about leveraging the Michigan Civilian Cyber Corps to connect civilian cybersecurity talent with communities impacted by ransomware to help investigation and recovery efforts. What metrics have you used to judge the success of this program? What has worked well in this program and where do you see challenges? What recommendations and best practices do you have to offer for other states wishing to establish a similar program and how can the federal government help?

   Response: One of the greatest challenges we have faced is awareness: many entities that could potentially leverage the Michigan Cyber Civilian Corps (MiC3) are not aware that such a resource is available to them. We are working to overcome this deficit by including MiC3 as a partner in our Cyber Partners initiative, which encourages coordination among local government officials in the state. As other states create similar organizations, we would encourage early and frequent collaboration with state-wide organizations that unite local government, education, healthcare, and other sectors and encourage cross-border incident response coordination. While each state will have its own unique experiences and challenges, all will face similar hurdles. This is where the Federal Government could prove to be a big help. If the Cybersecurity State Coordinator Act of 2020 becomes law, DHS will have a tremendous pipeline of information at its disposal. DHS could potentially build a civilian cyber corps starter kit, providing solutions to common challenges and templates these fledgling organizations will need. State security officers currently do this informally, but DHS could bring greater maturity and standardization.

EVOLVING THE U.S. CYBERSECURITY STRATEGY AND POSTURE: REVIEWING THE CYBERSPACE SOLARIUM COMMISSION REPORT

WEDNESDAY, MAY 13, 2020

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

The Committee met, pursuant to notice, at 9:30 a.m., via video conference, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, Lankford, Romney, Scott, Hawley, Peters, Carper, Hassan, Sinema, and Rosen.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. Good morning, everybody. This hearing is called to order. I certainly want to welcome the witnesses. We have the two co-chairs of the Cyberspace Solarium Commission (CSC), Senator Angus King and Congressman Mike Gallagher. If I lived just a little bit further north, Congressman Gallagher would be my Member of Congress.

We also are pleased to welcome Suzanne Spaulding, who—I will introduce people formally prior to the testimony—and also Thomas Fanning, two of the commissioners of the Commission.

I first of all want to thank the co-chairs and the two commissioners for their important work on the Cyberspace Solarium Commission. I think the end product is excellent. I think it has some solid recommendations that a number of these are within our Committee's jurisdiction and we will be working hard to evaluate those, and the ones that we can, get them passed into law. Other of these recommendations can be done through executive action.

What I would like to spend my time, just enter my formal written statement into the record,[1] I just really want to talk about two of the Commission's recommendations. When I got here in Congress in 2011, cybersecurity was a hot issue. It still is. It is not going away. But I remember the buzzword back then is we have to do something about this.

Now we have made a number of attempts, and quite honestly, we made a fair amount of progress. My own sense is that, the bad

[1] The prepared statement of Senator Johnson appears in the Appendix on page 159.

guys, they always have an advantage. But I think we are catching up. I think we are closing that gap between offense and defense.

But, there have been some very common themes. The first one is we have to do a better job of the information sharing. I think we have accomplished that, certainly, certainly with the establishment of the Cybersecurity and Infrastructure Security Agency (CISA), headed up by Chris Krebs right now.

By the way, we had a conference call with Director Krebs just last week, and he was reporting that, bad actors, cyber actors are trying to take advantage of coronavirus disease (COVID), trying to steal some of the medical information on development of vaccines. So again, this is a persistent threat. It is not going away, which is what makes the Commission's work so incredibly important.

But the first recommendation I want to talk about, that, quite honestly, we are working hard at getting hopefully included in the National Defense Authorization Act (NDAA) so it can become law, is the need to put somebody in charge, a national cyber director. We held a hearing a couple of years ago of the blue-ribbon study panel, and this was another type of panel established on biodefense. And it is interesting that their No. 1 recommendation is the same as this Commission's, is we need somebody in charge.

Not too long ago we held a hearing on 5G. Once again, the No. 1 recommendation out of that committee hearing was we need somebody in charge of the implementation and development of 5G if we are going to compete in the world. And so now, lo and behold, I think the No. 1 recommendation out of this Commission is we need somebody in charge.

Now there is some controversy behind that. Exactly how to set it up is complex. I signed on a letter with Senator Rounds, who is kind of leading the charge on the Senate Armed Services Committee, asking the Commission to continue, while you still have your Commission, to study and make recommendations exactly how that national cyber director would be established, what part of the administration that individual should be placed into that they can have the maximum positive impact. So hopefully the Commission will stay together and make that recommendation and we can get that included into the National Defense Authorization Act.

The other recommendation I want to talk about is something that we did cover in a hearing with Director Krebs, both in a secure setting as well as in a public hearing, is the need for—and this is actually, Senator Hassan and I have a bill on this. The bill is called Cybersecurity Vulnerability Identification and Notification Disclosure Act of 2020. There is just a need for CISA to be able to contact individuals where they have noticed that there is a threat, and right now the only way they can contact those people is if they can literally subpoena the records to find out who those individuals are, to identify them so they can contact them. This should not scare anybody. It should not be an issue with civil liberties. But it is a very necessary authority that CISA needs, and I am going to ask everybody on our Committee to do everything we can to by hook or by crook, hopefully get that in the National Defense Authorization Act as well.

So anyway, those are the two things I want to concentrate on. I do not want to steal the Commissioners' thunder here in their

testimony, or my Ranking Member, Senator Peters, his thunder, with his opening statement. So I will turn now to Senator Peters.

OPENING STATEMENT OF SENATOR PETERS[1]

Senator PETERS. Very good, Mr. Chairman. Thank you. Thank you for bringing us together for this hearing and thank you to our witnesses for joining us today and for your hard work on the Cyberspace Solarium Commission. I would especially like to thank our colleague, Senator King, for his leadership on cybersecurity policy, and for appearing before us here today and subjecting himself to our questions. So thank you, Senator King, for doing that.

Cyberattacks are clearly one of the greatest threats to our national security, and as the Commission found in your report, the United States is not thoroughly prepared to defend itself in cyberspace. The findings and recommendations included in your report could not come at a more important time. Adversaries like China, Russia, and Iran have repeatedly attempted to hack into our critical infrastructure, interfere in our democratic process, and engage in large-scale intellectual property theft.

Most recently, the Chinese government launched a cyberattack against our hospitals and health care research facilities in an effort to steal information on the coronavirus vaccine, an attack that threatened the health and the safety of Americans. Every one of these attempted attacks are targeted to undermine our national and economic security, and without sufficient cybersecurity tools, resources, and skilled personnel, these attacks could have a devastating impact on our daily lives.

Your report makes some critical recommendations that Congress must consider as we work to ensure that our country is better prepared to deter, to prevent, and to recover from malicious-style attacks. Your recommendations are very wide-ranging, but I think they boil down to basically three main goals. One, we must work with our allies to promote responsible behavior in cyberspace, we must deny benefits to our adversaries who exploit our vulnerabilities, and we must impose greater costs on those who engage in malicious cyberattacks.

I have been very proud to work on a bipartisan basis with many of my colleagues here on this Committee to advance legislation that will help meet some of these goals, and I look forward to discussing these recommendations today and finding some additional ways for us to come together and to make sure that we are dealing with cybersecurity issues.

So thank you again to all of our witnesses for joining us today, and I look forward to your testimony.

Chairman JOHNSON. Thank you, Senator Peters. I know this is a Web event, not an in-person hearing, but it is the tradition of this Committee to swear in witnesses. So I will just ask you to swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God.

Senator KING. I do.

Mr. GALLAGHER. I do.

---

[1] The prepared statement of Senator Peters appear in the Appendix on page 160.

Ms. SPAULDING. I do.
Mr. FANNING. I do.
Chairman JOHNSON. Thank you.

Our first witness is Senator Angus King. Senator King is the co-chair of the Cyberspace Solarium Commission. Since 2013, Senator King has served as the first independent Senator from the State of Maine. Prior to joining the Senate, Senator King was the Governor of Maine for two terms. He is a graduate of Dartmouth College and the University of Virginia Law School. Senator King.

TESTIMONY OF THE HONORABLE ANGUS S. KING, JR.,[1] CO-CHAIR, CYBERSPACE SOLARIUM COMMISSION

Senator KING. Chairman Johnson and Ranking Member Peters, I really appreciate the opportunity to testify before you. What I would like to do is give you a little background on the Commission, what our fundamental findings were, and then talk about our strategy of layered cyber deterrence.

First, the Commission. It was set up by the 2019 National Defense Act, and the mission of the Commission was to establish an overall strategic direction for American policy in cyberspace, that is No. 1, and No. 2, to make recommendations for implementing that strategy.

The Commission had 14 members, 4 from the Congress, 4 from the Executive, and 6 from the private sector. It was entirely nonpartisan. There were really no partisan discussions whatsoever, and apart from the four Members of Congress, I have no idea of the partisan affiliations of any of the other members of the Commission.

We had 29 in-person meetings. We interviewed over 400 people. We went through thousands of pages of documents. We ended up with 81 recommendations, 57 of which require legislative action, which have been submitted to the various committees and the staffs in the Senate and the House.

So what are the fundamental findings? The real basis of the Commission rests upon three issues. One is reorganization. Get the structure right, and the Chair talked about this at the beginning. The second is resilience. How do we build cyber defenses to keep ourselves safe from attack? And the third is response. How do we respond to attacks in such a way as to defend our country?

Now the fundamental strategy, if you will, is called layered cyber defense, layered cyber deterrence, and here are the layers. No. 1 is shape behaviors. That is, establish norms and standards in the international community so that this is not a unilateral, one-country kind of effort.

The second is to deny benefits, and that is to strengthen our cyber defense, and part of this is reorganization, part of this is strengthening CISA and other agencies that we will talk about later this morning. But to basically be more resilient, and that includes plans for the recovery of the economy, in the case of a cyberattack.

The third is the strategy of deterrence. We have been attacked over and over, over the last 10 or 15 years, and our adversaries

[1] The joint prepared statement of Senator King appear in the Appendix on page 162.

have paid very little price. We need to establish a clear declaratory policy that if you attack the United States in cyberspace you will have to pay a cost. And that is really the fundamental idea of deterrence, and we have to be clear about it, and we have to have our adversaries make the calculation that attacking us is going to cost them. I want to change their calculus when they are making that decision, and that is what the fundamental strategy is that we are going to be presenting to you today.

Thank you very much for holding this hearing. I look forward to answering your questions.

Chairman JOHNSON. Thank you, Senator King.

Our next witness is Congressman Mike Gallagher. Congressman Gallagher is the Co-Chair of the Cyberspace Solarium Commission. He represents Wisconsin's Eighth congressional District in the U.S. House of Representatives. He received a bachelor's degree from Princeton University and a Ph.D. in international relations from Georgetown University.

Congressman Gallagher served in the United States Marine Corps (USMC) for 7 years and did two deployments in Iraq. Congressman Gallagher.

TESTIMONY OF THE HONORABLE MIKE GALLAGHER,[1] CO-CHAIR, CYBERSPACE SOLARIUM COMMISSION

Mr. GALLAGHER. Thank you, Chairman Johnson, Ranking Member Peters, distinguished Members of the Committee. It is an honor to be here presenting the findings of the Cyberspace Solarium Commission, and thank you to you and your staffs for engaging so proactively with the work of the Commission as we try and turn our recommendations into actual legislation.

We start, really, from a sobering recognition, similar to the one which animated the original Project Solarium some 67 years ago, which is to say the status quo is not getting the job done. I would wholeheartedly agree with Chairman Johnson that we have taken important steps toward reform, such as standing up CISA, U.S. Cyber Command (CYBERCOM). But for a variety of reasons we have yet to achieve the speed and agility that is necessary for survival in cyberspace.

So how do we get there? As my good friend and fellow co-chair, Angus King, continually reminds me, structure is policy. And I would like to talk a bit about our recommendations related to structure.

First, we believe we must create a House permanent select and Senate select committee on cybersecurity in order to streamline congressional oversight and authority. Second, we believe we must establish a Senate-confirmed national cyber director, that Chairman Johnson talked about, to lead national-level coordination for cyber strategy, and really to serve as that public voice for cybersecurity and emerging technology issues.

Third, we believe we need to strengthen CISA to ensure the national resilience of critical infrastructure, conduct national risk management and cyber campaign planning, and lead public-private collaboration, ultimately allowing CISA to compete for talent not

[1] The joint prepared statement of Mr. Gallagher appear in the Appendix on page 162.

only with the National Security Agency (NSA) but with Google and other attractive private sector companies. Fourth, the Commission believe we need to recruit, develop, and retain a stronger Federal cyber workforce and thereby close our 35,000-person Federal cyber workforce gap.

And fifth and finally, we believe we need to strengthen our cyber supply chains. The Commission has taken an approach that believes in the power of free and fair competition to breed innovation, but our current strategy amounts to little more than occasionally limiting the access of firms that we do not trust into our markets. I believe this is not working, and consider the competition for 5G, where the Chinese Communist Party (CCP) is able to subsidize their national champions, like Huawei, thereby advance their goal of dominating the global market without having to respond to market forces.

To counter this, the Commission calls for investing information and communications technology (ICT), industrial capacity, and reinvigorating our investment in research and development (R&D). Of course, this will cost some money, but whether, in terms of responding to a pandemic or responding to a massive cyberattack, we believe that America can no longer afford to depend on the largesse of the Chinese Communist Party for critical technologies.

And with that I would like to once again thank Chairman Johnson, Ranking Member Peters, along with my co-chair, Angus King, as well as Commissioners Tom Fanning and Suzanne Spaulding. What really made this a unique experience was the quality of participation we got from our outside experts, the Executive Branch, and, of course, the sitting Members of Congress. And with that I look forward to your questions.

Chairman JOHNSON. Thank you, Congressman Gallagher.

Our next witness is Suzanne Spaulding. Ms. Spaulding is a commissioner of the Cyberspace Solarium Commission and the Senior Advisor for Homeland Security Center for Strategic International Studies. She was the Under Secretary for the Department of Homeland Security's National Protection and Programs Directorate (DHS NPPD), now the Cybersecurity and Infrastructure Security Agency, from 2011 to 2017.

Ms. Spaulding previously served 6 years at the Central Intelligence Agency (CIA) as Assistant General Counsel (GC) and Legislative Advisor to the director's Nonproliferation Center. Ms. Spaulding.

TESTIMONY OF THE HONORABLE SUZANNE E. SPAULDING,[1] COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Ms. SPAULDING. Chairman Johnson, Ranking Member Peters, and Members of the Committee, thank you for this opportunity to testify here today.

I want to touch briefly on three areas that I think can and should be acted upon quickly, particularly given the vulnerabilities that have been exposed by the pandemic. The first is strengthening DHS's Cybersecurity and Infrastructure Security Agency, or CISA, as the organization that I led as the Under Secretary at DHS is

[1] The joint prepared statement of Ms. Spaulding appear in the Appendix on page 162.

now called, thanks in no small measure to the work of this Committee, for which I am grateful.

Congress recognized CISA's central role in our country's efforts to reduce cyber risks, and the Commission strongly endorsed this view. With malicious cyber actors targeting hospitals and health research, and an at-home workforce presenting a massive attack surface, CISA's work has never been more important, which is why we urge Congress to provide the agency promptly with the resources and authorities that it needs, including mission support functions, to be able to be the national risk manager, provide continuity of the economy planning, identify systematically important critical infrastructure, and coordinate planning and research across the Federal Government and with the private sector.

Second, with regard to improving the cyber ecosystem and reducing vulnerabilities, the Commission understood that markets are usually more efficient than government and can drive better cybersecurity. We looked at why the market is not performing that function today, and a key reason is that markets need information in order to be effective. To provide this information, we ask that Congress establish a national cybersecurity certification and labeling authority to help consumers make informed decisions when buying connected devices, publish guidelines for cloud security services, create a bureau of cyber statistics, promote a more effective and efficient cyber insurance market, and pass a national data breach notification law.

Finally, I believe one of the most important pillars in the report is resilience. We need to reduce the benefits side in the adversary's cost benefit analysis. Sometimes the most cost-effective way to reduce cyber risks will be reducing our dependence on those network systems, developing redundancies, perhaps even analog backups or ways of interrupting cyber effects. Paper ballots are a way of building resilience into election infrastructure, for example.

We have a number of urgent election-related recommendations, but I would like to conclude this morning with our recommendations to build public resilience against disinformation. Media literacy can help, but we really need to focus on defeating a key objective of our adversary, which is to weaken democracy by pouring gasoline on the flames of division that already occupy online discourse, pushing Americans to give up on our institution, not just election but the justice system, the rule of law, and democracy. They seek to destroy the informed and engaged citizenry upon which our democracy depends.

To defeat our adversaries' objective, the Commission calls for reinvigorating civics education, to help Americans rediscover our shared values, understand why democracy is so valuable, that it is under attack, and that every American must stay engaged to hold our institutions accountable and continue to move toward a more perfect union.

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

Chairman JOHNSON. Thank you, Ms. Spaulding.

Our final witness is Thomas Fanning. Mr. Fanning is also a Commission of the Cyberspace Solarium Commission and the Chairman, President, and Chief Executive Officer (CEO) of South-

ern Company, one of the nation's leading energy companies. Mr. Fanning has worked for Southern Company for more than 38 years.

He currently serves as the co-chair of the Electricity Subsector Coordinating Council (ESCC), the principal liaison between the Federal Government and the electric power sector, on matters of national security, from terrorism and cybersecurity to disaster recovery. Mr. Fanning has previously served on the board of directors and Chairman of the Federal Reserve Bank (FRB) of Atlanta. Mr. Fanning.

TESTIMONY OF THOMAS A. FANNING,[1] COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Mr. FANNING. Good morning. Thank you, Chairman Johnson, Ranking Member Peters, and members of the Committee for the opportunity to testify today.

The United States is at war, virtually unchecked for years. Our adversaries have been stealing our intellectual property and disrupting American commerce and our democratic way of life. This war is being waged primarily on our nation's critical infrastructure, mainly the energy sector, telecommunications networks, and our financial system.

Fully 87 percent of the critical infrastructure in the United States is owned and operated by the private sector, making collaboration between the private sector and the government imperative.

The Cyberspace Solarium Commission was created to reimagine U.S. national security doctrine for this new digital reality.

The layered cyber deterrence approach outline in the Cyberspace Solarium Commission report serves as a practical roadmap to protect, repair, hold accountable, and respond to existential cyber threats. We propose a three-pronged strategy for success: reshape behavior on the battlefield, impose costs on our adversaries, and deny benefits to our enemies.

Certainly there is no internationally accepted principles of escalation and de-escalation in cyberspace. The first step in reshaping behavior on this battlefield is to define State-accepted behaviors in cyberspace to include clear consequences for behaviors that are not acceptable. Then we need to communicate these behaviors not only to our friends but also our adversaries who attack us.

Every day American companies like Southern Company face millions of cyberattacks, including from nation-state adversaries. With the full support of the private sector, the Federal Government must advance a strategy to defend forward and maintain an offensive posture in cyberspace through regular, persistent engagement with friends and foes alike. This engagement must include the full weight of the Federal Government, including the Department of Defense (DOD), the Federal Bureau of Investigation (FBI), the Secret Service, and the intelligence community (IC) to allow for rapid and effective responses to these attacks.

The third strategic prong is to deny benefits to our enemy. We do this by strengthening the critical infrastructure's ability to maintain continuity against a cyberattack. We must also take steps

[1] The joint prepared statement of Mr. Fanning appear in the Appendix on page 162.

to reshape the cyber ecosystem, the people, processes, and technology and data that make up cyberspace toward greater security.

Finally, we must create a true joint effort between private industry and government. This means moving beyond information sharing to allow common access to actionable intelligence, elaborative analysis, joint planning, and joint action. It also means clearly identifying the most systemically important critical infrastructure and bringing to bear the full resources of the United States Government in supporting and defending them from nation-state attacks.

Senators, the cost of inaction is too great. The public and private sectors are true partners in this effort and we must move forward in better harmony. I am confident the Cyberspace Solarium Commission's report and recommendations will help us to do that. I am happy to answer any of your questions.

Chairman JOHNSON. Thank you, Mr. Fanning.

Let me just quick start out with Senator King. I am assuming you received the letter from Senator Rounds, asking the Commission to study, and potentially up to the point of legislative language, propose the exact structure for the national cyber director. Is that a mission you have accepted, and something you may be able to conclude?

Senator KING. Absolutely. Yes, I talked with Senator Rounds about that last week, and I think the questions are good ones, and I think it is absolutely appropriate that we are going to apply ourselves to answering those questions and try to flesh out some of the details of how this new office would work, what the authorities would be, and how it would fit in with other structure of the Federal Government.

Chairman JOHNSON. OK. Thanks, Senator King. Congressman Gallagher, my second point was giving CISA that subpoena authority so that when they identify a threat they are also going to be able to find out who is being targeted by that threat and provide notice. What are the prospects of, for example, Senator Hassan's and my bill to accomplish that? What are the prospects in the house?

Mr. GALLAGHER. Well, we very much support the recommendation and appreciate the work that you are doing. We fully support the bill language.

As for the prospects in the House, I cannot give you a good assessment right now, but we are working with the committees and really sort of leveraging one of the unique strengths of the Commission, which is that Jim Langevin, who was the other House member on the Commission, a Democrat, has enormous influence within his caucus on these issues. He is a subcommittee chair on a relevant cyber-related subcommittee, and he has been a champion of this proposal, as well as some of the more hotly debated proposals, such as the creation of a special elect cybersecurity commission in the House.

But I just would say we believe that the administrative subpoena authority, as called for in the Commission's report, and as called for in your legislation, would strengthen CISA's ability to be proactively detecting vulnerabilities in critical infrastructure and help secure them before they are compromised.

And the final point I would make is this is very much in line with the approach we tried to take throughout the report, which is not to create a bunch of new agencies with fancy new acronyms, but to take a look at the agencies that exist right now, particularly CISA, and figure out how do we elevate and empower it and give CISA the tools it needs in order to accomplish its very important mission.

Chairman JOHNSON. If you could spearhead the efforts in the House so we can have common language, so if it passes one chamber we are not ping-ponging it back and forth. And again, my goal would be to get this attached to the National Defense Authorization Act.

Ms. Spaulding, you mentioned the need for a national data breach notification. When I started talking about we had to do something back in 2011, those are always the first two goals, better information sharing and a national preemptive standard for data breach, I did not realize how incredibly complex and difficult that was. That is part of your recommendation. Do you have a secret formula for actually accomplishing that?

Ms. SPAULDING. Unfortunately, Mr. Chairman, we do not. We understand that Congress is going to need to work through those issues. And our recommendation was really designed to describe the elements that we think need to be in such legislation and really to try to add wind to your sails as you attempt to corral your fellow members into reaching consensus, because it is something that is so important to achieve on a national level, as you fully understand.

We have breach notification laws in effect. There are over 50 of them, and every State has their own. And it is difficult, obviously, for businesses who operate across State lines, but it also does not result in the kind of statistics and information, on a national scale, that could help, for example, this national bureau of cyber statistics, that could help advance the cyber insurance market, could help Chief Information Security Officer (CISOs) who are trying to make cases to their management for return on investment. That is the kind of information that a national breach law could help accomplish.

Chairman JOHNSON. As you well know, we are going to need a lot of help. I am not even sure we have our sails up, much less wind in them.

Mr. Fanning, you and I have spoken in the past and met about my concern about, for example, electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) as a threat to our national grid. Cyberattacks represent a similar type of threat. Can you give us some assurance that we are addressing these problems, that we have resiliency within our electrical grid? I mean, what progress has been made?

And I am particularly concerned right now that Iran has launched, successfully, a satellite that is circling the globe and, coming up over America probably multiple times a day. That is a big concern of mine.

Mr. FANNING. Yes, Senator, thanks, and I appreciate our dialogues in the past.

I think one of the points that I have tried to make is that there needs to be comprehensive approaches to all of these issues. In fact, when the ESCC, my leadership now there has been about 7 years on the ESCC. And we have seen cyber issues, we have seen natural disasters like hurricanes and tornadoes, and now we see the coronavirus pandemic.

What we need to do is have a comprehensive approach where we harmonize the efforts of government with the efforts of the private sector, and let's not forget State and local governments and our international partners.

So the whole idea is to have a comprehensive approach to this. I would say that every silo of government, and I would say the silos of the strategically important sectors of the economy, have been doing a pretty good job. But what we have to do in order to advance the ball for America is to harmonize these efforts and collaborate.

Chairman JOHNSON. Well, again, thank you, Mr. Fanning. I will reserve the rest of my time and turn it over to Senator Peters.

Senator PETERS. Thank you, Mr. Chairman. My first question is for Senator King and Mr. Fanning. News reports have recently indicated that the Chinese government has been sponsoring cyberattacks against our hospitals, our government networks, and our medical research institutions, presumably in search of COVID–19 vaccine research. This is clearly unacceptable. It puts Americans' lives at risk.

So my first question to Senator King is how would some of the recommendations, specifically in this report of yours, enable us to combat these kinds of attacks that we are seeing from China?

Senator KING. Unfortunately I think it is important to note that China is a long-range problem in cyberspace. They are clearly active, they want to be more active, and they are coming at us. I think if you go back through our recommendations, No. 1, we need to step back and start talking about establishing international norms and standards so that if there is a violation it is not only us that are calling foul but it is the whole world. And I think that has to be part of the strategy for combating something like what China is doing.

Second, we are talking about resilience, which is strengthening our defenses.

But the final piece that I think is so important is to let the Chinese and the whole world know that if you pull something like this you are going to pay a price. And we do not define what the price is. It does not have to be kinetic. It does not have to be cyber. It does not have to be any particular price. But there will be consequence, because I believe that one real problem with the whole cyber posture has been that we have been basically taking the punches without responding, and I want our adversaries to say maybe if we do this we are going to get whacked in some way, shape, or form.

And so this is exactly the kind of thing that we have been talking about, and frankly, one of the things we talked about was if you come at us in a time of national crisis, like the pandemic, the response will be even stronger. The penalties will be stronger.

And so I think it has to be sort of a comprehensive strategy. But you are absolutely right. And, one of the things this pandemic has showed us is how vulnerable we are, particularly if you stop and think about it, how many people are working from home. We have the whole level of target space, if you will, that we were not showing to the world just 2 or 3 months ago.

Senator PETERS. Yes, absolutely. Thank you, Senator King. Well said.

Mr. Fanning, as the CEO of a critical infrastructure company I am sure you would like to jump in and add how we protect infrastructure from Chinese attacks and others.

Mr. FANNING. Look, it is all over the place. As I said, my company alone gets attacked millions of times a day. That is not unusual for any of the major critical infrastructure providers.

One of the things I championed over the years, and now we have formed is the Tri-Sector Group——

Senator PETERS. Yes. I know it.

Mr. FANNING [continuing]. Working with guys like Jamie Dimon at JP Morgan, Brian Moynihan at Bank of America (BOA), Randall Stephenson at American Telephone and Telegraph (AT&T), we developed a joint threat matrix, basically modeling what the different kind of consequences and likelihoods are for a whole spectrum of attacks. And so now we are developing a wish list. Now they show up in the Solarium recommendations. We have been kind of working through our work to make sure that we are consistent with what really is happening in the private sector and what we need to do about it as a Federal Government.

If I can, an important point in this whole, I think, report is you do not see very many words like "sharing" and "cooperate." It is collaborate. Since 87 percent of the critical infrastructure is owned by the private sector, and we are under relentless attack, we have to first illuminate the battlefield. We have to share the effort of the intelligence community, of our sector-specific agencies, and then the folks that will hold the bad guys accountable—Department of Defense, FBI, et cetera. We all have to work together and we all have to be accountable to make sure that we keep America safe.

Senator PETERS. Thank you. Thanks to both of you for that answer. We must do more to protect our nation's critical infrastructure from really these types of attacks, as you mentioned, and many other attacks that are happening on a daily basis.

Recently I have pressed the Administration to hold the Chinese government accountable. They need to be held accountable for irresponsible actions, to make it clear that this activity is simply not going to be tolerated, particularly during a time of pandemic, and that there needs to be consequences for these future attacks, whether it is addressing cyber threats or our overreliance on China for medical supplies needed to address the coronavirus pandemic. I think we need to all stand up to the Chinese government, and we have to strengthen our national security. This effort is so important.

My next question is for Senator King as well. The Solarium's recommendations regarding the continuity of the economy I think are particularly relevant, given the challenges that we are addressing here with the coronavirus pandemic. So in the event of a wide-

spread or a prolonged cyberattacks on critical infrastructure, I think we all agree that the impact could be catastrophic.

So my question for you, Senator King is can you discuss the recommendation, and what lessons do you think we are learning from COVID–19 that you think we should be considering for a long-term cyberattack?

Senator KING. I think one of the first things we have learned is the necessity of planning, the necessity of thinking the unthinkable, of putting smart people into a room and talking about what could happen and what would happen, and how to bring the economy back. I think the continuity of the economy planning and setting that up as a real function is one of our most important recommendations. And we have to be thinking about what happens if the Northeast grid goes down, or the Southern grid. But we have to be thinking about the lessons that we are learning now, some unanticipated.

Frankly, I think once we get through this awful situation that we are in now, one of the most important things is an after-action assessment, what I call an after-action assessment. What did we learn and what was missing? What are the critical functions? What are the pieces that we need to be paying attention to that are likely to be vulnerable?

Before I finish, also let me mention the Chairman asked a question about breach notification. Senator Wicker, Senator Cantwell, and Senator Moran, all three have bills on that. I think they are good bills. And so I think there are some models that we can go forward with.

But to get back to continuity of the economy, I think it is absolutely a critical function. It has to be strategic, it has to be specific, and I want to be ready when this happens. It is going to happen, Mr. Senator. It is going to happen. I told somebody the other day, "We are seeing the longest wind-up for a punch in the history of the world, but that punch is going to come."

Senator PETERS. Yes, absolutely. Thank you for that answer. Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Peters. Let me just read off the list of questioners in order: Senators Scott, Carper, Hawley, Hassan, Rosen, Romney, and Lankford. Now I do not see Senator Scott on the board, so if that is incorrect have somebody text me. But right now we will go to Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman. Very nice to see all of you here, and Senator King, thanks for your good work on so many fronts. Congressman Gallagher, I do not know that I have had the pleasure of meeting you but I am happy to see you and look forward to that.

I would say to Tom Fanning, when I heard your first name I liked you immediately. That was even before I read your bio. So welcome. And Suzanne, it is always great to have a Kappa in the house, and we welcome you.

I am going to ask you to step back just a little bit. I had the benefit of actually being up close and personal watching what we have

done or maybe failed to do, in the Congress in this regard, with regard to cybersecurity.

You will recall, Tom Coburn was my wingman on the Homeland Security and Governmental Affairs Committee (HSGAC) for a number of years and he worked with you and your colleagues at the Department of Homeland Security. I feel we accomplished a lot with the support of several of the Members of the Committee today in this hearing.

Just reflect back on some of the steps that we have plugged in, including making it easier for the Department of Homeland Security to hire people that are needed. With the EINSTEIN, as you may recall, we really got a lot done to try to improve our ability to defend against cyberattacks. What did we do well, and one of the things we have tried to do was try to create a system, and we finally did in 2018. But what are some things that we did well, and what is the unfinished business please? Thank you.

Ms. SPAULDING. It is great to see you, Senator Carper, and thank you for the question, and thank you for all of your hard work over those years and continuing to today in your leadership on cybersecurity and so many other important issues.

You did accomplish a great deal, and I would say some of the most important things were solidifying the authority of what was then the National Protection and Programs Directorate and is now—again, thank you—CISA, because that is really important. Government operates most effectively when it has a clear mission, and helping to codify the existing mission of the cybersecurity and infrastructure resilience effort at DHS was a really important step forward.

And so your work on the legislation to codify its operations center, the National Cybersecurity and Communications Integration Center (NCCIC), for example, very important to get those authorities in place. Its position, codifying its role as the primary central place for the business sector to come with information, right, and to be the key place that gets information back out to the private sector. So clarifying very clearly what that mission is, and that DHS has been tagged with that mission, was really important, and continues to be important.

Resourcing the agency, under your term the budget began to go up and has continued to rise. But really, it was so far behind to begin with that there needs to be significant increase in those resources, and particularly as I mentioned, for those mission support functions that do not get the attention. Typically it is easier to get funding for a specific program to go out and do something. But the back office support for the procurement, for acquiring the technology that needs to be acquired, for example, for the human resource (HR) functions, our human resources, so that we can bring in that talent that we need so badly to be able to do this mission. Funding those adequately becomes very important, and the Commission strongly recommends that.

To continue to make sure that the leadership there has the expertise that it needs. So we recommended a 5-year term for the CISA head of that agency, so that they can be in there long enough to become familiar and then really move out on a strategy and making sure that we are doing the mission effectively.

So the things that you started, that the Committee has continued to pursue, they need to continue but they need to be accelerated. And it all needs to be done as it has been to date on a bipartisan basis. I want to thank our co-chairs, Senator King and Congressman Gallagher, for leading us in such a bipartisan and really nonpartisan way. It is the way cybersecurity should be done, and I hope will continue to be done.

Senator CARPER. Thank you so much for those comments. Our friend and former colleague, Tom Coburn, passed away a little more than a month ago, as you may know.

Ms. SPAULDING. Oh, I am sorry to hear that.

Senator CARPER. And he, after a long battle with cancer, he left a great legacy, and this is just one, and we keep trying to build on that.

I think you mentioned in your remarks, Suzanne, you used the words "in order to form a more perfect union," which is, as you know, part of the beginning preamble of our Constitution. And it is a reminder again that as much as we have tried in past years to do a better job in this regard, the threats continue to evolve and the sources of the threats continue to evolve. So must the responses to them.

I remember when, right on the heels of September 11, 2001, we created the 9/11 Commission, and it was chaired by, I want to say, a former Governor. I forget who the co-chairs were. Lee Hamilton. I think Lee Hamilton was one of the co-chairs and a former Governor from New Jersey, as I recall, a Republican. And they presented us with 40-some recommendations. They were all bipartisan recommendations. John Lehman was on the commission, a bunch of wonderful people. And our Committee, the Committee that is meeting today, literally adopted all but maybe a handful out of about maybe 40 recommendations. It was a great bipartisan leadership co-chair. In the case of Angus and Congressman, and all of you have done today is critically important.

Senator KING. Senator Carper, if I could interject, Mike Gallagher has characterized our Commission, the work we are doing, we want to be the 9/11 Commission without 9/11.

Senator CARPER. That is great.

Senator KING. That is exactly what we are trying to do here, to think about how to respond, and how to respond in a systematic, across-the-government kind of way, and the private sector. But that is the key—the 9/11 Commission, without 9/11.

Senator CARPER. Thank you. When I give commencement addresses, Angus, one of the things that I tell my graduates is to aim high, work hard, embrace the golden rule, do not quit. But one of the areas we have not quit in, but we do not have a lot to show for it, are our efforts on data breach, and create a national approach, a uniform national approach, instead of having 50 States with their own approaches. That is what I think the legislature——

Senator KING. That is one of our key recommendations.

Senator CARPER. We look forward to working with you on that. There are so many different committees of jurisdictions and so many competing issues and interests. But with your help and support, and maybe the good bipartisan work, we will finally get the ball in the end zone.

Senator KING. Thank you.

Senator CARPER. Thanks so much.

Chairman JOHNSON. Thank you, Senator Carper, and we certainly appreciate you again pointing out Senator Coburn, that that was a huge loss for all of us, from the Senate and for this Nation. I also appreciated, Ms. Spaulding used the term "nonpartisan." I really prefer that to "bipartisan." It just totally eliminates the even thought of partisanship. There is nothing partisan about the threat that we really face and the solutions we need to enact. So I appreciate that.

Our next senator is Senator Hawley.

OPENING STATEMENT OF SENATOR HAWLEY

Senator HAWLEY. Thank you, Mr. Chairman, and thank you to all the witnesses for being here. Thank you for the excellent work of this Commission. Congressman Gallagher, can I start with you? I want to come back to something that you mentioned in your joint testimony, which is how China has used cyber-enabled economic warfare to fuel its rise, including the theft of trillions of dollars' worth of intellectual property and attempts to undercut our economic competitors. I particularly appreciated your focus on this, and I have appreciated your own work in the House on this issue.

I just want to give you a chance to expand on some of those themes which I think are so important. So let me just ask you, start by asking when it comes to cyberattacks, what is it you see? How does China typically operate? How do they typically attack? Whom do they typically target? And what is it that they seek to gain or disrupt?

Mr. GALLAGHER. Well, just quickly, my own awakening on this issue was painful. I spent most of the last decade as a Middle East specialist in uniform, not really understanding much about the way in which China operated. But I remember vividly getting a letter from the Office of Personnel Management (OPM) after the massive hack of over 22 million people's—Federal Government employees' records, saying, "Thank you for your service but your records have been hacked."

And that was really a wake-up call for me to recognize that I needed to widen my own aperture and understand what was going on. And, of course, General Secretary Xi Jingping had just come to power 2 years prior, and I think it is fair to say that even the most hawkish sinologists at that time did not yet fully understand how aggressive a direction he would take the Chinese Communist Party.

And, of course, since that point we have not only had the OPM hack, we have had multiple—a series of attacks that we know go all the way back directly to the Chinese Communist Party. In addition, we know that there are certain State champions, Huawei and Zhongxing Telecommunication Equipment (ZTE) in particular, that operate effectively as appendages of the Chinese Communist Party. We had the in-depth reporting from the Wall Street Journal suggesting that Huawei technology at the African Union headquarters essentially beamed back information every night at the same time, around midnight. We have had something called the Finite State

report, which pointed out the scale in which Huawei technology has been compromised.

And we found nothing to contradict that assessment in our own work on the Commission. If anything, we would emphasize the findings of the Blair Huntsman commission, which called the transfer of the intellectual property theft on the order of $300 billion a year, the greatest transfer of wealth in human history.

I would say that up to this point, and what I alluded to in my opening testimony, we have taken primarily a defensive approach, which has been necessary but insufficient. In other words, we have said, we are going to put Huawei on the entities list. We are going to do a variety of things to dissuade our allies from operating with certain CCP champions. However, what the Commission recommends is adding to that with a positive approach that involves a significant investment in research and development, finding creative ways to work with allied countries on key technologies in order to ensure that we are not dangerously dependent on China going forward, and finding a way just to make a positive case for American global leadership and a contrasting case with what we have seen from the CCP.

Senator HAWLEY. Yes. Very good. Thank you for that. Let me ask you just a little bit about a closely related topic, which is our supply chain vulnerability, and particularly as it relates to China. I was pleased to see the report acknowledge how extended supply chains threaten the U.S. ecosystem, our economic ecosystem, and, of course, I have been an advocate myself for reshoring and onshoring supply chains, particularly our critical supply chains, whenever and wherever possible.

Can you elaborate for us on some of the Commission's recommendations for addressing supply chain vulnerabilities through risk management techniques, and what role in particular do you see the private sector playing here?

Mr. GALLAGHER. Absolutely. So we recommend, and I believe recommendation 4.6 in our report, that Congress directs the government to develop and implement an information and communications technology industrial-based strategy to ensure more trusted supply chains and the availability of critical information and communications technology. So this starts with a simple identification of which technologies are critical and where we have single points of failure in the supply chain, so that we are not discovering those single points of failure in the midst of a crisis, which I would submit we are, in some cases, when it comes to advanced pharmaceutical indicators, certain basic medical equipment right now.

And so we are asking the Federal Government, with an enhanced CISA and an enhanced cyber focus more generally, to identify proactively where are the areas where, no kidding, we either have to bring that manufacturing back to the United States, as you have had multiple pieces of legislation aimed at doing that, but potentially also work with partners.

So, for example, when it comes to semiconductors, Taiwan is an obvious target for enhanced cooperation. I believe the Administration right now is exploring some sort of deal with a major Taiwanese Semiconductor Manufacturing Company (TSMC), in order to build certain facilities in the United States.

But it all starts with that identification of our domestic and our allied ICT industrial capacity and identifying those key areas of risk where a foreign adversary could potentially restrict the supply of a critical technology or intentionally introduce supply chain compromise at a large scale. And that, in turn, should direct our actual investments in those key areas and our investments in research and development.

Senator HAWLEY. Yes. That is really good. Tell me about what role you think the private sector plays here and how we get a balance of both requirements and also incentives to help the private sector get to where it needs to be.

Mr. GALLAGHER. I think this is one of the major things we wrestled with throughout the Commission's entire work, which is to say how do you get that balance between, we do not want to sort of out-CCP the CCP, for lack of a better term. We cannot adopt a one-size-fits-all, heavy-handed, top-down series of regulations, and Tom Fanning can attest to that better than anyone else, given his unique position. How do we, instead, pursue that incentivizing approach?

And what we sort of landed on is there are simple things we can do to incentivize the private sector rather than mandate they do certain things. So, for example, one of the recommendations you see in the report is mandatory penetration testing for publicly traded companies, so that they have to invest more in cybersecurity. Because what we saw time and again is that wherever the C-suite did actually prioritize and take cybersecurity seriously, those companies outperformed their competitors.

And so we would like to, for example, over time, see certain best practices that are emerging right now become the industry standard. So for example, there is something called the 1–10–60 rule, where, you are able to detect an intrusion on your network in 1 minute, you are able to have someone look at it within 10 minutes, and then you are able to isolate it, quarantine it within 60 minutes. By incentivizing the C-suite to invest in cybersecurity we believe that, over time, best practices like that can become the norm.

And I would say, and Suzanne alluded to this before, we deliberately tried to adopt an approach that harnessed market forces so that the private sector could step up and respond to a clear incentive that the Federal Government is setting.

Senator HAWLEY. Very good. Thank you. Thank you all for——

Senator KING. Senator Hawley, I would like to touch on your question for a moment.

Senator HAWLEY. Yes, please.

Senator KING. The supply chain. No. 1, we have learned in the COVID situation how critical the supply chain is and what a mistake it is to rely on supplies for critical materials outside of our borders.

The second piece is we have to realize that the Chinese are integrating economic policy with intelligence and national policy by subsidizing things like Huawei to make it cheaper in order to insinuate itself into the nation's, or the world's internet infrastructure. We have to realize the cheapest may not be always the answer, and maybe a little premium on the price to have control of the supply chain is an insurance policy.

And I think that is the way we have to look at this, because historically we just said, well, we will get the cheapest wherever we can, and that is going to bite us. And supply chain, I think, we just have to analyze every piece of military equipment and every piece of critical infrastructure and say where is it coming from, and is it safe? Because I think you have identified one of the most serious issues that is facing us, and it is not going to quit.

Senator HAWLEY. Thank you. Thank you for that, Senator King, and thank you for your leadership over many years on this issue, and it is a privilege to get to serve with you on the committees that we do.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Senator Hawley. Senator Hassan.

OPENING STATEMENT OF SENATOR HASSAN

Senator HASSAN. Thank you for this hearing and thank you to our panelists for your work, all the effort you have put in, and for being with us in this new remote hearing world we live in.

Senator King, I wanted to start with a question to you. The comprehensive report outlines many key steps that the Federal Government can take to prevent and mitigate the effects of cyberattacks. However, the report is relatively quiet on how the Federal Government can help strengthen State and local government's ability to prevent against attacks.

Just recently, the National Governors Association wrote a letter to House and Senate leadership, asking for funding to help State and local government defend against crippling cyberattacks amid the COVID–19 pandemic. And even before this crisis, legislation was introduced to both the House and Senate to create a sizable Federal cybersecurity grant program for State and local governments.

We all know that our collective cybersecurity is only as good as our weakest link, to your last point that you were just making, so it is critical that we work to improve our nation's cyber resiliency down to our smallest localities. Did you examine the possibility of Federal support for State and local cybersecurity, and if so, what were your conclusions?

Senator KING. We absolutely did, and, in fact, a major wave of ransomware has attacked our cities and towns.

Senator HASSAN. Yes.

Senator KING. We have had small towns in Maine that have been talked about—that have had hits of ransomware. I think there was something like 45 mentions of State, local, Tribal governments.

But here is what we wrestled with. We believe, and we will advocate for the creation of a fund to assist States and localities in dealing with these issues, not only money but also technical expertise, which CISA has and we have throughout the Federal Government. But part of it, part of the thing we wrestled with was what I call moral hazard. We do not think the Federal Government should relieve the States of their own obligations to protect their own networks and to do what is necessary.

So what we proposed was a matching program, where it would start with a 90 percent Federal share, 10 percent match for im-

proving critical infrastructure on the State level, which, year by year, would scale up and end up be 50–50. We want the States to be engaged as well. We do not want them to say, "Well, cybersecurity is the Fed's job. That is not our job." That will not work.

So that was the way we approached it, but we understood, and believe deeply, that working with the States on critical infrastructure is absolutely important. I mean, it is elections. National Guard has a role to play here. I think there are a lot of ways that we can integrate with the States properly.

But it needs to be a shared responsibility, I guess is the way I would put it. The Commission wrestled with this but that is where we came out.

Senator HASSAN. I thank you for that. I would make the note, and New Hampshire has seen ransomware attacks on very small jurisdictions, tiny school systems.

Senator KING. Yes.

Senator HASSAN. When it comes to town meeting time, or when it comes to State budget balance, what you do not want to do is have the matching obligation be so great that you put at risk Federal cybersecurity because a small town cannot meet a cyber obligation, or a State has to cut its budget to balance it. So those are always the things we have to think about.

I wanted to move on to Ms. Spaulding, and I wanted to build on something that Senator Johnson asked about. As you know, one of the Solarium conditions, recommendations is for Congress to pass the Cybersecurity Vulnerability Identification and Notification Act. The bipartisan bill passed our Committee, and Senator Johnson and I are continuing to work to pass the bill into law.

Ms. Spaulding, drawing on your experience at the Department of Homeland Security, can you explain why CISA needs the administrative subpoena authority, particularly in the context of the COVID–19 pandemic?

Ms. SPAULDING. Yes, Senator. Thank you for that question and thank you for your efforts to try to get this authority passed through Congress. It is something that we have needed for quite some time, and going back to my time at DHS.

DHS has the tools to scan the internet for vulnerabilities, for known vulnerabilities, to find systems that are publicly facing the internet that we can tell have the vulnerability that we are looking for. What we cannot do, without a tremendous amount of effort and sometimes not at all, is to identify then who owns that system, so that we can reach out to them and warn them. So this would be an administrative subpoena.

The folks who have the information about who owns that system are the providers, the internet service providers (ISPs). And so what we need to be able to do is to take that Internet Protocol (IP) address, which the tools allow us to know, and go to those providers and say, "We have found this. It looks like an industrial control system, which is something that may power our critical infrastructure. It could be in the energy infrastructure, transportation, all kinds of infrastructure. And we see that they have this very dangerous vulnerability that an adversary, a bad actor, could exploit and cause problems." But we do not know who it is and we cannot tell them.

Senator HASSAN. Thank you for that response, and I look forward to continuing to work with Senator Johnson and Members of the Committee on getting this legislation passed.

Ms. Spaulding, I also wanted to talk to you about cyber threats in health care. Prior to the pandemic, the health care sector was a top target for malicious cyber actors, and in the context of COVID–19, when hospitals are already facing strained resources, I am really concerned that ransomware attacks could have a real impact on human life.

It appears that the threats are not just to hospitals now. CISA recently released a warning that some nation-state bad actors are targeting U.S. COVID–19 medical research efforts. So obviously that is very concerning.

Can you help us understand what we can do right now and going forward to improve the resiliency of our health care sector, the cyber threats, including the current threats to these critical medical research facilities?

Ms. SPAULDING. Yes, Senator. It is such an important point, and it is addressed by our Commission recommendations in a number of ways.

This is really the kind of event, series of events, that, for example, could be covered under the cyber State of distress that we talk about in the Commission report, which falls short of the kind of national emergency where you have physical destruction and consequences along the lines of a hurricane or a superstorm, but are beyond the routine, day-to-day occurrences that we deal with every day.

The attacks during a pandemic on this vital infrastructure could rise to the level of the cyber State of distress, and the key there is that it would trigger the ability for CISA, particularly, to use funds to tap into a recovery, a responsive recovery fund, to scale up, to go out and help these researchers, these facilities that are being attacked, the hospitals, our health care providers, and to bring in additional resources, particularly to call on assistance from experts within the DOD or the intelligence community, where we have to reimburse them. So that is a key part of that authority and really critically important.

Senator HASSAN. Well thank you, and I see I am over time, Mr. Chair. If there is any time for additional questions I have one more for Senator King, which we can do later, on the National Guard. Thanks.

Chairman JOHNSON. OK. Sounds good. Thank you, Senator Hassan. Next will be Senator Rosen, and then Romney and Lankford. But Senator Rosen.

OPENING STATEMENT OF SENATOR ROSEN

Senator ROSEN. Thank you, Mr. Chairman. I thank you and the Ranking Member for bringing this great hearing today with these amazing witnesses. Thank you for your work, and especially my colleagues, Senator King and, of course, Congressman Mike Gallagher. We were freshmen in the House together and we were both founding members of the bipartisan Problem Solvers Caucus. And so we did a lot of great work there and I am happy to see that you

are continuing with that, and I look forward to seeing what you are doing.

We know that the Cyberspace Solarium Commission report found that shortages in our nation's cybersecurity talent are both widespread in the public and private sector. As a former computer programmer and systems analyst I have introduced a number of bipartisan bills to promote our cybersecurity workforce, including legislation to prepare our junior reserve officers training corps (ROTC) candidate students for careers in cybersecurity, build and support apprenticeship programs in cybersecurity modeled after Nevada's in-state cybersecurity apprenticeship program.

So Ms. Spaulding, what do you think are the additional forward-thinking solutions that Congress can offer to provide our business communities, our government with the skilled workforce they need to strengthen our nation's cybersecurity infrastructure and protect Americans from bad actors? And even considering what is happening now, in the pandemic and COVID crisis, also addressing retraining. These are jobs that are going to continue to grow where other jobs may not come back as robustly.

Ms. SPAULDING. Senator, thank you for the question, and thank you so much for your efforts on this really important issue. I noted it earlier and I think making sure that we are doing everything we can to build the talented workforce that we need, on the scale that we need it across this country. It is a huge challenge and something we all need to tackle.

We have a number of recommendations in the Commission report along these lines. One of the most important that we think is to continue to build on the things that are working and that we think are successful. And certainly the Scholarship For Service program, building the cyber corps, is one of those that we think is very important and worth building, where the government reaches out early on to encourage students to study cybersecurity, helps them with their education. And then they have a job with CISA or others across the government.

Where I always used to say to the private sector, "I will take them right out of school. I will give them on-the-job training. I know that you in the private sector will then lure them away with higher salary. But I believe that after a number of years after they have put their kids through college they will come back to government because they will miss "the mission." And oftentimes the audience would laugh, but I know that you know what a strong draw that mission can be.

I think it is also important to focus not just on recruitment but also on retaining that cyber workforce. And one of the things that we certainly worked on at DHS and learned is the importance of an inclusive work environment, so that when you have succeeded in, for example, teaching girls to code, and recruiting women, and a diverse workforce, women and minorities, into the cybersecurity workforce, that you retain those talents by creating an inclusive workforce.

So those are the kinds of things that we looked at and really important programs for Congress to continue to support.

Senator KING. Senator Rosen, if I could join in and——

Senator ROSEN. Oh, yes.

Senator KING [continuing]. Provide another answer to that question?

One thing, and this sounds minor but it can be very major, we need to work on our security clearance process.

Senator ROSEN. That was my next question.

Senator KING. We have been doing a lot of work on it in the Intelligence Committee because we were losing good people. I know of people who just gave up after a year or more of waiting. I must say the Administration has improved that considerably. The backlog is down. They are working better on reciprocity, so if you get a security clearance for one agency it can apply to another. But, that is one of these issues.

The other thing that we talked about was the creation of a ROTC-like program, where you could get scholarship aid and then you would make a commitment when you came out. But you are absolutely right to focus on this issue, because if we do not get the talent, we are in trouble. And we need—I think Mike Gallagher mentioned at the beginning a shortfall of like 35,000 people across the government that we need in the cybersecurity area. So it is one of our most important priorities.

Senator ROSEN. And hundreds of thousands across the country. And I was pleased that last December my Building Blocks of Science, technology, engineering, and mathematics (STEM) bill did pass, which is going to promote STEM education for young girls. And thank you for answering my security clearance question. That was my next question. I do think it is hurting us here in government.

With the short time I have left I just want to talk a little bit about protecting data through cloud services. So Senator King, could you—and for Ms. Spaulding—quickly, what can the Federal Government learn from the private sector's experience in migrating to the cloud services, and how can we better partner with that to be sure that we are able to do that?

Senator KING. Let me start and then I will turn it over to Suzanne. The movement to the cloud can be a very positive development because you do not have all your data in 10,000 locations, all of which are vulnerable. But that means that the cloud itself has to be more secure. And we do talk, in the report, about developing a security standard for cloud-based services so that companies and governments, whoever wants to use a cloud service, can have some knowledge, some assurance that they are dealing with a secure service.

Suzanne, do you want to touch on that issue?

Ms. SPAULDING. Yes, no, that is exactly right. The Commission felt strongly that we really wanted to encourage folks to move to the cloud. For most, that is going to be a more secure environment. You are going to have real experts who are securing that data.

But not all cloud service providers are equal, and so we thought it was really important, again, to try to push the market by providing information for folks on which cloud providers need certain basic security standards. If we are going to encourage folks to move to the cloud, we have to make sure that those cloud environments are indeed secure.

So our recommendation is for the development of guidelines, and that those guidelines be made public, and folks can see whether cloud security providers are indeed providing a secure environment. It cannot just be that it goes to the lowest bidder.

Senator ROSEN. I think you are right. I think we also have to include just not national cloud services but think about our international security as we share data across global borders. That is important to secure that as well.

Thank you so much.

Chairman JOHNSON. Thanks, Senator Rosen. Senator Romney.

OPENING STATEMENT OF SENATOR ROMNEY

Senator ROMNEY [continuing]. Be a part of this discussion. It is a bit of déja vu for me, because many years ago, when I was serving as a Governor in Massachusetts I was part of the Homeland Security Advisory Committee. And we came together and spoke about this topic and felt that we were behind and there were actions we needed to take if we were going to be effective in protecting our cyberspace. And what is somewhat alarming is to find that we are still talking about it, and not as much as I might have anticipated being done has actually been done.

And so I would like to focus for a moment on what it is that prevents something from happening. In an authoritarian regime, the person at the top can command something happens and everybody jumps, or in the case of Kim Jong Un they find themselves, no longer breathing.

So we do not have that model and I am not suggesting we do, but we have to use the tools that we have. So I am going to ask Mr. Fanning to begin with. Is there not the potential to create a lot of pressure coming from the corporate sector on the White House? We need to have the White House get fully behind this, because it is hard at the congressional level for us to push a string uphill. I am mixing two metaphors there, but nonetheless it is hard for us to do this from the bottom up. Would it not be helpful if corporate America were to start shouting and saying, "we need the Federal Government to step in here, to provide the following elements to get behind this report."

How do we do that, Mr. Fanning, and why has it not happened so far?

Mr. FANNING. Senator Romney, great to see you again. Look, I think that is happening, the fact that all of the critical infrastructure in America has been working with their sector-specific agencies. I think the issue is really now how do we harmonize and collaborate at all levels of government.

One of the important facts, that I know with your background you will get here, is that not all private sector is created equal. We have called forward a designation, I guess it is Systemically Important Critical Infrastructure (SICI). And so working through CISA, which has already identified on a risk-based approach what the most critical infrastructure is in America, and we do that at the asset level. So we identify assets that can either prevent major loss of life, significant economic disturbance, or prohibit or hurt our ability to defend ourselves, to fight back, to see, to listen.

And so what we are doing is to identify the most critical assets in America, and then evaluating the layers around those assets of the private sector to really work with the Federal Government. And in my opinion it is not just a voice that says "we need more." I think the private sector has a special obligation in this new cyber digital world that we are in to join in the effort to defend America, to join in the effort to have a special relationship with the intelligence community, sector-specific agencies, the DOD et al., to really create a more resilient America. That is why we have the designation of high-priority areas, SICI, a joint collaborative analytic framework, and a variety of other recommendations that will carry this out.

As I walk the halls of Congress and I work in the Administration, my sense is there is a great desire to have this happen. We are not without motivation. And really, I think now says we have got to pool that effort and direct it at a certain way. I think the Solarium Commission report does that.

Senator ROMNEY. I sure hope so.

Senator KING. Senator Romney, can I touch on that for a minute?

Senator ROMNEY. Yes, sure. Angus.

Senator KING. I have a life principle that structure is policy. If you have a messy structure, you are going to have a messy policy. And right now we have a structure in our government that is—we have really good people and really good agencies like CISA, like Cyber Command, but there is nobody in charge. Again, I am going back to my business days, I always like to have one throat to choke, and that is the national cyber director. We need somebody at a very high level who can oversee and coordinate, and work on the planning, with all of these different disparate parts of the Federal Government that are working on this. I think that is an absolutely critical need.

The other recommendation, which has not gotten much discussion today, is we recommend that the Congress reorganize itself and develop select committees on cyber, because we have cyber jurisdiction scattered across, I have heard as high as 80 subcommittees in the Congress. It is very difficult to get anything done.

Now that is going to be difficult because I am on Intelligence and Armed Services. We are talking now to Homeland Security. People are going to have to give up some jurisdiction in order to gain a more coherent approach to this issue, both in Congress and in the Executive Branch.

So you are onto something, and you know, you want some centralized leadership, and if you are Governor or you are President you want somebody you can go to and say, "I want this to work." But right now if you are President you have to go to a whole bunch of different places, and that is our goal here.

Senator ROMNEY. I fully agree. So in one question—I have like five to go and I have one minute to go, so I am not going to be able to get them in. But I wanted to ask Ms. Spaulding whether the intelligence community cannot get behind this effort, particularly with regards to structure, and say "Look, let us tear down some of these barriers between us. Let us go to the White House. Let us get the White House to get fully behind this." It would strike me that if the head of the CIA and the Department of Defense, the

Secretary of Defense were to say to the President, "We really need to have this one person. We need to restructure this in the following way," that is going to happen. But if the White House is dragging its heels on this, it is not going to happen.

I mean, can we get support from the leaders of, if you will, the agencies that deal with this topic, to get behind this principle?

Ms. SPAULDING. So one of the advantages that we had on this Commission, Senator, was that unlike any other commission I have been involved with, and I have been associated with many, we had people from the Executive Branch sitting on the Commission, and they attended every meeting, all of our nearly 30 meetings, over time. And while they were not in a position to sign onto the final report, given sort of separation of powers issues, et cetera, I think there is a strong understanding of the need to coordinate and to have coordination at a senior level for cybersecurity efforts. And the intelligence community is an absolutely essential part of that effort.

So I would like to think, along with you, that we can get consensus around the need for this coordination effort and push this through.

Chairman JOHNSON. Thanks, Senator Romney. By the way, this hearing is clicking along pretty quick. Senator Hassan would like to ask another question. If you want to stick around, I will certainly give you another opportunity to do that.

And Senator King, real quick, our Committee did pass a bill to—a pretty simple bill. I mean, recognizing the fact that there are so many committees of jurisdiction just under Homeland Security, and making it pretty difficult for the Department to really respond properly to Congress, when you are going to that many different committees.

A similar concern you have in terms of cybersecurity, we could not even get that simple commission established into law to take a look at it. That got kiboshed. But I am happy to work with you on both issues, because, again, this is a little insane in terms of how, dispersed the congressional authority is on both cyber as just homeland security.

With that I will turn it over to Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thanks, Mr. Chairman. Thanks for the hearing. I have a ton of questions like Senator Romney was mentioning before. Let me try to click through several of these.

Congressman Gallagher, let me ask you a question. What is the difference, as you would see this, between the national cyber director and what CISA is doing now? Congress has a really bad habit of saying this is not working as we want to so we are going to leave that in place plus add another thing onto it. Are we talking about taking CISA and elevating it, or are we creating two different things, where CISA works for a national cyber director? What is the difference?

Mr. GALLAGHER. Yes. CISA, in the first instance, we are recommending elevating and empowering CISA in a variety of simple ways that I think might surprise you do not already exist. So, for example, starting at the top, we shift the director of CISA to a 5-

year term and increase their pay. We push for new facilities, resources, authorities to elevate their stature in the Federal Government. But CISA is always—and Suzanne, having worked in this job, is the best person to talk about this—in my mind always primarily going to have that mission of defending critical infrastructure, defending the dot-gov space in a similar way in which NSA and CYBERCOM defend the dot-mil space.

So one of the, I think, least appreciated recommendations in the report that could have the biggest impacts is giving CISA the authority to do persistent threat-hunting on dot-gov networks so that they can defend prior to an attack. And the national cyber director, in my mind, has a more coordinating function that is making sure that CISA, in performing that mission, is also working well with NSA, with CYBERCOM, and all the other Federal agencies at play in the cyberspace.

And finally, I think the advantage of a national cyber director, particularly one that is Senate-confirmed, and therefore, in theory, more responsive to Senate and House oversight, is that proximity to the President, having the ear of the President, which would hopefully enhance their ability to coordinate across missions and do long-term planning at CISA, sort of in the fight on a day-to-day basis.

Senator LANKFORD. Right. So more of an Office of Director of National Intelligence (ODNI) type structure.

Mr. GALLAGHER. Oh, we did look at the ODNI structure, and we debated it as a model for national cyber director. Ultimately, we arrived at something that was more modeled after the U.S. trade representative. We found that to be a compelling model, because it is interdisciplinary, it is functionally oriented, and it is institutionalized with Senate-confirmed leadership and situated within the Executive Office of the President.

But this was really one of the more robust debates we had on the Commission.

Senator LANKFORD. OK. Suzanne, do you want to add to that?

Ms. SPAULDING. Thank you. The Congressman had it exactly right. CISA has the role of coordinating across the civilian government agencies, and really from a defensive, if you will, deny benefits, asset response function. So this national cyber director, among other things, would be able to bring together the defensive and the offensive planning to make sure that those things are coordinated, that they are working in a synergistic way and not at cross purposes, and bring in the Title 50, if you will, intelligence and Title 10 DOD authorities into that broader whole of nation, whole of government planning.

Senator LANKFORD. Is that a civilian role, though, not a military role for this position?

Ms. SPAULDING. That would certainly be our recommendation, yes, particularly to be able to do the whole-of-nation work with the private sector.

Senator LANKFORD. Thank you. Senator King, let me ask you about the select committee proposal here. I am shifting out. You and I had talked before that our committee structure was designed in a way that it should have never been designed. It has been more accidental than by design. And over the years, as agencies have

been created, Congress has not kept up with the structure of the House and the Senate committees, and it has become more and more chaotic in trying to be able to hold people to account.

Trying to do another select committee and to be able to strip those away, is it easier to create another select committee or is it easier to strip away all those authorities and land them in a committee? For instance, in Homeland Security Governmental Affairs, ultimately it is designed to do something like this, with a whole-of-government approach on it, but obviously it has other areas that it gets into. Is it better to have it freestanding or better to strip everything away and land it in an existing committee?

Senator KING. I think a select committee, and the analogy, Senator, is to the Intelligence Committees, because they did not exist before the late 1970s, and there was a realization after the Church Committee that there was a real need to have one committee with special expertise in a fairly technical area. And we are talking not only about CISA, but there are military aspects of this, of course—CYBERCOM, NSA, the intelligence agencies.

So I think there is an argument, a good argument to be made for a special select committee. And frankly, one of the things we talked about was having the membership of that committee be the leadership of the various committees, such as this one. That is who would be the members, the Chair and the Ranking Member, or designees. And I think there is a way to do it, and I realize, jurisdiction is life around here. But I think this is a moment like the 1970s where there is a specialized area that is incredibly important to the future of the country, and right now, as Senator Johnson said, you can have a very simple bill and it takes years. And I do not want to go home after a cyberattack and say, "Well, Congress really—we were talking about that and there were a couple of bills, but there were four different committees that had jurisdiction, and it was really hard." I do not think that is going to wash with my constituents.

Senator LANKFORD. Nor should it on that. Tom, let me ask you a question about standards. I saw in the report multiple different times to be able to push the private sector to have better standards, higher standards, creating a standard. There has been a lot of conversation on the Internet of Things (IoT). Once you hit a government standard it does not take long for it to be stale. In the cyber world you have a lot of technology that is tapping a lot of innovation. By the time government, any agency, any entity, sets a standard, it is already out of date. How do we keep a standard from slowing down innovation and actually making things worse?

Mr. GALLAGHER. Yes. Well, and boy, you raise a very important point. A standard should not be thought of as a static certification. Rather, a lot of the standards that will be certified will include a process to evaluate gaps in the future, to evaluate how to improve whatever it is. It will also be kind of weighted by the importance in the critical infrastructure of America. In other words, if it is thought of to be incorporated into the systemically important infrastructure then it will have a much higher standard, a much quicker response time.

So look. I think the private sector, in working with government now, in collaborating, not cooperating, has a special burden to work

to make sure that whatever we do fits the national interest. There will be benefits and burdens.

So if there is more for us to do, and perhaps it is more extensive, I think the benefit will be that you will have a real-time evaluation of the battlefield. As I mentioned, the battlefield today is the electric networks, the telecom, and the financial system. We have to make sure that our stuff works. And if we can get real-time evaluation, collaborating with the intelligence community, our sector-specific agencies, and folks like DOD, we will all be better off. I think this is a big carrot for private industry.

Senator LANKFORD. Chairman, thank you.

Chairman JOHNSON. Thank you, Senator Lankford. I see Senator Sinema, so if she is ready to go she can go. But I also ask any Senator that wants to ask additional questions, use that little hand function. Raise your hand here in the form and I will call on you, starting with Senator Hassan, after Senator Sinema.

Senator Sinema, are you there?

OPENING STATEMENT OF SENATOR SINEMA

Senator SINEMA. Yes, I am. Thank you so much, Chairman Johnson and Ranking Member Peters for holding today's hearing, and I want to also thank our witnesses for your service to the Commission and for participating today.

As our country navigates the coronavirus pandemic, we clearly see the importance of cohesive strategies to ensure public safety. And this pandemic has also shown us the need to fortify our cybersecurity. Overnight, many Americans expanded their virtual footprints through telework, virtual schooling, telemedicine, and virtual social gatherings. We will continue to face immense challenges from the coronavirus pandemic for some time, and we must take steps to ensure our networks are secure.

The parallel between these two threats should also make us ask whether the United States is prepared to sustain and recover from a potential cyberattack. I hope today we can look at this Commission report through the lens of the ongoing pandemic and identify some of the challenges we need to tackle now so we are better prepared for the next crisis.

My first question today is for Ms. Spaulding. This report was published as the United States was pivoting to implement social distancing protocols and stay-at-home orders in response to the pandemic. The pandemic has caused a rapid transition to a much greater reliance on virtual environments. Could you expand on the recommendations you feel are most critical to prioritize, given this new environment?

Ms. SPAULDING. Yes. Thank you, Senator, and you are absolutely right about the heightened risk environment that we face in the context of this pandemic.

There are a number of things. I think as we have this at-home workforce everyone is using their home routers and Wi-Fi networks to interact. And so one of the recommendations that we have is for this national certification and labeling authority, and I do think that is the kind of thing that could get up and running fairly quickly. It is like an underwriter's laboratory, and would help provide information to consumers as they look at securing, purchasing de-

vices like home routers, webcams, et cetera, that we know have been vectors for malicious activity, how to evaluate their purchases from a cybersecurity perspective.

So I think that is critically important to continue to inform the public about how to make wise choices, but also for our business owners. Critically important around the Internet of Things and the industrial Internet of Things that they too have the information that they need to make informed decisions as they are purchasing equipment.

Strengthening CISA and making sure that it has the resources that it needs to do the kind of outreach to the American public and to the business community, to let them know when we are seeing heightened activity in a given area, how to secure their home, devices that they already own. Those are things that can be done right now and that really are—there is a strong sense of urgency about.

Senator SINEMA. Thank you. Senator King, in the Chairman's letter introducing the report you and Congressman Gallagher state very clearly that election security must become a greater priority. I agree with you. One of the report's key recommendations is that Congress should improve the structure and enhance the function of the Election Assistance Commission to help States and localities better protect election integrity.

Arizona's Secretary of State continues to share with me the importance of Federal assistance in helping Arizona's efforts to secure elections. What steps can Congress take to gain bipartisan support for these recommendations about election cybersecurity, and after your response I would pose the same question to Congressman Gallagher.

Senator KING. I will give you two thoughts. First, we need to stabilize the funding for the Commission and enable it to do its job. But second, we have a kind of interesting recommendation. As you know, the Commission is set up on a bipartisan basis, and the problem is that it is deadlocked and quite often cannot take any action whatsoever. We are suggesting the appointment of a fifth commissioner, with technical expertise in the cyber area, who could only vote on cyber-related issues. And this would break the deadlock on the kind of issues that we are talking about here this morning, to enable us, for the Commission to actually do this important work on behalf of all the States.

So those are two specific suggestions, stabilize funding, fifth commissioner limited in their vote to cyber-related issues, to break the deadlock so that actions by the Commission can move forward to deal with this really critical issue.

Mr. GALLAGHER. First of all, Senator, we miss you in the House. It is great to see you again.

Senator SINEMA. Not mutual, but thanks. [Laughter.]

Mr. GALLAGHER. But in addition to everything Senator King said, I just would foot-stomp the fact that we are—something that Ms. Spaulding said earlier, which is we are very much coming out strongly in favor of paper balloting and auditable paper trail. And we recognize the irony of a fancy cyber commission having such a recommendation. In addition to stabilizing the Election Assistance Commission we have a recommendation that intends to streamline

and modernize the sustained grant funding for States to improve election systems.

And then we are intrigued and try to recommend ways in which, in addition to funding from the top down, how can we take advantage of what I would call the bottom up. There are a lot of nonprofits in this space that are providing free cyber literacy campaigns, and we think that is a good thing. We want to encourage those efforts, because a lot of times the top-down funding is entirely dependent on the individual personalities and systems in those States. And so we need a mix of top down and bottom up, going forward.

Senator SINEMA. Thank you so much, Congressman Gallagher. On a personal note, congratulations on your wedding, and one day I will see you in the gym again.

Mr. Chairman, I have no further questions.

Chairman JOHNSON. Thanks, Senator Sinema. I do not see Senator Hassan's hand up but I know you had a question. I see your little video thing on there, so Senator Hassan, do you have your question?

Senator HASSAN. Yes, I do. Thank you. And this is just to Senator King, and again, thanks to all of the panelists today for a really superb discussion.

Senator, the Commission's report includes recommendations to leverage the capacity of the National Guard to help States prepare for cybersecurity incidents. Yet, as you point out, our current Department of Defense policy does not provide clear guidance about what activities the National Guard can conduct or whether these activities can be supported by Federal funding. I know this has been an ongoing issue in my State. What do you think is the best mechanism to engage the National Guard in helping States with preventive measures that decrease cybersecurity vulnerabilities? Do you believe current authorities are sufficient, or does the Guard need clearer authorization to conduct these preventive measures?

Senator KING. I will distinguish between the words "authorities" and "guidance." I think the authorities are sufficient, and as you know, the Guard can be a tremendous asset to the States in this kind of situation, because of their technical abilities.

I think what we believe—I say I think—what the Commission recommends is a clarification of guidance from the Department of Defense that would allow reimbursement to the Guard under Title 32, so that should be able to be cleared up fairly straightforwardly, and that is our recommendation.

The Guard is a tremendous asset. Let us use it and let us not have obstacles to its use.

Senator HASSAN. Because it is really about making clear that when the Guard does cybersecurity work with the State there is a Federal interest in it too.

Senator KING. Absolutely. There sure is a huge Federal interest. So, yes, that was one of our specific recommendations.

Senator HASSAN. Thank you very much, and thank you, Mr. Chairman.

Chairman JOHNSON. Senator Romney.

Senator ROMNEY. Congressman Gallagher, the line of questioning that you described with regards to China's intrusion into our cyber-

space, both corporate and government, was really quite revealing and very effectively presented. And I think you made the point that we, as well as our international partners, need to push back against the intrusions that are being made by China.

And I guess the question is, how can we go about doing that? Any thoughts about that? Right now there is move not only in our country but around the world, everybody pulling back to their own country, whether it is American first or France first, whatever. People are pulling back and becoming less associated on a global basis, to say how do we work on these things together.

But like you, I figure the only way we are really going to get China to be dissuaded from the course they are on is if we and other nations that follow the rules of law, if we come together and say, "Hey, China. If you keep doing these things you can no longer have unfettered free access to our markets. We will respond collectively. You cannot have access to any of our markets."

But I am interested in your thoughts. Can we get there? How do we get there? Does the United States have to lead this? Does someone else lead it? How do we create a recognition on the part, not just here but around the world, that we need to come together and collectively push again the world's most malevolent actor right now, which is China?

Mr. GALLAGHER. Senator, that is a great question, and in some ways I think it is actually the question that we are going to be grappling with for the next two decades. My own view, having watched this play out over the last 2 months, is that I think the momentum for some form of selective decoupling from China will continue, in some ways regardless of who is President come 2021, 2024, or 2025. And I think our challenge—and again, this is my view and this is a bit outside the actual strict text of the Commission report—is that the smart way to avoid autarky, because we cannot make everything in America, while sort of weaning ourselves off dependency on China, is to harness that Made-in-America energy into more productive partnerships with our allies.

So I mentioned Taiwan when it comes to semiconductors earlier. There is an obvious opportunity to expand our partnership with Australia when it comes to rare earths. And what we recommend, particularly in the 5G space, is pooling our resources with like-minded countries who have expertise in this space in order to not just say Huawei and ZTE are bad, but say we, as a free world, have a better product, a more secure product, that we can offer to you, and it is going to cost a little bit more, but it is not going to be cost prohibitive.

So that is sort of the general direction we are trying to push, to sort of push our cooperation with allies. There are a variety of smaller recommendations in line with that, for example, elevating the Assistant Secretary of State position in order to facilitate our cooperation with allies.

The final thing I would say, just to tie it to the question you had asked Senator King earlier, is that while it is very hard to deter the Chinese Communist Party at present, we believe that this is further evidence of the need for a clear declaratory policy. Right? And we are recommending both a strengthening of the existing declaratory policy above the use-of-force threshold to say, hey, if you

attack us we will respond, but also the promulgation of a second declaratory policy below the use-of-force threshold, so China cannot do what reports suggest it is doing right now, hack certain American companies in order to get access to information on a coronavirus vaccine without fearing the consequence.

So there is a lot there. I apologize for going on, but it is a very important and difficult question.

Senator KING. Senator Romney, there is a really important principle, and I think you have hit on it, on a key question. Churchill once said, "The only thing worse than fighting with allies is trying to fight without allies." And in my visits to Asia, what I have found is China has clients and customers. We have allies. And we do not take sufficient advantage of that.

And one of our recommendations is a new position of Assistant Secretary of State for International Norms in Cyberspace. We have to involve the rest of the world in setting what the guardrails are. So if China violates them, just as you have said, they are not just going to be facing some kind of sanctions from us but from the entire world, and they are, above all else, sensitive to economic responses. If it is an international economic response, it is going to be a lot more power than if it is unilateral from our side.

So I think you are asking a key question. I think part of the answer has to be what we have talked about in the report, is the importance of elevating norm-setting and talking about how we can provide some international guardrails to this kind of malicious activity.

Senator ROMNEY. Thank you. I yield my time, Mr. Chairman. Thank you. Very well said, both of you. Thank you.

Chairman JOHNSON. Senator Lankford.

Senator LANKFORD. Let me drill down on that a little bit more, because that is part of my question as well, that was really talking on a nation-state entity. We also have a big problem with cybersecurity with individual actors within nation-states, and we have found it exceptionally difficult to be able to hold them to account.

Some of them, we maybe get a chance to walk through. There is a great story of two Romanians that were basically living like the Kardashians, stealing bitcoin from people all over the world, that they were just basically buying on the dark web information and then putting out ransomware. They happened to hit on some on Pennsylvania Avenue, through our security camera. It was right before President Trump's inauguration. They took over someone's security cameras on Pennsylvania Avenue. It caused an international incident, from two folks in Romania that did not even know what they had. They were just doing ransomware out there. That is a case where we were able to track it back down, be able to get to them and get to arrest them.

But in many countries, whether that be in India, whether that be in South America, whether that be in Eastern Europe, we have actors that are doing this and finding increasing difficulty of working with local governments to be able to hold them to account.

So a lot of our conversation today has been about nation-states. What recommendations do you have on individual actors, and to be able to work with nation-states to hold people to account within their country? What are the options we have?

Senator KING. I mean, that is one of the tough things about cyber is it is sort of changes all the power relationships. You can have two guys in Romania who can really wreak havoc, or even have a small country like North Korea that can also wreak havoc, and you do not have to be a superpower in order to play effectively in this area.

I think this is another place where talking—there are sort of two aspects, two sides of this. One is improving resilience, and we really have not talked a lot about that today, but to really upgrade our games in terms of protection. And you talked earlier about the idea of an underwriter's laboratory label. It would be voluntary, it would be consumer driven, but have people be more careful about what it is they are buying.

And this is going to become much more important as we go to the Internet of Things. It is not only your router that can spy on you. It might be your microwave, or your car, for sure. So we have to be better at defense.

But then I get back into this international piece. If we impose sanctions on two guys in Romania, they may not care. But if the sanctions are also imposed by Hungary, Austria, Russia, and their neighbors, and maybe Romania, then we can get after them. The international cooperation is a way of breaking down the national barriers for law enforcement, in effect, so that we can go against some of these people, wherever they are. But that means we have to expand our reach, and that means we have to be cooperating with our allies.

Mr. GALLAGHER. Could I just quickly add, Senator Lankford, that there is a school of thought out there that we engage with and continue to debate with, that suggests this is precisely the reason why deterrence is not possible in cyberspace. We very much believe it is, because at the end of the day we are not deterring cyber or cyber instruments. We are deterring human beings using those instruments.

And so what you are really touching on is a problem of attribution and the need for us to improve a rapid attribution capability. And we do have a variety of recommendations that attempt to do that, such as codifying and strengthening agencies that already exist, like the Cyber Threat Intelligence Integration Center, in ODNI, so that they can better partner with the private sector and ultimately arrive at a cultural change where they are more proactive in sharing the results of rapid attribution with the private sector entities that may be the target of those lone actors that you identified.

Senator LANKFORD. Yes, the challenge is not just attribution, though that is a significant challenge. It is also enforcement. If there is a group of folks in Pakistan that decide to do this, and we go to the Pakistani government and we say, "We believe this is one of your citizens," and they say, "We believe it is not," now what do we do?

Ms. SPAULDING. So we do have some recommendations to strengthen the FBI ability to bring its law enforcement tools to this whole-of-nation effort, including strengthening their overseas presence and cyber attachés in embassies, and also recommendations that would strengthen mutual legal assistance. So at least in coun-

tries where you can get some cooperation and build relationships, a lot of that is being on the ground, being able to provide assistance to the country in which where this Legat might be based, so that you have built a relationship that when you need information from them, they are willing to cooperate.

Senator LANKFORD. That would be helpful, because this is an ongoing issue, whether that is robocalls in massive numbers, trying to be able to target fraud toward social security recipients, or whether it is a cyber threat directly toward an industry, an infrastructure, or toward stealing credit card numbers and such. We have a global issue on this, and right now we do not have a lot of tools in the toolbox to be able to put pressure on nation-states, to be able to put pressure on individuals within their country to knock it off. And so we have to find some ways to be able to have some leverage. Right now our focus seems to be on nation-states more than it is on individuals within nation-states, and we have to have a balance of both.

So I appreciate all of your work. I do not think I said that earlier. You all have put a significant amount of time into this. For Mike and for Angus, we have talked multiple times about the number of hours that you all have spent on this. So thanks for all the work in compiling this together, and let us make sure it does not sit on the shelf somewhere. There is a lot implement.

Senator KING. Thank you. We agree.

Chairman JOHNSON. Thanks, Senator Lankford. I see that Senator Hassan found the little hand. Senator Hassan, do you have another question?

Senator HASSAN. Just really a comment and a reminder. First of all, let me echo Senator Lankford's thanks to all of you. But just a reminder, Mr. Chair, that this Committee passed an Internet of Things standards bill that would say that when the Federal Government purchases Internet of Things that certain security standards would have to be met. So we have something we passed out of committee that we might be able to work from and keep pushing on. So I just wanted to make that note. Thanks.

Chairman JOHNSON. OK. Thank you. I have one last question for Ms. Spaulding, and then what I will do is give all the witnesses a chance for a closing comment, and I will do it in reverse order, starting with Mr. Fanning.

But Ms. Spaulding, you mentioned that the Commission is recommending that most people transfer their data into the cloud, and again, it makes a lot of sense. You would assume that the cloud probably has the absolute best security versus a bunch of other smaller actors.

But can you provide some assurance, because I think the counter of that is the fact that now rather than have just a huge dispersement of all this data across thousands and thousands of companies, now we are going to have all of our eggs, all of our data eggs in one or a few very large baskets, that if that security is breached it could represent a really big problem, make a really big mess.

Can you just kind of address that aspect of it?

Ms. SPAULDING. That is an excellent point, and it is something, for example, in elections in 2016, we looked at the decentralization of elections across the country as a way of mitigating the risk of

a national impact from hacking activity. But really, if you look—and that is a good example. If you look carefully at that, particularly in States and counties and locations around the country where there might be a very close election, that decentralization is not necessarily going to buy you protection.

It is an ongoing discussion about the value of biodiversity, if you will. The diversity of systems and assets, making it more challenging for the adversary.

I think what we have seen, however, is that the adversary is able to overcome a lot of that. And so as we have seen these broad attacks in which the adversary, for example, takes over routers and webcams, hundreds of thousands of them across the country and around the world, millions, we realize that we are not getting as much benefit from that distributed network. And if you have secure cloud providers, you really can, we have concluded, increase your overall security of your systems.

But that is key and that is a point we emphasize with our recommendation. You need to have security standards for those cloud service providers.

Chairman JOHNSON. That gets to your recommendation of some kind of national certification of those types of services.

Ms. SPAULDING. That is exactly right, both the certification of the kinds of equipment that folks might purchase and then guidelines and making sure that those cloud service providers meet the relatively high level of security standards.

Chairman JOHNSON. OK. Thank you. Mr. Fanning, do you have some closing comments?

Mr. FANNING. Yes, Senator and Chairman, thank you so much for your leadership in this. I have always enjoyed our chats, and your whole Committee is doing really the Lord's work here.

Let me just say this. We did not talk as much during this hearing about the importance of the collaboration between the private sector and government. This is not going to be a government-led issue, in my view, at the end of the day, because so much of the infrastructure is in the hands of the private sector. We really do need to join the obligation, and there are some important issues that arise out of that, that are really different from the way we think about it today.

One of the clear examples is this continuity of the economy. The old model in our industry, in electricity, was reliability. There was a cost associated with an outage and we could figure out how reliable the equipment must be in order to prevent that cost. The notion of resilience says this is how my system operates under abnormal conditions, whether it is a hurricane, a snowstorm, a COVID virus, or a cyberattack. The only way that we will be able to continue the economy and provide an American way of life that we are all used to is for the private sector to pitch, not catch, and to work with the Federal Government and the State and local governments, whether it is the fusion centers, the Governors themselves, or the State and local government, to really think about a different way to turn the economy back on and get us back on our feet.

This Commission's report, I think, deals with a lot of those important issues, and I think it is really important to consider the ramifications of that going forward.

So thank you for your time. I really appreciate it.

Chairman JOHNSON. Thank you, Mr. Fanning. Ms. Spaulding.

Ms. SPAULDING. Thank you, Mr. Chairman, and I want to add my thanks for your leadership on these issues and for giving us the time this morning to talk with the Committee and answer your questions and talk about our Commission report.

I thanked our outstanding leadership earlier, but I do want to thank Tom Fanning. He is really somebody who walks the talk. He has not only been an outstanding contributor to the Commission report, bringing that valuable insight, but I know from my time at DHS, when he and I worked closely together with the Electricity Subsector Coordinating Council, which he has chaired for such a long time, that he is somebody who really gets this issue and is out there every single day, trying to make sure that our infrastructure, not just in electricity but across other critical sectors, is going to be there when the American public needs it.

His point about resilience is so important. This is an exercise not in risk elimination. We will never have 100 percent security. This is risk management. And resilience, the ability to be reliable, that is just baked into the electric sector, for example, is such an important lesson for us to spread across this country as we talk about cybersecurity.

So thanks very much.

Mr. FANNING. Thanks, Suzanne.

Chairman JOHNSON. Well, thank you, Ms. Spaulding. Congressman Gallagher, you are up to the plate.

Mr. GALLAGHER. Thank you, Mr. Chairman, and thank you, Ranking Member Peters, for this opportunity. I just would add that we very much view our unique makeup of this Commission as an asset with not only participation from outside experts but the Executive Branch and sitting legislators as a way we can avoid the report just collecting dust on a shelf somewhere.

Your staffs have been excellent in terms of working with us and our staff thus far. We hope to continue that collaboration and partnership as we fight to get some of our recommendations in the National Defense Authorization Act and other legislation. And we are at your disposal in terms of anything you need from us or our team as we debate these issues. Though we did not solve everything in this report, we attempted, if nothing else, to provoke a debate and build upon the work that you have already done.

So thank you for allowing us to talk about it today.

Chairman JOHNSON. Well thank you, Congressman Gallagher. Senator King, you have the bases loaded. You are batting clean-up. Knock it out of the park.

Senator KING [continuing]. Beginning, Mr. Chairman, and talk about why we are here. We are here because this nation is under threat, and we are in the midst of this coronavirus crisis now, which is absolutely an unprecedented crisis. There is no doubt about that, and that is taking a lot of the attention. But the fact is this threat has not gone away. In fact, it has been magnified by this crisis.

And so the job we have now is action. And we have talked this morning, and all of us on this hearing, in this hearing share an understanding of these issues, share an understanding of how impor-

tant they are. But we have to communicate that to our colleagues, that this is not something academic. This is coming at us. And it is not something that may come at us. It is coming at us today. Our private sector is being pinged millions of times a day right now by malicious actors.

And so we have really got a responsibility, it seems to me, to move forward. You have already taken a lot of leadership on this issue. You have already talked about bills, about the administrative subpoena bill. We ought to get rid of the word "subpoena," by the way. I think that scares people. We need another word, because what we are really doing is seeking information in order to warn and assist companies that are under attack.

But we have talked about the need for national leadership, for some kind of coordination, for better resiliency, and also for a declaratory policy that puts our adversaries on notice that they will pay a price for coming after the United States of America.

We have the means. I think the Commission report has given us some important guidance, and now it is up to us, as Members of Congress and as people from the private sector who have made such a huge contribution to this project, to work together to do something. I do not want to walk away and say, "Well, we had a great Commission. It was a good report. 81 recommendations, 57 legislative proposals, but we really did not accomplish much."

I think the onus is on us now to make it happen, and this Committee has certainly been on this for a long time, and I deeply appreciate the support you have already indicated for some of our major recommendations. And I really look forward to working with you to get the details right, to work with the House and other committees in the Senate so that we can take action here to defend this country that we love.

Thank you, Mr. Chairman. We really appreciate the time you took with us today and the attention you have given to this critical subject.

Chairman JOHNSON. Again, thank you, Senator King. Yes, I completely agree with you. We have to turn this report into real action.

So I want to thank the four of you, all of the other Commissioners, all the staff members who have worked so hard on this for your hard work, your dedicated efforts, and your very thoughtful recommendations. We will do everything we can to bring those to fruition and get them, where required, signed into law or try and get implemented through executive action.

So again, thank you all for all your hard work.

That concludes this hearing. The record will remain open for 15 days, until May 28 at 5 p.m.

Yes? Senator Carper.

Senator CARPER. I sent a message to you that I wanted to add, if I could, just a short thought here at the end. I apologize for interrupting but apparently you did not get that message.

Chairman JOHNSON. No, I did not. Do you have a question?

Senator CARPER. No, I do not. I just have a short thought I would like to add.

Chairman JOHNSON. Oh sure. Go ahead. I am sorry.

Senator CARPER. Yes. Thank you very much. Again, our thanks to each of you, not just for the work you have done on this project,

but you have led extraordinary lives and continue to lead extraordinary lives. Some of you know, we pretty well are in debt to all of that.

I came here like 20 years ago. I joined the Governor—as Angus knows. I served with some of our colleagues in the House of Representatives before that. I was a naval flight officer (NFO) for many years, and served throughout the Cold War, 23 years and all active and reserve. And my father and my father's brothers, my mom's brothers served in World War II. The battle that they took on the threat, that they addressed, was fascism, Nazism. And they rose to the occasion and we came through that. A lot of loss of life, but we came through it, thank to their courage.

Much of my life I spent in airplanes chasing Soviet nuclear submarines all over the world, trying to make this world a safer place from communism.

A couple of months after I arrived here to the U.S. Senate we suffered a terrible attack on 9/11, that we all remember. And then terrorism became our threat. Today that is still a threat. Communism is not. Fascism and Nazism is not. But security threats, they evolve from the use of cyberattacks. That is a major threat to our security as a Nation.

The reason why we have succeeded and came out of 9/11 is extraordinary leadership, and not just the leadership of our President—I commend him—and not just the leadership of those in the Congress. But I want to again raise up Tom Kean, the former Governor of New Jersey. And I want to raise up, if I could, Lee Hamilton, a great leader in the House of Representatives. Pretty extraordinary leadership that they provided to the 9/11 Commission. And to Susan Collins and to Joe Lieberman, who provided extraordinary leadership to our Committee, extraordinary leadership to our Committee. They led the adoption of almost unanimous adoption of virtually every one of the recommendations.

The key here is the leadership. It is the leadership. You have done your part. And you have brought to us, I think, a great game plan, and our challenge is to pursue it. And it is up to our Chairman, Ron Johnson, and the Ranking Member, Gary Peters, and those of us who serve on this Committee to make sure that your good work does not go to waste.

And often the Chairman says, and I commend him, he says one of the reasons why we are successful at the Committee and one of the reasons we are successful in Congress is because we set aside our partisanship and we work as Americans to address the challenges and go forward. It is huge challenge. And we are always stronger together. If we are in this case we will do just fine, and America will be grateful for it. Thank you.

Chairman JOHNSON. Thank you, Senator Carper, for those comments. We are going to teach you how to use that little hand, show you where the button is. I was right in the middle of my wind-up, so I will finish.

Senator CARPER. I apologize. Thank you.

Chairman JOHNSON. No, I appreciate those comments, and I appreciate, really, the way you have approached your chairmanship when you were Ranking Member as well. And I think we have all continued the tradition that Susan Collins, Senator Lieberman,

yourself, Senator Coburn have really laid out for this Committee. So thank you for your work.

But with that we will conclude the hearing. The record will remain open for 15 days, until May 28, at 5 p.m., for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 11:36 a.m., the hearing was adjourned.]

APPENDIX

"Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report"
Opening Statement of Chairman Ron Johnson
May 13, 2020

As prepared for delivery:

Today's hearing will focus on examining the findings and recommendations from the Cyberspace Solarium Commission's recent report. The Commission's report is a call to action that identifies critical cyber shortcomings across the public and private sectors, and recommends holistic, coordinated, nonpartisan solutions to those problems.

The cybersecurity challenges we face are growing in number and sophistication. From data breaches in the retail sector to the financial sector, no industry is immune from hackers. In the last few years, we have seen an emergence of ransomware attacks. It is estimated that 966 government, education, and healthcare entities have been victims of ransomware such attacks in 2019, causing operational and financial costs of roughly $7.5 billion. The COVID-19 pandemic necessitates an even greater need for vigilance to protect against these threats to the healthcare system. Other issues – like how we develop and maintain secure supply chains, particularly with the emergence of China, Inc. in the telecommunications equipment market – are equally challenging.

As our federal agencies have evolved to counter these threats, ultimately expanding federal programs and bureaucracy, it has become more and more clear that we can't answer a simple question: "who's in charge?"

I am pleased that the President appointed a senior White House official as the point person on 5G issues who can define that problem and provide a clear federal strategy. Yet I believe we need that kind of clarity across all cybersecurity policy.

Accordingly, I am particularly interested in the Commission's recommendation to establish a National Cyber Director. This is an important recommendation that deserves careful consideration. A National Cyber Director could set a president up for success and ensure that his or her policies are being implemented across the government.

There are many outstanding questions, however, like how a National Cyber Director would be involved in defensive cyber operations; combating the theft of intellectual property; and reviewing budgets. We also need to find consensus on the appropriate scope of authorities and powers a National Cyber Director would need to be successful. We need to get these details right to ensure that this new position can cut through the bureaucracy, not add to it.

Another important Commission recommendation is the need for the Cybersecurity and Infrastructure Security Agency to have administrative subpoena authority to identify and warn critical infrastructure owners and operators of vulnerabilities. I sponsored legislation that would provide this authority with Senator Hassan, the *Cybersecurity Vulnerability Identification and Disclosure Act*, and we passed it out of committee by voice vote. This is an important authority that will make the critical infrastructure of this nation more resilient from hackers and I appreciate the Commission's support as we work to get this authority signed into law this year.

I want to thank all of the witnesses for participating virtually today and I look forward to our discussion.

U.S. Senate Committee on Homeland Security and Governmental Affairs
"Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report"

OPENING STATEMENT OF RANKING MEMBER GARY C. PETERS
May 13, 2020
AS PREPARED FOR DELIVERY

Thank you to our witnesses for joining us today and for your hard work on the Cyberspace Solarium Commission. I especially would like to thank our colleague Senator King for his leadership on cybersecurity policy and for appearing before us today and subjecting himself to our questioning.

Cyber-attacks are one of the greatest threats to our national security and, as the Commission found in your report, the United States is not thoroughly prepared to defend ourselves in cyberspace.

The findings and recommendations included in your report could not have come at a more important time.

Adversaries like China, Russia, and Iran have repeatedly attempted to hack into our critical infrastructure, interfere in our democratic processes, and engage in largescale intellectual property theft.

Most recently, the Chinese government launched a cyber-attack against our hospitals and health care research facilities in an effort to steal information on a Coronavirus vaccine – an attack that threatened the health and safety of Americans.

Every one of these attempted attacks are targeted to undermine our national and economic security.

Without sufficient cybersecurity tools, resources, and personnel, these attacks could have a devastating impact on our daily lives.

Your report makes critical recommendations that Congress must consider as we work to ensure our country is better prepared to deter, prevent, and recover from malicious cyber-attacks.

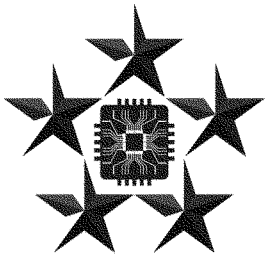
Your recommendations are wide-ranging, but boil down to three main goals:

We must work with our allies to promote responsible behavior in cyberspace; We must deny benefits to adversaries who exploit our vulnerabilities; And we must impose greater costs on those who engage in malicious cyber-attacks.

I have been proud to work on a bipartisan basis with many of my colleagues on this committee to advance legislation that will help meet some of these goals. I look forward to discussing these

recommendations today and finding additional ways we can continue to strengthen our cybersecurity protections.

Thank you again for joining us today, and I look forward to your testimony.



UNITED STATES OF AMERICA
CYBERSPACE SOLARIUM COMMISSION

Testimony of:

Senator Angus King,
Representative Mike Gallagher,
Ms. Suzanne Spaulding, and
Mr. Tom Fanning

Commissioners of the
Cyberspace Solarium Commission

Before the United States Senate Committee on Homeland Security and Governmental Affairs

"Report of the Cyberspace Solarium Commission"

May 13, 2020

INTRODUCTION - INTENT OF THE COMMISSION

The Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The Commission consists of fourteen Commissioners, including four serving legislators, four executive branch leaders, and six recognized experts with backgrounds in industry, academia, and government service. Senator Angus King and Representative Mike Gallagher serve as Co-Chairmen. The Commissioners spent the past eleven months studying the issue, investigating solutions, and deliberating courses of action to produce a comprehensive report. As a group we met 29 times in weekly meetings and the staff conducted nearly 400 interviews with industry, federal, state and local governments, academia, non-governmental organizations, and international partners. We then stressed tested our findings and red teamed different policy options in an effort to distill the optimal approach.

The Commission developed a strategic approach of layered cyber deterrence and identified 82 specific policy or legislative remedies. The legislative recommendations were subsequently turned into 57 legislative proposals that have been shared with the appropriate Senate and House committees. The final report was presented to the public on March 11, 2020.

Throughout this process the Commission always considered the Congress as its "customer." Through the NDAA, the Congress tasked the Commission to investigate the issue of cyber threats that undermine American power and to determine an appropriate strategic approach to protect the nation in cyberspace and identify policy and legislative solutions to achieve that objective. We four Commissioners are here today to tell you what we learned, advocate for our recommendations, and work with you to assist in any way we can to solve this complex challenge.

FOCUS OF OUR EFFORT

Cyber defense and resilience of the nation form the foundation of the Commission's strategy. Critical infrastructure - the systems, assets, and entities that underpin our national and economic security, and public health and safety - are increasingly threatened by malicious cyber actors. Effective critical infrastructure security and resilience require a clear and consistent declaratory policy backed up with the credible threat to impose costs to deter adversaries from targeting the nation in the first place. This also requires reducing the consequences of adversary disruption of critical infrastructure, minimizing its vulnerabilities, and thwarting adversary operations that seek to hold critical infrastructure at risk.

First and foremost, Congress should establish a National Cyber Director within the Executive Office of the President to centralize and coordinate the cybersecurity mission at the national

level. The National Cyber Director will work among Federal departments and agencies to bring coherence both to the development of cybersecurity policy and strategy as well as its execution. This Senate confirmed position will provide clear leadership in the White House and signal cybersecurity is an enduring priority in U.S. national security strategy.

Additionally, a key element of a coherent and consistent cyber strategy across the U.S. government is a clearly articulated deterrence posture, buttressed by a strong declaratory and signaling policy that the U.S. will swiftly respond to impose costs against adversaries who seek to use cyberspace to undermine our interests and values and attack us where we are asymmetrically vulnerable. This declaratory policy should span the range of malicious adversary behavior, including cyberattacks above the use of force threshold as well as adversary campaigns that occur below the level of war. To be credible, we must back up our statements with consistent (and, where possible, transparent) action if and when our adversaries test us.

Second, the government should continue to improve the resourcing, authorities and organization of the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience. The Commission recommends empowering CISA with greater tools to strengthen public-private partnership, including a Joint Collaborative Environment for real-time information exchange and analysis; an Integrated Cyber Center for person-to-person collaboration; and a Joint Cyber Planning Cell for public-private planning that can be rapidly actioned in a crisis. These changes will forge the public-private collaboration necessary to quickly detect, mitigate, and respond and recover from a significant cyber incident.

Third, the United States should take immediate steps to strengthen the resilience of our critical infrastructure. Reducing the consequences of a cyberattack is critical for denying benefits that our adversaries can expect from their operations. These include disruption, intellectual property theft, and espionage. The Commission recommends that Congress codify Sector-Specific Agencies as Sector Risk Management Agencies and strengthens their ability to aid critical infrastructure sectors in identifying and managing the risks they face. This work will be critical to establish a Continuity of the Economy Plan: government-wide and public-private contingency planning to rapidly restart the U.S. economy after a major disruption. In addition, the Commission recommends establishing a Cyber State of Distress tied to a Cyber Response and Recovery Fund. This would give the government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical national functions can continue to operate during a sustained disruption or crisis.

Finally, the Commission recommends two relevant initiatives to reshape the cyber ecosystem and reduce vulnerabilities. The first, the creation of a National Cybersecurity Certification and Labeling Authority, will establish standards and transparency to allow consumers of technology products and services to demand more security and less vulnerability in the technologies they purchase. The second, forming a Bureau of Cyber Statistics, will create better information to

improve the security behavior of individuals and organizations. A Bureau of Cyber Statistics will provide private companies, the public, and government policymakers with an empirical evaluation of what does and does not work in cybersecurity. It will also publish cybersecurity data to inform public policy and cybersecurity investments in the public and private sectors.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID-19 pandemic has been a learning experience for us as it illustrates the challenge of ensuring resilience and continuity in a connected world. It is an example of a type of crisis that spreads rapidly through a system, stressing everything from emergency services and supply chains to basic human needs. The pandemic produces cascading effects and high levels of uncertainty. This situation undermines normal policy-making processes and forces decision makers to craft hasty and ad hoc emergency responses. The Commission evaluated exactly this type of event--complex emergencies that rely on coordinated action beyond traditional agency responses--so that the U.S. does not get caught unprepared by a massive cyberattack.

The lessons the country is learning from the ongoing pandemic are not perfectly analogous to a significant cyberattack, but some parallels are obvious. First, the pandemic and a significant cyberattack are global in nature. Second, both require a whole-of-nation response effort and are likely to challenge existing incident management doctrine and coordination mechanisms. Finally, and perhaps most importantly, prevention is usually far cheaper and more effective than response.

The global health crisis has reinforced the urgency of many of the core recommendations in the Commission's March 2020 report. Responding to complex emergencies will require a balance between response agility and institutional resilience in the economy and critical infrastructure sectors. It relies on strategic leadership and coordination from the highest offices in government, underscoring the importance of a National Cyber Director. It also demands a strong understanding of the risks posed by a crisis and a data-driven approach to mitigating them before, during, and after it, validating the Commission's recommendation to codify Sector-specific Agencies, create a Bureau of Cyber Statistics, and establish a National Risk Management Cycle. Agility in responding to a crisis rests on clear roles and responsibilities for critical actors in the public and private sectors as well as established, exercised relationships and plans, highlighting the importance of Continuity of the Economy planning. The imperative of social distancing during the crisis has brought renewed urgency to securely digitize critical services, stressing the importance of the Commission's recommendation to incentivize the movement to the cloud and broader modernization in state, local, tribal, and territorial governments.

THE CHALLENGE

The more connected and prosperous our society becomes, the more vulnerable we are to nation-state rivals, rogue states, extremists, and criminals. As a result, for the last twenty years, adversaries have used cyberspace to attack American power and interests, and our lack of

response has taught them that, if they attack us in cyberspace, they will not pay a price. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the U.S. government, the private sector, and the public at large.

The American public relies on critical infrastructure, 85% of which, according to the U.S. Chamber of Commerce, is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment to hospitals—are connected and vulnerable. Furthermore, new industries and services, such as cloud computing, have become increasingly important economic growth. As we saw last year, malicious cyber actors don't just target the U.S. government and military personnel--they increasingly target our cities and counties with malware and ransomware attacks.

Creating a secure nation in the 21st century requires an interwoven system of both public and private networks defended from state and non-state threats.

China wages cyber-enabled economic warfare to fuel its rise while simultaneously undercutting U.S. economic and military superiority. Chinese cyber campaigns have enabled the theft of trillions of dollars in intellectual property. At the same time, Chinese APTs' aggressive cyber-enabled intelligence collection operations provide Chinese officials with improved intelligence information to use against the United States and its allies. Chinese operators constantly scan U.S. government and private-sector networks to identify vulnerabilities they can later exploit in a crisis.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In the spring of 2014, Russian-linked groups launched a campaign to interfere in Ukrainian elections that included attempts to alter voter tallies, disrupting election results through distributed-denial-of-service attacks, and smearing candidates by releasing hacked emails. During the 2016 U.S. presidential campaign, Russian operatives used cyber operations to collect and release damaging information on political parties and candidates and conduct influence operations using social media. Since 2016, Russia has continued to spread hate and disinformation on social media to polarize free societies and seek to interfere in democratic elections. But Russia has not stopped there. The 2017 NotPetya malware attack, attributed to Russia, spread around the world and temporarily shut down major international businesses and affected critical infrastructure. Russian-affiliated groups have even gained access via cyberspace to surveil nuclear power plants in the United States.

Iran and North Korea also use cyberspace to attack U.S. and allied interests. Iranian cyber operations have targeted the energy industry, entertainment sector, and financial institutions. Iranian-affiliated threat actors have also targeted dams in the United States with distributed-denial-of-service attacks. North Korea exploits global connectivity to skirt sanctions and sustain an isolated, corrupt regime. According to UN estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year. The 2017 WannaCry ransomware attack, attributed to North Korea, impacted over 300,000 computers in 150 countries, including temporarily disrupting UK hospitals.

Finally, a new class of criminals thrives in this environment. Taking advantage of widespread cyber capabilities revealed by major state intrusions, criminal groups are migrating toward a "crime-as-a-service" model in which threat groups purchase and exchange malicious code on the dark web. In 2019, ransomware incidents grew over 300% compared to 2018 and affected more than 40 U.S. municipalities. More recently, opportunistic hackers have hijacked hospitals and healthcare systems during the COVID-19 pandemic, taking advantage of poorly protected systems in their most vulnerable states. As the world changes to meet the needs of a global pandemic, remote access and the growth in the work-from-home economy continue to increase the threat vectors for criminal actors.

STRATEGIC APPROACH

In the face of this challenge, the Commission understands that to secure America in the 21st century requires securing cyberspace. To accomplish that end, the Commission proposes a new approach: layered cyber deterrence. This strategy combines a number of traditional deterrence mechanisms and extends them beyond the government to develop a whole-of-nation approach. It also updates and strengthens our declaratory policy for cyberattacks both above and below the level of armed attack. The United States must demonstrate its ability to impose costs while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking us in cyberspace.

Since America relies on critical infrastructure that is primarily owned and operated by the private sector, the government cannot defend the nation alone. The public and private sectors, along with key international partners, must collaborate to build national resilience and reshape the cyber ecosystem to increase its security, while imposing costs against malicious actors and preventing attacks of significant consequence.

The Commission acknowledges that, while deterrence is possible in cyberspace, it is not the same as nuclear deterrence. Successful nuclear deterrence was defined as the absence of any use of nuclear weapons. However, in cyberspace, the reality is that no action will stop every operation. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly for malicious actors to benefit from targeting American interests through cyberspace. Therefore, layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries, such as denial and cost imposition, with forms of influence optimized for a connected era, such as promoting norms that encourage restraint and incentivize responsible behavior in cyberspace. Strategic discussions all too often prioritize narrow definitions of deterrence that fail to consider how technology is changing society. In a connected world, those states that harness the power of cooperative, networked relationships gain a position of advantage over other states. However, vulnerabilities that come with this connectivity means that leading states, such as the United States, need to arrive at shared understandings about what constitutes acceptable behavior in cyberspace. It also requires shaping adversary behavior by changing the ecosystem in which competition occurs, not only threatening to impose costs. Finally, it demands international engagement and collaboration with the private sector.

Layered cyber deterrence emphasizes working with the private sector to efficiently coordinate how the nation responds with speed and agility to emerging threats. The federal government alone cannot fund or solve the challenge of adversaries attacking or exploiting the networks on which America and its allies and partners rely. The federal government must collaborate with state and local authorities, leading business sectors, and international partners, within the rule of law. Layered cyber deterrence also addresses the planning needed to ensure continuity of the economy and the ability of the United States to rebound in the aftermath of a major, nationwide cyberattack of significant consequences. Such planning adds depth to deterrence by assuring the American people and our allies, and conveying to our adversaries that the United States has the will and capability to respond to any attack on its interests.

The implementation of layered cyber deterrence is organized around 6 different pillars, each of which focuses on one aspect of the strategy.

THE NEED TO REORGANIZE THE U.S. GOVERNMENT (PILLAR 1)

To defend U.S. interests in cyberspace, key government authorities and processes must be adjusted and aligned. This requires that the Legislative and Executive Branches better align their authorities and capabilities; the public and private sectors improve collaboration in the defense of critical infrastructure and integration in the planning, resourcing, and employment of government cyber resources; and strategic continuity and unity of effort across the U.S. government.

First, Congress must reestablish clear oversight responsibility and authority over cyberspace within the Legislative Branch. The large number of committees and subcommittees claiming some form of jurisdiction over cybersecurity matters is actively impeding action and clarity of oversight. By centralizing responsibility in the new House Permanent Select and Senate Select Committees on Cybersecurity, Congress will be empowered to provide coherent oversight to government strategy and activity in cyberspace.

Next, select entities in the Executive Branch that address cybersecurity must be restructured and streamlined. Multiple departments and agencies have a wide range of responsibilities for securing cyberspace. These responsibilities tend to overlap and at times conflict. Executive Branch departments and agencies tend to compete for resources and authorities, resulting in conflicting efforts that produce diminishing marginal returns. Establishing a Senate confirmed National Cyber Director within the Executive Office of the President would consolidate accountability for harmonizing the Executive Branch's policies, budgets, and responsibilities in cyberspace while implementing strategic guidance from the President and Congress.

In addition to the National Cyber Director, properly resourcing and empowering CISA is critical to achieving coherence in the planning and deployment of government cyber resources. Multiple administrations and Congressional sessions have worked to establish CISA as a keystone of national cybersecurity efforts. However, work remains to be done to realize the Commission's ambitious vision for this critical organization. This includes strengthening CISA's director with a five-year term and elevated executive status, adequately resourcing its programs to engage with

the private sector while managing national risk, and securing sufficient facilities and required authorities for its vital and growing mission. These changes will remove key limitations in CISA's ability to forge a greater public-private partnership and its mission to secure critical infrastructure.

Finally, the U.S. government must more effectively recruit, develop, and retain a cyber workforce capable of building a defensible digital ecosystem and deploying all instruments of national power in cyberspace. This requires designing innovative programs and partnerships to develop the workforce, supporting and expanding current high-performing programs, and connecting with a diverse pool of promising talent. Successfully building a robust federal workforce, in some cases, may depend on stakeholders outside the federal government, such as educators, non-profits, and businesses. Policymakers should support these important partners by providing the tools they need to be effective, such as classroom-ready resources, incentives for research on workforce dynamics, and clear routes for collaborating with the government.

DETERRENCE BY DENIAL (PILLARS 3/4/5)

Denying adversaries the benefits of their cyber campaigns is a critical aspect of layered cyber deterrence. Denial comprises ensuring the resilience of critical pillars of national power, reducing our national vulnerability, and disrupting threats through operationalizing collaboration between the government and private sector. Together, these actions can effectively force adversaries to make difficult decisions regarding resourcing and carrying out malicious cyber operations and campaigns.

Denying benefits to adversaries starts with ensuring that our most critical targets are able to withstand and quickly recover from cyberattacks. In other words, we must build resilience. Effective national resilience efforts fundamentally depend on the ability of the United States to accurately understand, assess, and manage national cyber risk. Current efforts to do so at the national level are relatively new and are significantly hindered by resource limitations, immaturity of processes, and inconsistent capacity across the departments and agencies that participate in national resilience efforts.

Today, under the direction of Presidential Policy Directive 21, sector-specific agencies are the lead federal agencies tasked with day-to-day engagement with the private sector on cybersecurity and resilience. However, there are significant imbalances and inconsistencies in both the capacity and the willingness of these agencies to manage sector-specific risks and participate in government-wide efforts. In addition, the lack of clarity and consistency concerning the responsibilities and requirements for these agencies continues to cause confusion, redundancy, and gaps in resilience efforts. For this reason, the Commission recommends codifying sector-specific agencies in law as "Sector Risk Management Agencies," establishing baseline responsibilities and requirements for managing risk in the sector or sectors under their purview, and appropriating necessary funds to carry out their responsibilities. In addition, the

Commission recommends that Congress recognize, in law, the lead role of the CISA in national risk management.

With more robust risk management capability in the federal government, Congress must also codify the process whereby these agencies come together to provide the federal government with a clearer picture of where we are vulnerable and where we need to place greater resources. The U.S. government has made great strides at understanding national risk through DHS's national critical functions work. However, the U.S. government lacks a rigorous process for identifying, assessing, prioritizing, and ultimately buying down national risk to critical infrastructure. To fill this gap, the Commission recommends that Congress codify a five-year "national risk management cycle" in law to culminate with a "Critical Infrastructure Resilience Strategy" and an accompanying "National Cybersecurity Assistance Fund" to ensure consistent funding for initiatives that underpin or build resilience.

National resilience similarly requires sufficient national capacity and preparedness to respond to and recover from attacks when they do happen. The United States has well-established mechanisms and processes to respond to physical and natural disasters and states of emergency. However, the U.S. government has not yet applied the same rigor to understanding and responding to cyber states of distress and disasters. To address this shortcoming, the Commission recommends Congress pass a law codifying a Cyber State of Distress and an accompanying Cyber Response and Recovery Fund to assist state, local, tribal, and territorial (SLTT) governments and the private sector beyond what is available through conventional government technical assistance and cyber incident response programs.

Similarly, while Continuity of Operations and Continuity of Government have long been cornerstones of government contingency planning, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major disruption. That is why the Commission recommends that Congress direct the Executive Branch to develop and maintain Continuity of the Economy planning to ensure continuous operation of critical functions of the economy in the event of a significant cyber disruption. The planning process should analyze national critical functions, outline priorities for response and recovery, and identify areas for resilience investments. In doing so, the Continuity of the Economy plan should identify areas for preservation of data and mechanisms for extending short-term credit to ensure recovery efforts.

Beyond ensuring resilience, a second major aspect of denying benefits to adversaries lies in reducing our national vulnerability at scale. Today, vulnerabilities in our cyber ecosystem not only derive from technology, but also from human behavior and processes. The Commission sought to improve the security of both the technological and human aspects at scale. Moving the technology markets to emphasize security requires increasing transparency about the security characteristics of consumer technology products. Therefore, the Commission recommends creating a National Cybersecurity Certification and Labeling Authority to develop and facilitate authoritative, easy to understand security certifications and labels for technology products.

Driving down vulnerability in human behavior and processes requires a combination of better empirics to understand what constitutes good cybersecurity behavior and incentives to nudge humans and organizations toward that better behavior. To address the former, the Commission recommends the creation of the Bureau of Cyber Statistics, which will gather relevant data, analyze it, and publish insights for policymakers and the public.

Armed with better information about best practices in cybersecurity, policymakers must find a mixture of incentives to encourage individuals and organizations to adhere to them. Insurance is one such incentive. Although the insurance industry plays an important role in enabling organizations to transfer a small portion of their cyber risk, it is falling short of achieving the public policy objective of driving better practices of risk management in the private sector more generally. Because insurance falls under the purview of state regulators, the federal government can do little to directly affect change in the market for insurance specific to a given industry. Thus, to improve the market for cybersecurity insurance, Congress should appropriate funds and direct DHS to resource a Federally Funded Research and Development Center to develop models for underwriter and claims adjuster training and certification and establish a public-private partnership on modeling cyber risk.

The final aspect of denying adversaries benefits lies in disrupting their operations. Cyber defense, while a shared responsibility, will significantly depend on the underlying efforts of the owners and operators of private networks and infrastructure. The U.S. government and industry thus must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This "collective defense" in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense. Therefore, the Commission recommends codifying the "systemically important critical infrastructure" designation for entities responsible for systems and assets that underpin national critical functions. This will hold these entities to a higher standard and ensure they are fully supported by the U.S. government. Additionally, U.S. government support must be better informed through a Joint Collaborative Environment that would pool public-private sources of threat information to be coordinated through a Joint Cyber Planning Cell and an Integrated Cyber Center at DHS.

DETERRENCE BY SHAPING BEHAVIOR (PILLAR 2)

Layered cyber deterrence includes shaping cyber actors' behavior through strengthening norms of responsible state behavior and employing non-military instruments of power, such as law enforcement, sanctions, diplomatic engagement, and capacity building. A system of norms, based on international engagement and enforced through these instruments of power, helps secure American interests in cyberspace.

To strengthen cyber norms and build a likeminded international coalition to enforce them, the Commission recommends Congress create and adequately resource the Bureau of Cyberspace Security and Emerging Technologies led by an Assistant Secretary of State. The Bureau will bring dedicated cyber leadership and coordination to the Department of State.

Leading internationally also means having strong and coordinated representation in bodies that set global technical standards. Therefore, the Commission recommends that Congress should sufficiently resource the National Institute of Standards and Technology to bolster participation in these bodies. American values, interests, and security are strengthened when international technical standards are developed and set with active U.S. participation. The U.S. must also facilitate robust and integrated participation from across the federal government, academia, civil society, and industry. The U.S. is at its best when we draw input from *all* our experts.

In parallel to robust participation in multilateral bodies, law enforcement activities also provide fruitful ground on which to work with international partners and allies to hold adversaries accountable for malicious behavior. The Commission recommends providing the Department of Justice Office of International Affairs with administrative subpoena authority that streamlines the Mutual Legal Assistance Treaties process. This will enable U.S. law enforcement to better assist allies and partners to prosecute cybercriminals. Additionally, the Commission recommends Congress create and fund 12 additional Federal Bureau of Investigation Cyber Assistant Legal Attachés to facilitate intelligence-sharing and help coordinate joint law enforcement actions. Investing in these types of international law enforcement activities improves the credibility of enforcement and signals America's commitment to bring malicious actors to justice.

DETERRENCE BY COST IMPOSITION (PILLAR 6)

A key element of the Commission's strategy entails imposing costs to deter malicious adversary behavior and reduce ongoing adversary activities short of armed conflict. As part of this effort, the Commission puts forth two key recommendations: to conduct a force structure assessment of the Cyber Mission Force; and to conduct a cybersecurity and vulnerability assessments of conventional weapons systems and of the nuclear command, control, and communications enterprise.

Today, the United States has not created credible and sufficient costs against malicious adversary behavior below the level of armed attack—even as the United States has prevented cyberattacks of significant consequences. Our nation must shift from *responding* to malicious behavior after it has already occurred to *proactively* observing, pursuing, and countering adversary operations. This should include imposing costs to change adversary behavior using all instruments of national power, including the military instrument, in accordance with international law.

To achieve these ends, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives in and through cyberspace. The CMF is currently considered at full operational capability (FOC) with 133 teams comprising a total of approximately 6,200 individuals. However, these requirements were defined in 2013, well before our nation experienced or observed some of the key events that have shaped our government's understanding of the cyber threat. The FOC determination for the CMF was also well before the development of the Department of Defense's (DoD) defend forward strategy. Therefore, the

Commission recommends Congress direct the DoD to conduct a force structure assessment of the CMF to ensure the United States has the appropriate force structure and capabilities in light of growing mission requirements. This should include an assessment of the resource implications for intelligence agencies in their combat support agency roles.

If deterrence fails, the United States must also be confident that its military capabilities will work as intended. However, deterrence across all of the domains of warfare is undermined, and the ability of the U.S. to prevail in crisis and conflict is threatened, if adversaries can hold key military systems and functions, including nuclear systems, at risk through cyber means. Therefore, the Commission recommends Congress direct the DoD to conduct a cybersecurity vulnerability assessment of all segments of nuclear command, control, and communications systems and continually assess weapon systems' cyber vulnerabilities.

Our hope is that, by implementing these recommendations, we can ensure our nation is willing and able to counter and reduce malicious adversary behavior below the level of armed conflict, impose costs to deter significant cyberattacks, and, if necessary, fight and win in crisis and conflict.

CONCLUSION

The recommendations put forward by the Commission represent important first steps toward reducing adversaries' ability and willingness to exploit cyberspace to undermine American interests and values. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. Cyber operations have become a weapon of choice for adversaries seeking to hold the U.S. economy and national security at risk. Near-peer adversaries such as China and Russia are attempting to reassert their influence regionally and globally, using cyber and information operations to undermine American security interests. The concept of deterrence must evolve to address this new strategic landscape. Reducing the scope and severity of these adversary cyber operations and campaigns requires adopting the Commission's strategy of layered cyber deterrence.

Senate Homeland Security & Governmental Affairs Committee
Hearing, May 13, 2020, Statement for the Record

Evolving the U.S. Cybersecurity Strategy and Posture:
Reviewing the Cyberspace Solarium Commission Report

The College of Healthcare Information Management Executives (CHIME) is pleased to offer a statement for the record. We applaud the Senate Homeland Security & Government Affairs Committee for tackling the tough issue of cybersecurity, the seemingly invisible threat to our nation and its sixteen critical infrastructures, in your hearing on May 13, 2020, *Evolving the U.S. Cybersecurity Strategy and Posture: Reviewing the Cyberspace Solarium Commission Report.*

Healthcare is deemed a critical infrastructure by the Department of Homeland Security (DHS) and as such, patient safety and patient data should be viewed as a public good; protecting those things should be a national priority. Cybersecurity attacks are highly disruptive and can be crippling to healthcare entities, as illustrated by the WannaCry and Petya ransomware attacks in 2017 which affected 34 percent of the United Kingdom's health trusts and several still unnamed healthcare providers in the U.S. While the cybersecurity posture of the sector has improved over the past few years, much work remains, especially in light of the challenges to our sector posed by the COVID-19 pandemic.

In addition to the patient safety implications, there is a heavy toll in terms of costs to the healthcare system. This is because healthcare data is considered more lucrative than data from other industries; it can fetch upwards of ten times more money than a patient's financial data (source: PhishLabs). Consequently, the healthcare sector can be prone to more attacks. In fact, our sector is attacked twice as frequently as other sectors (source: FortiGuard) and the average healthcare data breach costs $6.45 million (source: Ponemon Institute's 2019 Cost of a Data Breach Report). This is 65% higher than the average total cost of a data breach. Providers with limited resources struggle to balance the huge demands for cybersecurity technology and information risk management programs.

The global COVID-19 pandemic has created a new urgency to guard against cyber threats in the healthcare sector. Bad actors are attempting to capitalize on the pandemic for nefarious gain. These threats have been recently highlighted by federal authorities. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a joint Public Service Announcement on May 13 concerning China's targeting of COVID-19 research organizations. And, the CISA and the UK's National Cyber Security Centre (NCSC) issued a joint alert on May 5 warning that advanced persistent threat (APT) groups are actively targeting organizations involved in both national and international COVID-19 responses.

College of Healthcare Information Management Executives (CHIME)
710 Avis Drive, Suite 200 | Ann Arbor, MI 48108 | 734.665.0000 | www.chimecentral.org

These types of threats have contributed to a significant uptick in cyber activity in the healthcare sector. Since January there has been a 30,000 percent increase in cyberattacks aimed at remote users related to COVID-19 (source: Zscaler). Alarmingly, experts are warning that we have not seen the worst of it. The barrage of cyberattacks lodged against healthcare providers was already escalating in both volume and sophistication prior to COVID-19. The increased activity will only exacerbate existing threats to patient safety and our national security. We are aware of three hospitals that have experienced a cyberattack during COVID-19, however, there are likely many more.

As the healthcare sector has grown increasingly interconnected with a burgeoning internet of things (IoT), and more recently a spike in demand for virtual care spurred by COVID-19, the need to fortify the healthcare sector has never been more urgent. The pandemic has also required healthcare providers to repurpose staff, pulling them away from vital security operations, and many providers are experiencing layoffs and furloughs. While providers' workforce may be shrinking, the old adage "criminals never sleep" rings increasingly true.

Our members continue to worry about the threats to patient care and safety that cybersecurity attacks pose. New innovations, techniques and capabilities have been introduced to improve health outcomes, but they also may introduce additional risk. With this evolution, the role of the clinician is also changing; they are becoming more reliant on availability of key critical information at the moment of care. Of particular concern, 70 percent of attacks on healthcare facilities are directed at facilities with fewer than 500 employees that are more likely to pay to prevent disruption to patient care (source: RiskIQ).

Taking into account these additional alarming statistics, this becomes a matter of when not if our healthcare system will sustain a crippling attack. Many hospitals are under-resourced, and some do not even have a single full-time employee devoted to oversight of cybersecurity. On top of insufficient staff, one of the biggest issues in helping fend off cyberattacks is having access to good cyber intelligence, which can be costly. And, several rural providers already teetering on thin financial margins prior to the pandemic are on the brink of financial collapse barely able to support patient care let alone fend off a cyberattack. With the health sector only as strong as its weakest link, it is imperative to assist the smaller and lesser resourced providers.

Ensuring cybersecurity threats and the recognition of their potential to disrupt healthcare delivery should be a national priority. Had the pandemic occurred in 2017 during the WannaCry and Petya attacks, this could have crippled our ability to fight COVID. We agree with recommendation 5.1 which says, in part, "In defining the critical functions by which to designate systemically important critical infrastructure, the U.S. government should focus on national critical functions that...Support or underpin public health and safety or are so foundational that their disruption could endanger human life on a massive scale." While the *Solarium Report* contains a few mentions of the impact of cyber on the healthcare sector, we urge the committee to make threats to the healthcare system a national priority.

CHIME stands ready to serve as a resource to the Committee. Our members have deep experience fending off cyberattacks and a strong command of the threats facing our sector. We appreciate the opportunity to share our perspective with the Committee on this important issue.

College of Healthcare Information Management Executives (CHIME)
710 Avis Drive, Suite 200 | Ann Arbor, MI 48108 | 734.665.0000 | www.chimecentral.org