HOMELAND CYBERSECURITY: ASSESSING CYBER THREATS AND BUILDING RESILIENCE

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

FEBRUARY 10, 2021

Serial No. 117–2

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE
44–379 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

Bennie G. Thompson, Mississippi, *Chairman*

Sheila Jackson Lee, Texas
James R. Langevin, Rhode Island
Donald M. Payne, Jr., New Jersey
J. Luis Correa, California
Elissa Slotkin, Michigan
Emanuel Cleaver, Missouri
Al Green, Texas
Yvette D. Clarke, New York
Eric Swalwell, California
Dina Titus, Nevada
Bonnie Watson Coleman, New Jersey
Kathleen M. Rice, New York
Val Butler Demings, Florida
Nanette Diaz Barragán, California
Josh Gottheimer, New Jersey
Elaine G. Luria, Virginia
Tom Malinowski, New Jersey
Ritchie Torres, New York

John Katko, New York
Michael T. McCaul, Texas
Clay Higgins, Louisiana
Michael Guest, Mississippi
Dan Bishop, North Carolina
Jefferson Van Drew, New Jersey
Ralph Norman, South Carolina
Mariannette Miller-Meeks, Iowa
Diana Harshbarger, Tennessee
Andrew S. Clyde, Georgia
Carlos A. Gimenez, Florida
Jake LaTurner, Kansas
Peter Meijer, Michigan
Kat Cammack, Florida
August Pfluger, Texas
Andrew R. Garbarino, New York

Hope Goins, *Staff Director*
Daniel Kroese, *Minority Staff Director*
Natalie Nixon, *Clerk*

CONTENTS

Page

STATEMENTS

WITNESSES

APPENDIX

HOMELAND CYBERSECURITY: ASSESSING CYBER THREATS AND BUILDING RESILIENCE

Wednesday, February 10, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
Washington, DC.

The committee met, pursuant to notice, at 2:07 p.m., via Webex, Hon. Bennie G. Thompson (Chairman of the committee) presiding.

Present: Representatives Thompson, Jackson Lee, Langevin, Payne, Correa, Slotkin, Cleaver, Green, Clarke, Titus, Watson Coleman, Rice, Demings, Barragán, Gottheimer, Luria, Malinowski, Torres, Katko, Higgins, Guest, Bishop, Van Drew, Miller-Meeks, Clyde, LaTurner, Meijer, Cammack, Pfluger, Garbarino.

Chairman THOMPSON. The Committee on Homeland Security will come to order.

The committee is meeting today to receive testimony on "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience."

Without objection, the Chair is authorized to declare the committee in recess at any point. The gentlelady from New York, Ms. Clarke, shall assume the duties of the Chair in the event that I run into technical difficulty.

Good afternoon. We are here today to begin what I hope will be a bipartisan endeavor in the 117th Congress, making cyber space more secure and networks more resilient.

During the Trump administration, Federal efforts to raise the National cybersecurity posture were stunted by a lack of steady, constant leadership from the White House. In contrast, from Day 1, President Biden has treated cybersecurity as an urgent National and economic security issue.

The President has started by surrounding himself with experts to spearhead sound cybersecurity policy. He has already confronted Vladimir Putin about Russian election meddling and the SolarWinds compromise and has publicly committed to an aggressive stance on China. Further, to bolster cybersecurity of Federal networks, the President included much-needed funding for cybersecurity and technology modernization in the American Rescue Plan proposal.

Thankfully, Congress now has a willing and able cybersecurity partner in the White House, and I am optimistic about the progress we can make. We must work quickly to make up for lost time.

Our witnesses today are a seasoned group of cyber experts, many of whom recently served in Government and made important contributions to our National cyber space posture. They are here to tell us about the challenges we face and how to chart a course toward cyber defense, deterrence, and resiliency.

In the not-too-distant past, when our witnesses were serving in Government, most of us had never heard of SolarWinds, but now it dominates cybersecurity conversation. Late last year, we learned that Russian actors breached targeted Federal networks and critical infrastructure, in part through a sophisticated supply chain compromise of the SolarWinds Orion platform. For almost a year, Russian actors burrowed into networks, hiding their tracks and patiently stealing data.

Although we are engaged in an in-depth investigation with other key House committees to learn more about this malicious Russian campaign, we know enough to begin asking difficult questions and start correcting course.

For instance, we know that it will take months to fully understand the scope and impact of the compromise and eradicate bad actors from our network. We also know that, despite prior significant investment in Federal network security and active defense, the Russian campaign evaded detection.

The task before us is to zero in on how we can mature our defenses to match the capabilities of our adversaries. The Russian SolarWinds campaign threatens our Nation and cannot be tolerated.

It is evident that prior responses to cyber attack, such as naming and shaming, sanctions and indictments, have not deterred bad actors from engaging in malicious cyber behavior that threatens our National security. I am interested in hearing from our witnesses how we can deter this behavior or raise the cost of it.

We must also be mindful that not every cyber attack is a sophisticated one carried out by a well-resourced nation-state actor. Cyber criminals ranging in sophistication continues to wreak havoc on State and local governments and private-sector critical infrastructure with less mature cybersecurity capabilities.

Just this week, for example, a hacker breached a water treatment facility in Florida and attempted to poison the water supply. This follows a year when cyber criminals hacked schools, hospitals, and workplaces transitioning to remote work. According to McAfee, cyber crime cost the global economy $1 trillion in 2020.

The Federal Government must work to raise the baseline cybersecurity posture across Government entities and the private sector to reduce avoidable, opportunistic attacks. This will free up talent and resources to focus on more sophisticated problems. We must also do as President Biden has done and treat cybersecurity as a central National security priority and not a boutique add-on.

To be sure, today is just the first of several hearings this committee will hold on the cybersecurity threats facing the Nation and how the Government and private sector should work together to address them.

I would like to thank our witnesses for their testimony and look forward to continuing the committee's work on this critical issue.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

FEBRUARY 10, 2021

We are here today to begin what I hope will be a bipartisan endeavor in the 117th Congress—making cyber space more secure and networks more resilient. During the Trump administration, Federal efforts to raise the National cybersecurity posture were stunted by a lack of steady, consistent leadership from the White House. In contrast, from Day 1, President Biden has treated cybersecurity as an urgent National and economic security issue.

The President has started by surrounding himself with experts to spearhead sound cybersecurity policy. He has already confronted Vladimir Putin about Russian election meddling and the SolarWinds compromise and has publicly committed to an aggressive stance on China. Further, to bolster the cybersecurity of Federal networks, the President included much-needed funding for cybersecurity and technology modernization in the American Rescue Plan proposal. Thankfully, Congress now has a willing and able cybersecurity partner in the White House, and I am optimistic about the progress we can make. We must work quickly to make up for lost time.

Our witnesses today are a seasoned group of cybersecurity experts, many of whom recently served in Government and made important contributions to our National cybersecurity posture. They are here to tell us about the challenges we face and how to chart a course toward cyber defense, deterrence, and resiliency. In the not-too-distant past, when our witnesses were serving in Government—most of us had never heard of SolarWinds, but now it dominates cybersecurity conversations.

Late last year, we learned that Russian actors breached targeted Federal networks and critical infrastructure, in part through sophisticated supply chain compromise of the SolarWinds Orion platform.

For almost a year, Russian actors burrowed into networks, hiding their tracks and patiently stealing data. Although we are engaged in an in-depth investigation with other key House Committees to learn more about this malicious Russian campaign, we know enough to begin asking difficult questions and start correcting course.

For instance, we know that it will take months to fully understand the scope and impact of the compromise and eradicate bad actors from our networks. We also know that despite prior significant investments in Federal network security and active defense, the Russian campaign evaded detection. The task before us is to zero in on how can we mature our defenses to match the capabilities of our adversaries. The Russian SolarWinds campaign threatens our Nation and cannot be tolerated.

It is evident that prior responses to cyber attacks such as "naming and shaming," sanctions, and indictments have not deterred bad actors from engaging in malicious cyber behavior that threatens our National security. I am interested in hearing from the witnesses how can we deter this behavior or raise the cost of it. We must also be mindful that not every cyber attack is a sophisticated one carried out by a well-resourced nation-state actor.

Cyber criminals—ranging in sophistication—continue to wreak havoc on State and local governments and private-sector critical infrastructure with less mature cybersecurity capabilities. Just this week, for example, a hacker breached a water treatment facility in Florida and attempted to poison the water supply. This follows a year when cyber criminals hacked schools, hospitals, and workplaces transitioning to remote work. According to McAfee, cyber crime cost the global economy $1 trillion in 2020.

The Federal Government must work to raise the baseline cybersecurity posture across Government entities and the private sector to reduce avoidable, opportunistic attacks. This will free up talent and resources to focus on more sophisticated problems. We must also do as President Biden has done and treat cybersecurity as a central National security priority and not a "boutique add-on."

To be sure, today is just the first of several hearings this committee will hold on the cybersecurity threats facing the Nation and how the Government and private sector should work together to address them.

Chairman THOMPSON. With that, I recognize the Ranking Member, the gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Mr. Chairman. I appreciate your comments. Thank everyone for being here today, including the witnesses. Thank you for holding this important hearing.

As you know, cybersecurity remains an area of great bipartisan cooperation in Congress, and for that we should be thankful. Because of it, it is also the preeminent National and homeland security threat of our time.

Every action we have heard about the importance of cybersecurity is more true than ever before. It underpins almost every aspect of our way of life. It impacts resilience of every single critical infrastructure sector, and it stands between our most sensitive data being secure or being exploited by our enemies.

While general awareness of cyber threats is becoming commonplace, the cybersecurity resilience of our great Nation leaves undeniable room for improvement. We are still living in the wake of the SolarWinds campaign, one of the most devastating cyber-espionage campaigns in history, with our State and local governments, businesses, and constituents being affected by malicious cyber campaigns every single day.

Think about it: The past year, while we were indicting our operatives of the Chinese Ministry of State Security for actively trying to compromise COVID vaccine research, Russian actors were simultaneously sitting in Federal and non-Federal networks, quietly executing what is arguably the most sophisticated cyber-espionage campaign in our Nation's history.

Both of those state-backed campaigns that were taking place via a weekly and often daily drumbeat of ransomware campaigns crippled city, State, hospital, and school networks already heavily impacted by the pandemic.

In my district alone, the Syracuse City School District and Onondaga County Library System both fell victim to ransomware attacks that shut down their systems and halted the critical services they provide. Just days ago, a hacker reportedly gained access to a water treatment facility in Oldsmar, Florida, and attempted to adjust the water chemical levels through cyber means to poison thousands of residents.

These cyber threats clearly have real-world consequences, and we must do everything we can to help bring these malicious actors to justice. The bottom line is that we are still struggling against both the highly sophisticated and the routine. We can do better, and we must do better.

There is, luckily, some reason for optimism. The creation of CISA as the Nation's lead civilian cybersecurity agency was necessary and long overdue. The agency's work to harden election systems from 2016 to 2020 was nothing short of heroic. Like everyone in this hearing, I extend my heartfelt gratitude to Chris Krebs and his team for his service and leadership.

The Cyberspace Solarium Commission created a venue for activists to voice bold ideas and a mechanism for those ideas to become law. I am very proud to have helped usher multiple new authorities for CISA as part of the fiscal year 2021 NDAA, which will bolster its visibility across Federal networks, among other important authorities.

CISA should be doubling down on its implementation of these provisions, most importantly the authority to conduct threat hunting on agencies' networks. But the work does not stop there, not by a long shot. It is easy to sit here and become numb to what often feels like a "breach of the week" in cyber space.

Complicating this landscape further is that cybersecurity risk management, supply chain risk management, third-party trust and assurance, and critical infrastructure protection are now inexorably linked. They are layers on top of one another, impossible to disaggregate.

The sheer volume of the data that our connected systems must secure in transit and at rest is increasing exponentially, a reality only accelerated by the deployment of the 5G networks Nationwide.

Meanwhile, our nation-state cyber adversaries, like China, have sophisticated, multi-decade agendas to compromise data and leverage it for malicious purposes aimed at eroding America's dominance.

We have a distinguished panel of witnesses who have all spent considerable time in the trenches working valiantly to keep America safe from cyber threats, and I welcome their guidance on how we can strengthen our Nation's cybersecurity posture.

I want this to be a hearing about opportunity for action, not just admiration of the problem. We have already ceded critical ground to our global adversaries, and there is simply no time to waste.

I remain deeply concerned that the Federal roles and responsibilities for dot-gov security are too confederated, too clunky, and ultimately inadequate. Giving CISA Federal hunt authorities was an incremental step in the right direction, but CISA simply does not have the centralized visibility or authority to nimbly respond. I look forward to hearing ideas from our witnesses about how we can remedy this situation.

On the heels of SolarWinds, and with enough not-insignificant potential the Russian actors may still have access to some of our networks, I call on all my colleagues to work together in a bipartisan manner quickly to find a legislative vehicle to give CISA the resources it needs to fully respond and protect us.

Cybersecurity is a team sport that is ultimately about partnership. We are all in this together, so let's get to work.

I yield back, Mr. Chairman.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

FEBRUARY 10, 2021

Thank you, Mr. Chairman.

Thank you for holding this important hearing. As you know, cybersecurity remains an area of great bipartisan cooperation in Congress.

For that, we should be thankful, because it is also the pre-eminent National and homeland security threat of our time.

Every axiom we've heard about the importance of cybersecurity is more true than ever before. It underpins almost every aspect of our way of life, it impacts the resilience of every single Critical Infrastructure sector, and it stands between our most sensitive data being secure—or being exploited—by our enemies.

While general awareness of cyber threats is becoming commonplace, the cybersecurity resilience of our great Nation leaves undeniable room for improvement.

We're still living in the wake of the SolarWinds campaign—one of the most devasting cyber espionage campaigns in history, with our State and local governments, businesses, and constituents being affected by malicious cyber campaigns every single day.

Think about it, this past year, while we were indicting operatives of the Chinese Ministry of State Security for actively trying to compromise COVID vaccine research, Russian actors were simultaneously sitting in Federal, and non-Federal networks, quietly executing what is arguably the most sophisticated cyber espionage campaign in history.

Both of those State-backed campaigns were taking place while a weekly, and often daily, drumbeat of ransomware campaigns crippled city, State, hospital, and school networks already heavily impacted by the pandemic. In my district, the Syracuse City School District and Onondaga County library system both fell victim to ransomware attacks that shut down their systems and halted the critical services they provide.

Just days ago, a hacker reportedly gained access to a water treatment facility in Oldsmar, Florida, and attempted to adjust the water chemical levels through cyber means to poison thousands of residents.

These cyber threats clearly have real-world consequences, and we must do everything we can to bring these malicious actors to justice.

The bottom line is that we are still struggling against both the highly sophisticated and the routine.

We can do better. We must do better.

There is, luckily, some reason for optimism.

The creation of CISA as the Nation's lead civilian cybersecurity agency was necessary and long overdue. The agency's work to harden election systems from the 2016 to 2020 elections was nothing short of heroic. Like everyone in this room, I extend my heartfelt gratitude to Chris Krebs for his service and leadership.

The Cyberspace Solarium Commission created a venue for experts to voice bold ideas, and a mechanism for those ideas to become law. I am proud to have helped usher multiple new authorities for CISA as a part of the fiscal year NDAA, which will bolster its visibility across Federal networks, among other important authorities.

CISA should be doubling down on its implementation of these provisions, most importantly, the authority to conduct threat hunting on agencies' networks.

But the work doesn't stop there.

It's easy to sit here and become numb to what often feels like a "breach of the week" in cyber space. Complicating this landscape further is that cybersecurity risk management, supply chain risk management, third-party trust and assurance, and critical infrastructure protection are now inexorably linked. They are layers on top of one another, impossible to disaggregate.

The sheer volume of the data that our connected systems must secure in transit and at rest is increasing exponentially—a reality only accelerated by the deployment of 5G networks.

Meanwhile, our nation-state cyber adversaries, like China, have sophisticated, multi-decade agendas to compromise this data and leverage it for malicious purposes aimed at eroding America's dominance.

We have a distinguished panel of witnesses who have all spent considerable time in the trenches working valiantly to keep America safe from cyber threats and I welcome their guidance on how we can strengthen our Nation's cybersecurity posture.

I want this to be a hearing about opportunity for action, not just admiration of the problem. We have already ceded critical ground to our global cyber adversaries, and there is simply no time to waste.

I remain deeply concerned that the Federal roles and responsibilities for .gov security are too confederated, too clunky, and ultimately inadequate. Giving CISA Federal hunt authorities was an incremental step in the right direction, but CISA simply does not have the centralized visibility or authority to nimbly respond. I look forward to hearing ideas from our witnesses about how we can remedy this situation.

On the heels of SolarWinds, and with the not insignificant potential that Russian actors may still have access to some of our networks, I call on all my colleagues to work together, quickly, to find a legislative vehicle to give CISA the resources it needs to fully respond.

Cybersecurity is a team sport that is ultimately about partnership. We're all in this together, so let's get to work.

Chairman THOMPSON. Other Members of the committee are reminded that, under the committee rules, opening statements may be submitted for the record.

[The statement of Honorable Garbarino follows:]

STATEMENT OF HONORABLE ANDREW R. GARBARINO

FEBRUARY 10, 2021

I am honored to have been selected by Ranking Member Katko to serve as the Ranking Member of the Cybersecurity, Infrastructure Protection, and Innovation (CIPI) Subcommittee. I believe that cyber attacks are the most pressing threat to our National security today. Nation-state actors are growing more sophisticated and increasingly infiltrating our networks and stealing National security secrets, personal data, and intellectual property. I am eager to get to work to defend our Nation's most critical infrastructure from foreign adversaries like Russia, China, Iran, and North Korea.

As the lead Federal agency tasked with helping stakeholders understand and manage risk across all 16 critical infrastructure sectors, the Cybersecurity and Infrastructure Security Agency (CISA) plays a key role in ensuring every aspect of our society is resilient to cyber threats. As such, CISA must operate as a strong, centralized authority to ensure the cyber resilience of all the lifeline services that Americans so heavily rely on—including the Nation's electric grid, telecommunications systems, health care institutions, and water facilities. In fact, just today it was reported that a water utility in Florida was the victim of a cyber attack that put the clean water supply of 15,000 Americans in jeopardy.[1] We must do better to ensure underfunded and under-resourced utilities in every critical infrastructure sector have the security protections in place to provide reliable services to Americans.

As my constituents on Long Island and all Americans across the country continue to adapt to working and learning remotely as a result of the COVID–19 pandemic, I believe it is now more important than ever to work with agencies like CISA combat malicious cyber actors from targeting COVID–19 relief programs for our struggling small businesses, as well nation-state actors such as China targeting pharmaceutical institutions involved in vaccine development. We must keep Chinese-owned technology and telecommunications companies, like Huawei, out of our data, infrastructure, and networks across all critical infrastructure sectors. I will be tough on all companies influenced by the Chinese Communist Party, as well as any other nefarious nation-state actors.

The recent SolarWinds cyber espionage campaign launched by a sophisticated nation-state actor, likely Russia, is one of the worst intrusions of U.S. Government and private-sector networks in our Nation's history. We will be dealing with the impacts of this campaign for years to come. We must move forward by centralizing Federal network authority under CISA, understanding the current risk landscape, and holding cyber adversaries accountable. I look forward to continuing to address these complex issues with Ranking Member Katko and the CIPI subcommittee in the months ahead.

As we begin the 117th Congress, I strive to improve our Nation's cybersecurity posture at every level of government, including preventing ransomware attacks at the State and local level. Throughout 2020, ransomware attacks increased significantly and targeted many health care organizations and schools that were already overwhelmed by the COVID–19 pandemic. In fact, just a few months ago, both the Bay Shore and Lindenhurst school districts on Long Island were hit with cyber attacks.[2] I am determined to work with hospitals, schools, and small businesses in New York's 2d district and across the country to improve their cybersecurity posture in the wake of increasing threats.

I am ready to get to work with the Nation's leading cybersecurity experts from both the public and private sectors and I look forward to engaging with all these stakeholders in my new role on the subcommittee. I look forward to combating this threat as one Nation and finding bipartisan and innovative ways to protect our communities moving forward.

Chairman THOMPSON. Members are also reminded that the committee will operate according to the guidelines laid out by the Chairman and Ranking Member in our February 3 colloquy regarding remote proceedings.

I welcome our witnesses.

[1] Hack exposes vulnerability of cash-strapped U.S. water plants: *https://apnews.com/article/water-utilities-florida-coronavirus-pandemic-utilities-882ad1f6e9f80c053ef5f88a23b840f4*.

[2] Cyber attack disrupts operations in Bay Shore school district: *https://www.newsday.com/long-island/education/bay-shore-schools-hack-1.50010940*.

Mr. Chris Krebs, who is no stranger to this committee, served as the director of the Cybersecurity and Infrastructure Security Agency, commonly referred to as CISA, until November 2020. Since leaving Government, he has founded the Krebs Stamos Group, and he is now serving as Newmark senior cyber fellow at the Aspen Institute. SolarWinds is one of Mr. Krebs' clients; however, he is testifying today in his personal capacity as a former CISA director.

Ms. Sue Gordon served as the principal deputy director of national intelligence at the Office of the Director of National Intelligence from August 2017 to August 2019. Ms. Gordon has served in the intelligence community for over 3 decades in a variety of leadership roles spanning numerous intelligence organizations and disciplines.

Mr. Michael Daniel is the president and CEO of Cyber Threat Alliance. Prior to joining CTA in February 2017, Michael served from June 2012 to January 2017 as special assistant to President Obama and cybersecurity coordinator on the National Security Council staff.

Mr. Dmitri Alperovitch is executive chairman of Silverado Policy Accelerator, a nonprofit focusing on advancing solutions to critical geopolitical and cybersecurity policy challenges. He is cofounder and former chief technology officer of the cybersecurity firm CrowdStrike, Incorporated.

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

I now ask Mr. Krebs to summarize his statement for 5 minutes.

STATEMENT OF CHRISTOPHER C. KREBS, FORMER DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairman Thompson, Ranking Member Katko, Members of the committee, good afternoon, and thank you for inviting me to appear today.

As the director of the Cybersecurity and Infrastructure Security Agency, or CISA, leading CISA, I had the pleasure to work with many of you as Members of the primary oversight committee, and I have testified, as you pointed out, many times in front of this committee.

To the new Members of the committee, congratulations on being given the honor to represent your constituents in the 117th Congress.

I look forward to helping as I might, and thank you for holding this timely hearing.

The cyber threat landscape is more complicated than ever, with foreign governments and criminal gangs alike using capabilities that enable everything from run-of-the-mill cyber crime, information operations, intellectual property theft, destructive attacks, and operations with kinetic effects.

The bulk of the malicious cyber activity targeting the United States emanates from 4 countries: Russia, China, Iran, and North Korea. Even in those countries, the difference between State action and criminal activity is increasingly blurred as contracted or proxy cyber actors support or act on behalf of State-directed operations. As long as the tools are available, vulnerabilities exist, money and secrets are to be had, and a lack of meaningful consequences persist, there will be malicious cyber actors.

Complicating matters further, oftentimes we make it far too easy for the bad guys. When an organization is struggling to make payroll and keep systems on a generation of technology created in the last decade, even the basics of cybersecurity can be out of reach.

Even then, the purpose of IT is to make things easier to manage. So it is almost counterintuitive that managing a system over the internet might be a bad thing.

So we have a dilemma on our hands. But all is not lost. In my written testimony, I provide a series of recommendations that can put us on a collective path toward a more secure and resilient economy. Are we going to stop every attack? No. But we can take care of the most common risks and make the bad guys work that much harder and limit their success.

To get there, we must make 3 strategic shifts.

First, we need stronger cybersecurity leadership in industry and more centralized oversight in Government. This includes building on the authorities provided to CISA in the National Defense Authorization Act, including the administrative subpoena authority and continuous hunt over Federal civilian agencies.

Second, we must allocate more and smarter investments into private-sector capabilities and increase support to all levels of Government. This includes accelerating investment into Federal IT modernization, boosting CISA's ability to execute, and providing grant programs for State and local governments like the post-9/11 antiterrorism programs.

Third, industry and Government must come together collectively to democratize cybersecurity, better understand where our real risk lies, increase capacity, and work in a meaningful way beyond information sharing. This includes coming together to counter the scourge of ransomware.

The parts are in place for our Nation to dramatically improve our cybersecurity defenses. As a society, we need to accept that every organization in the country, whether in the private sector or in Government, can be targeted by a cyber actor. The Government cannot stop all attacks, but there is much that the industry can do on their end. Companies have a responsibility to their customers, their stakeholders, and, depending on where they sit in the economy, a responsibility to the country.

Meaningful progress will take time, and we may never see a finish line, but change for the better is possible. To get there, we need to employ the courage and resolve that has driven American innovation throughout our National history.

Before I conclude, I would once again like to thank the committee for your steadfast support of CISA in its cybersecurity mission. You deserve great credit for the agency's progress in the last few years. I firmly believe that we are on the right track and can accomplish much more together.

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

[The prepared statement of Mr. Krebs follows:]

PREPARED STATEMENT OF CHRISTOPHER C. KREBS

FEBRUARY 10, 2021

INTRODUCTION

Chairman Thompson, Ranking Member Katko, Members of the committee, my name is Chris Krebs, and it is my pleasure to appear before you today to discuss "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience." As you know, I previously served as the first director of the Cybersecurity and Infrastructure Security Agency (CISA), leading CISA and its predecessor organization, the National Protection and Programs Directorate, from August 2017 until November 2020. Over the last several years, I have had the pleasure of working with many of you as Members of the primary oversight committee for CISA and have testified in front of this committee many times. To the new Members of the committee, congratulations on being given the honor to represent your constituents in the 117th Congress. I look forward to working with you.

It is an honor to appear before this committee to testify about the current cybersecurity threat landscape and how it intersects with American businesses and Government agencies. Given my recent experience as CISA director, and now as founding partner of the Krebs Stamos Group, a cybersecurity risk management consultancy, as well as the Newmark senior cyber fellow at the Aspen Institute, I am continuing my efforts to improve the Nation's cybersecurity and resilience. My time at CISA most acutely helped shape my view of the effectiveness of our current approach and its shortcomings, particularly with a focus on critical infrastructure. Operating from an assumption that our adversaries are technically capable, both opportunistic and highly targeted, yet bound by the laws of physics and the realities of the Gregorian calendar, I firmly believe that we can make progress in defending our cybersecurity.

In order to make progress, I believe there are several truisms that are useful to framing an organization's approach to cybersecurity and resilience: First, the Federal Government is not going to save you, but they are an essential partner. Second, cybersecurity competency requires leadership buy-in. Third, good guys and bad guys alike make mistakes, how fast you find both makes a difference. Fourth, your mistakes are likely going to get out anyway, the faster you protect your customers, the better off everyone will be. And fifth, everyone has bad days, preparation will determine how bad that day is. These truisms represent a simple acknowledgement that 100 percent security is not the desired or realistic end-state, instead a resilient organization that is empowered, informed, humble, and agile cannot just survive in today's environment, but actually thrive.

In my testimony today, I will provide a series of recommendations to improve our approach to making the internet a safer and more secure place for all Americans. These recommendations are rooted in the need to continually improve our understanding of our Nation's physical and digital infrastructure, introduce friction into the adversaries' activities, and increase investments and centralized services for Government and industry alike. My recommendations align with the more defensive actions associated with "Deterrence by Denial."

(1) Continue to invest in CISA's National Critical Functions (NCFs) Initiative, improve our understanding of the risk facing our Nation's infrastructure, and expand roll out to highest-risk functions.

(2) Prioritize identification of systemically important enterprise software and services, update Federal contracting for greater transparency and sharing, and launch operational defensive partnerships called for in the 2021 National Defense Authorization Act.

(3) Launch a National countering ransomware initiative to improve defenses, disrupt the ransomware business model, and use broader set of authorities against actors.

(4) Proceed with Department of Commerce rulemaking on Executive Order 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities" to counter adversary abuse of Virtual Private Servers.

(5) Improve Federal cybersecurity posture through enhanced governance, increased funding, and centralized services offered by CISA.

UNDERSTANDING CYBER RISK

When thinking about the cybersecurity risks we face today, I find the traditional risk formula most useful to organize the various players on the field: $r=t*v*c$.

Where r = risk, t = threat, v = vulnerability, and c = consequence. Likelihood of an attack is assumed within the t variable.

Those 3 variables combined yield the risk we are constantly trying to manage. The 3 variables, however, are not static nor are they singular, and therefore a risk manager's job is never done. The cyber implications of COVID–19 are a useful case study. In the spring of 2020, our Nation's critical infrastructure risk shifted dramatically. The coronavirus spread across the country sickening many Americans and overwhelming hospitals, particularly in New York City. The consequences of a threat—non-state actor ransomware—hitting a hospital would lead to loss of life due to reduced capacity in patient care. To manage the risk in the calculation, through CISA's "Project Taken" we engaged to both minimize vulnerabilities in patient care facilities, but also by messaging threat actors to avoid attacking those facilities. There were also state actor threats from China and Russia conducting espionage on vaccine manufacturing research labs. Those intrusions, exploiting vulnerabilities in the networks and systems of the labs, if conducted recklessly, could result in disruptive consequences to vaccine development, where days and weeks delay in vaccine roll out meant real lives lost. In part, through Operation Warp Speed, CISA worked with vaccine developers to minimize vulnerabilities by sharing threat intelligence, investigate suspicious activity, and scanning for unpatched systems. We also worked to better understand supply chains and manage consequences by identifying and diversifying or hardening single points of failure in the chain from research and development to shots in the arm.

Both real-life scenarios offer just a glimpse into the challenges facing information security teams and risk managers in general across the country. They also highlight the focus cannot solely be on understanding and stopping the threat actors—we must also invest in our ability to understand why we might be targeted by threat actors, how they might come at us, and if they do, how do we survive or minimize any attack.

THE T(HREAT) VARIABLE

The cyber threat landscape is more complicated than ever, with state and non-state actors investing in and building capabilities that enable everything from run-of-the-mill cyber crime, information operations, destructive attacks, and operations with kinetic affects. Over the last few years, the "state actor cyber club" has evolved from the traditional big 4 of cyber adversaries—China, Russia, Iran, and North Korea—to a more stratified set of actors. The sorting is based on capability, with China and Russia at the top of the pyramid, and Iran and North Korea, while still capable, a rung below. Non-state actors including cyber criminals are also gaining ground.

Further complicating the ability to paint a clear picture of the cyber threat actor landscape is the increasingly blurring line between state and non-state actors. For example, contracted or proxy cyber actors support or act on behalf of state-directed operations. Conversely, state actors sometimes moonlight as cyber criminals after-hours to earn additional income. And in other cases, non-state cyber actors operate with the tacit approval of the home state, if the actors do not target their own domestic organizations, in other words "anyone but us." New actors enter and leave the playing field daily. Agencies reorganize, break up, and consolidate. Criminal gangs are busted, go dark, or give up the life of crime. If the tools are available, money and secrets are to be had, vulnerabilities exist, and a lack of meaningful consequences persist, there will be malicious cyber actors.

Unfortunately, across the full set of actors, there is no authoritative perfect picture or master list of the agencies and their tradecraft, tools, personnel, or targeting lists. Instead, we have a modern-day parable of the "Blind Men and the Elephant," where different defenders have a unique perspective based on their viewpoint from where they sit across American infrastructure or from their incident response investigations. This leads to a confusing mashup of threat actor names, be they pandas, APTs, or Periodic Table elements. And that is just from the cybersecurity vendor community. Inside Government and across allied partners there are myriad codenames and jargon for the cyber actors knocking on our networks every day.

Case Study: Same Nation, Different Tactics

Cyber actors use various techniques, from opportunistic and commonly available, to highly sophisticated and only available to those with resources and time. We saw both play out last year. The Russian FSB, the main successor to the Soviet-era KGB, carried out a broad campaign scanning for unpatched network access points known as VPNs in a variety of sectors, from Federal, State, and local government, to the aviation sector and the defense industrial base. There was nothing particularly sophisticated about this activity, they simply looked for the out-of-date VPNs and exploited them with common techniques. At the same time, the Russian SVR, the main foreign intelligence service, launched a stealthy campaign in late 2019 that used a variety of techniques exploiting trust—the that keeps networks going the world round. They moved downstream from Texas-based information technology (IT) company SolarWinds into customer networks, while also exploiting authentication techniques to gain access to email systems. As we were chasing the noisy FSB (and other actors, like the Iranians and ransomware crews) around the country, the ghostlike SVR was lost in the noise, patiently moving through a select list of targets. And that is just 2 actor sets from 2 agencies within 1 foreign adversary. Each agency has multiple groups, each nation has multiple agencies. Each group, agency, and nation have different strategic objectives and tactics to achieve them.

THE CHALLENGE OF SECURING DOMESTIC INFRASTRUCTURE

Our critical infrastructure is what drives our economy, supports National security, and contributes to public health and safety. Most critical infrastructure in the United States, however, is owned and operated by the private sector with only a patchwork of security oversight in place. It is hard to overstate the massive scope of the critical infrastructure security and resilience challenge. The levers Government has at its disposal to change behaviors, on the other hand, is underwhelmingly small.

This leads to 3 conditions limiting the ability of Government and industry to collectively improve critical infrastructure cybersecurity: (1) Lack of a deep understanding of what is truly systemically important across the economy, (2) a need for more meaningful methods for operational engagement with industry to address risk; and (3) insufficient funding and investment in security improvements.

Understanding Risk

The first challenge to overcome in enhancing the cybersecurity of our Nation's infrastructure is our understanding systemic importance must improve. Even within classic infrastructure sectors and systems that are generally easy to define—banking and finance, energy, and transportation—only now are we really identifying the highest-risk functions within those sectors. Fortunately, the effort to understand systemic importance of industry functions is a growing area of focus for the Federal Government, in part driven by CISA's National Risk Management Center through the National Critical Functions (NCF) initiative.[1] By gaining a deeper understanding of the critical functions and systems that drive our Nation's economy the Government can bring together key players to operationalize risk management partnerships and make measurable progress toward a more resilient economy.

One of the most critical aspects of the NCF work will be to support efforts to understand the prevalence of more intangible sectors like information technology and communications. The IT sector is a horizontal or enabling sector rather than a vertical sector. The products and services offered by the IT sector, like computer operating systems, network management software, and cloud computing, are core to nearly every aspect of the economy—even our Nation's agriculture sector increasingly relies on automated technology to improve efficiency and increase capacity.

To more broadly understand systemic importance of enterprise software and platforms, Government and industry must work together to map the key components and players of our Nation's IT and communications infrastructure. Of particular focus should be those companies that have a dominant position in their market segment, and any disruption or compromise would have cascading and outsized impacts on the ecosystem. As a byproduct of enjoying economic success, those companies should recognize they have broader corporate citizenship responsibilities and must dedicate resources, personnel, and expertise to protect the very economy they so richly benefit from. At a minimum, companies should reexamine and ensure their approach to securing their products, processes, and customers.

NCFs In Practice: Defending the 2020 Election

The concept of organizing around a key NCF was central to the success of the protection of the 2020 election. Led by CISA, the election security community across Government and industry came together to understand the greatest risks to the administration of the election, developed strategies and plans to improve security of the key subfunctions and successfully defended the election. We must repeat that intensity of effort across the rest of the NCF set. The NCF initiative, as shown in the defense of the 2020 elections, has already laid the groundwork for the Continuity of the Economy recommendation in the 2020 Cyberspace Solarium Commission (CSC) report, subsequently included in the 2021 National Defense Authorization Act.

[1] National Critical Functions/CISA.

Improving Engagement between Government and Industry

In addition to improving our understanding of infrastructure, we must improve the methods by which we collectively engage on risk management efforts. CISA can lead this important endeavor. The agency supported the President's National Security Telecommunications Advisory Committee (NSTAC) in developing the 2014 Report to the President on Information and Communications Technology (ICT) Mobilization.[2] The core concept of the report was to develop a working partnership between industry and Government that could be immediately activated in the event of a large-scale cyber attack approaching a National emergency, yet many of the lessons of the report equally apply to steady-state resilience building activities. Two recommendations emerged from the report that are even more important than they were just a half decade ago.

(1) Conducting a Unified Risk Assessment.—The first is tighter integration between the collectors and analyzers from industry and Government of foreign cyber actor intelligence, in part through a Unified Risk Assessment Process for Mobilization. This fusion of private and public intelligence expertise can overcome the current imperfect nature of understanding, decision making, and response. A unified risk assessment process in both steady-state and response scenarios would bring together informed and experienced hands to determine means, intent, and ability to understand a potential or on-going threat actor campaign. Most importantly, the private sector and civilian agency experts can bring context and relevance to intelligence analysts that may not have a sufficient understanding of the domestic infrastructure landscape, which can lead to overlooking the relevance of collected intelligence. This risk assessment process and the contributing analysts should be a core function of the Integrated Cyber Center recommended by the Cyberspace Solarium Commission (Recommendation 5.3) and included in the 2021 NDAA, Section 1731 (Establishment of an Integrated Cybersecurity Center). The concept also echoes the recommendation of the President's National Infrastructure Advisory Council (NIAC) for the establishment of a Critical Infrastructure Command Center (CICC).[3]

(2) Establishing a ICT Enablers Working Group.—The 2014 NSTAC report also "developed a working model of the functional capabilities (in 6 categories) associated with the broader global ecosystem."[4] The companies that execute these capabilities are known as "ICT Enablers." While the core functions of the ICT Enablers no doubt require a fresh look and update, the purpose is the same—we must understand the core functions and the companies that substantially make up those functions. This is the essence of systemic importance in the IT Sector, those companies that dominate or hold a lynchpin position in the ecosystem have an outsized responsibility to contribute to the National defense. We must know who these companies are and then establish meaningful partnerships between industry and Government. Not just to trade business cards, but to share information on emerging threats or observed attacks.

Through the knowledge transfer associated with trusted partnerships, combined with the commitment and support of corporate leadership, the baseline of security across the ICT enablers should improve. Prior models have fallen short principally due to a lack of specificity in tasks and the inability of Government to host industry representatives outside of a handful of Information Sharing and Center (ISAC) representatives. By adopting a risk management agenda with discrete tasks and skillsets required, and industry organizing itself with deliberate representation of the companies that truly matter, much like the United Kingdom's National Cyber Security Centre Industry 100 model, CISA can more effectively identify and work with industry partners. The entity resulting from the Integrated Cyber Center or CICC mentioned above, building on existing CISA coordination mechanisms, can bring Government and industry together to improve partnership models to operationalize intelligence and risk management efforts.

Increasing Funding for States and Incentivizing Industry Investment

Even by identifying our infrastructure of concern and creating the mechanisms for engagement, it requires resources to secure systems, hire and train personnel, and engage in collective efforts. For State and local government partners, even if aware-

[2] NSTAC—Information and Communications Technology Mobilization Report 11–19–2014.pdf (cisa.gov), *https://www.cisa.gov/sites/default/files/publications/NSTAC%20-%20Information-%20and%20Communications%20Technology%20Mobilization%20Report%2011-19-2014.pdf*.

[3] *https://www.cisa.gov/sites/default/files/cisa/NIAC%20Actionable%20Cyber%20Intelligence__DRAFT-PREDECISONAL__508c%20(002).pdf*.

[4] NSTAC Report to the President on Information and Communications Technology Mobilization, pg 14.

ness is not an issue, lack of funding is an ever-present inhibitor to improving security.

1. State and Local Cyber Grants.—Congress should identify grant programs, much like the Homeland Security Grant Program, to distribute funding to State and municipal infrastructure programs to help improve their security programs. Grant programs should incentivize regional collaboration and coordination, creating a mutually supporting culture and community of security.

2. Expanding Training to Government Infrastructure.—CISA should also be authorized and funded to provide entry and mid-level information security and operational security education and training programs. These programs should prioritize remote learning opportunities in order to engage more students, but where more advanced or hands-on learning is more effective, CISA should be funded for mobile training capabilities to bring training to the students where they are.

3. Industry Incentives.—Industry should similarly be encouraged to invest in security programs, ideally through sector self-organization and implementation. In the mean time, the Executive branch should conduct a meaningful review of existing regulatory programs for cybersecurity requirements or extant authorities that could be used to require additional security. We are also seeing a emerging class of corporate leaders that understand the importance of cybersecurity and the need to invest. Conversely, there will always be a set of executives that look to shave costs and minimize outlay until forced to spend, if even then. With the appropriate engagement and education, the former class—particularly when identified as systemically important and provided the opportunity to best improve the security of their operations—should outpace the latter. After a period of time, all executives may prefer a more prescriptive approach with certainty.

4. Government Contracting Requirements.—The Government should start with where it does business with industry, Government should require standardized security practices as a matter of contracting. The U.S. Government can immediately improve visibility and understanding across Federal networks (though there will be cascading benefits to industry) by amending the contracting process to require transparency about the software itself, the level of access the software requires to operate, and the security measures in place to ensure the software cannot be manipulated through development, build, installation, operation, or maintenance. In addition, CISA should be included in the contract as an authorized recipient of vulnerability and incident notifications. As of now, privity of contract and the bounds of Non-Disclosure Agreements (NDAs) limit the sharing of information on risks or incidents beyond the vendor and the customer. This puts the vendor in the position of not being able to share information with CISA for broader understanding of an emerging or on-going incident.

THE GROWING RANSOMWARE NATIONAL EMERGENCY

Today's cyber threat landscape is not monopolized by state actors, in fact, the threat that most immediately and measurably affects the average American is cyber crime. Ransomware, specifically, has been on a steady rise over the last several years, with ransomware gangs typically operating out of countries that turn a blind eye toward their crimes, as long as the victims are foreign, and the money comes back home. According to the 2020 Verizon Data Breach Report, ransomware accounts for 27 percent of malware incidents, with the highest rate of occurrence in the education, health care, and Government administration sectors.[5] Ransomware crews have been propelled and professionalized by commodity malware and specialization across various hacking techniques, but also thanks to the availability of cryptocurrencies that allow for anonymous financial transactions.

The United States along with our allies need to take a new, more strategic and coordinated approach to overcoming the emerging National security emergency posed by ransomware. The counter ransomware "triplet" includes improving cyber defenses, disrupting the criminals' business model, and increased coordinated action against ransomware gangs and their enablers. This strategy will require Government and the private sector to contribute and commit to partnering together to break the ransomware cycle.

Improving Defenses

First, we must improve defenses of our businesses and agencies across all levels of Government. Ubiquitous use of multifactor authentication (MFA) for access to

[5] 2021 Verizon Data Breach Report, Figure 5., pg 7. Available for download here.

networks can limit credential abuse, updated and patched systems can prevent actors from exploiting known vulnerabilities, and a well-practiced incident response plan accompanied by backed up and off-line systems can enable rapid reaction and restoration. In many cases, even these straightforward steps are beyond the reach of many companies or State or local agencies. We need to rethink both our approach to technology deployment, including MFA by default, and the Federal Government should consider increasing technology upgrade grants to States and localities to retire legacy systems and join the digital transformation. The return on investment will extend beyond increased security and improve the efficiency of citizen services, support the U.S. technology sector, and open up more skilled technology jobs for a sluggish American workforce.

Disrupting the Ransomware Business Model

Second, we must break the business model of ransomware. Simply put, ransomware is a business, and business is good. The criminals do the crimes and their victims pay the ransom. Often it is easier to pay and get the decryption key than rebuild the network. There are 3 problems with this logic: (1) You are doing business with a criminal and expecting them to live up to their side of the bargain. It is not unusual for the decryption key to not work. (2) There is no honor amongst thieves and no guarantee that the actor will not remain embedded in the victim's network for a return visit later, after all the victim has already painted themselves an easy mark. (3) By paying the ransom, the victim is validating the business model and essentially making a capital contribution to the criminal, allowing them to hire more developers, more customer service, and upgrade delivery infrastructure. And, most worrisome, go on to the next victim. A useful law school exam question may be whether in a string of ransomed companies, if a victim of a subsequent ransomware attack might pursue legal action against a prior victim of the same crew that had paid off the criminal. There is likely no viable course of action here but continuing to allow for ransom payments is a net public policy negative.

We must address the ransomware business model head-on and disrupt the ability of victims to pay ransom. First, cryptocurrencies should be either more heavily-regulated or provide for more transparency via Know Your Customer regimes for cryptocurrency exchanges. Second, we need a National policy conversation on whether payments should be lawful. The Office of Foreign Asset Control (OFAC) has already started this dialog, declaring ransom payments to identified entities may be a violation of economic sanctions laws. Because the identity of the ransomware actor is not always obvious, the OFAC advisory may have an overall chilling effect on ransom payments.

More Aggressive Action Against Ransomware Actors

Third, we need more coordinated action against ransomware actors using the range of authorities available to Federal agencies, as well as capabilities and rights resident in the private sector. To be perfectly clear, I am not suggesting extrajudicial kinetic actions against ransomware gangs. However, other authorities available to law enforcement and military should be on the table, with great care taken not to blur the lines between the two. Traditional approaches have clearly not been sufficient to prevent the outbreak of ransomware. More aggressive disruption of malware command and control infrastructure, like the recent action against Emotet, is a good start.[6]. Where there are clear ties between ransomware actors and state actors or a potential imminent threat to an event or infrastructure of significance like a National election, action should be on the table. The private sector also has options available, as demonstrated by Microsoft's aggressive policing the abuse of its trademark and source code, including last fall's operation against Trickbot.[7] When coordinated and jointly conducted, private and public sector can make the internet an inhospitable place for cyber criminals. The recent establishment of the National Ransomware Task Force, hosted by the Institute of Security and Technology,[8] is a promising private-sector collaboration to change the rules of the game, assuming strong engagement and coordinated action with the Federal Government.

[6] Emotet Botnet Disrupted in International Cyber Operation/OPA/Department of Justice. *https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation.*

[7] New action to combat ransomware ahead of U.S. elections—Microsoft On the Issues. *https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/.*

[8] Institute for Security and Technology (IST) Ransomware Task Force (RTF). *https://securityandtechnology.org/ransomwaretaskforce/.*

ADVERSARY ABUSE OF INFRASTRUCTURE AS A SERVICE

Much of the state and non-state actor cyber activity targeting U.S. businesses and agencies uses our very own technology against us. State and non-state actors alike are using cloud infrastructure services and the protections afforded by law and the Constitution to steal intellectual property and potentially position themselves for future attacks. According to Ambassador Robert O'Brien, President Trump's last National Security Advisor, "(m)align actor abuse of United States (Infrastructure as a Service) products has played a role in every cyber incident during the last 4 years."[9] To stem the abuse of IaaS products, the last administration signed out Executive Order 13984, "Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities."[10] The EO directs the Department of Commerce to release for notice and comment regulations within 180 days that describe a regime that would require cloud service providers to implement "Know Your Customer" and Suspicious Activity Reporting measures.

While the new administration is obviously within its rights to review and revise or withdraw any pending rulemaking, this regulation, with adequate input from industry and cloud users, can limit abuse of cloud services through increased transparency. Even in the absence of the regulation, it would be wise for industry to consider adopting a voluntary set of transparent practices that would achieve the same outcome, absent Federal Government intervention.

IMPROVING FEDERAL CIVILIAN AGENCY CYBERSECURITY

As demonstrated by recent Russian intelligence activities, Federal agencies remain at the top of the targeting list for foreign cyber actors. Our Nation's 101 Departments and Agencies civilian agencies hold a wealth of unclassified information across a vast assortment of unevenly secured, monitored, and even mapped networks and systems. Despite an increased availability and deployment of cybersecurity tools via the National Cyber Protection System and the Continuous Diagnostics and Mitigation (CDM) program over the last 6 years, more must be done. Other shifts and gaps in the Federal Government IT space have hampered the ability of agencies to keep pace with the threat landscape. At the macrolevel, there are 3 general themes that hamper our ability to properly secure the .gov, even after several years and billions of dollars invested in security. First, there is still insufficient funding for modernization and new security tools. Second, there is a need for stronger governance across agencies. And third, visibility into network traffic is eroding due to increased use of encryption (a good thing!) and a shift to cloud-based services (also a good thing, if done properly).

Accelerated Investment in CISA Security Programs

Investing in Federal IT is not a one-shot deal, maintaining a modern and secure environment is simply the cost of doing business in today's world. This is particularly true as more and more services go digital and most of the Federal workforce remains remote due to COVID (and may remain remote for the foreseeable future). In the face of the these shifts and the attackers' relentless efforts to find seams in our defenses, Congress must not blink, even in the wake of the SolarWinds supply chain compromise.

The CDM program remains the critical core of Federal cybersecurity, though it is not currently deployed broadly or deeply enough in part due to agency ability to deploy at scale quickly, underestimation of required services, and funding constraints. CDM focuses on who and what makes up the network, including assets, identity, and data. Recently, NDAA Section 1705 authorized CISA to conduct proactive threat hunting across civilian networks, a key development in improving visibility across the 101 agencies. For this advancement to be successful, CISA will need to deploy detection capabilities, hire analysts to conduct the activities, gain access to the appropriate data, and the buy-in and cooperation from the agencies CISA is hunting across. With accelerated capability coverage and additional Federal agency support through expanded financial resources, CDM will more effectively and efficiently serve Federal agencies to search for and where necessary remediate Russian actor intrusions. CDM can also serve as a force for change and modernization across the Federal Government. Last spring, as COVID sprung up and threat actors targeted Health and Human Services networks, the program rapidly responded to help

[9] Press Release—Statement from National Security Advisor Robert C. O'Brien/The American Presidency Project (ucsb.edu). *https://www.presidency.ucsb.edu/documents/press-release-statement-from-national-security-advisor-robert-c-obrien-9.*

[10] 2021–01714.pdf (govinfo.gov). *https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01714.pdf.*

HHS upgrade security and systems to protect pandemic response and research. [sic] can be a catalyst for continued IT and cyber modernization across the Federal enterprise.

Stronger Governance Across Federal Civilian Agency Networks

At the governance level, roles and responsibilities across the Federal Government are unclear, potentially further complicated by the newly-authorized National Cyber Director (NCD) created by Section 1752 of the NDAA. Regardless of the organizational structure, the Executive branch must establish a comprehensive strategy and vision for Federal network modernization and security, drawing in the Budget side of the Office of Management and Budget (OMB) to coordinate and consolidate budgetary oversight, the Federal CISO as the policy framer, CISA as the tool provider and enforcer of security policy. The respective roles and responsibilities of the Federal CISO and CISA should also be examined. In effect, CISA is serving as the operational CISO for the Federal Government, particularly with the recent NDAA authorities—this position should be strengthened. Federal agencies are of course a part of this effort, but as time and our adversaries have proven, there are currently not enough technical resources and personnel available at the individual agency level to meaningfully protect the .gov in 101 different instantiations. Therefore, the Federal Government must set very clear cybersecurity expectations and standards for agencies and Congress should fund those expectations. There should be two paths for agencies to choose: (1) You either meet the enhanced standards set out or (2) CISA can do it for you. The first option, while achievable and likely appealing to agencies mature and confident in their ability to manage their enterprise risk, will also require funding unavailable to most agencies. Even then, it is economically inefficient for even the most mature agencies if a comparable offering exists elsewhere.

Increasing Visibility Through Centralized Services

The second option plays into the third area for improvement, increased visibility through centrally-managed services. The NDAA threat-hunting authorities provided to CISA will provide increased visibility at the host level, however, there are additional visibility gaps that need to be addressed. For example, as agencies have shifted to cloud-based services—particularly during the pandemic—CISA lost visibility into network traffic. That decrease in visibility is in part due to increased encrypted traffic, but also because the entire point of modern cloud-based "Workplace as a Service" is for the user to interact directly with the cloud rather back to the agency's network via a trusted connection. To do this securely, however, requires consistency and discipline in implementing the appropriate security controls, as well as collecting and maintaining the forensic records to empower detection, analysis, and response. To ensure consistency and appropriate logging, CISA should work with OMB and GSA to create a customer-centric, security-first hardened cloud-based email environment. This approach would be economically sensible at the macro and micro levels and would be centrally defensible to adversary attacks.

Even this may be too permissive of an arrangement and only a half-step toward the most logically defensible arrangement for civilian agencies—a centrally-managed and secured "Govnet." Common services that touch the public internet, including email, should be consolidated as much as possible, ideally by CISA's Quality Service Management Office (QSMO).[11] Such a configuration would clearly be an attractive target to attackers, and yet by consolidating security teams, visibility, and ability to act, a more resilient infrastructure is possible.

CONCLUSION

The piece parts are in place for our Nation to dramatically improve our cybersecurity defenses. We need to as a society accept that that, yes, each and every organization in the country whether private sector or Government, can be targeted by a cyber actor. And no, the Government is not going to save you. And yes, there is something that you can do about it, in fact you have a responsibility to your customers, stakeholders, and depending on where you sit in the economy, a responsibility to the country.

The key ingredients needed are leadership awareness and commitment in the private sector and a bolder vision from Government. That alone will not immediately solve the problem, but with those two pieces folded together, investment will follow, defenses will improve, and organizational and economic resilience will increase. It will take time and we will never reach or even see a finish line. Cybersecurity is an ever-evolving discipline, and the threat actors are motivated by a variety of in-

[11] Cyber QSMO Marketplace/CISA.

centives that we may never fully comprehend. But change for the better is possible, we just need to stop waiting for it to happen to us and instead, to quote Mahatma Ghandi, "be the change we wish to see in the world."

Thank you not only for this opportunity to testify before the committee today on this critical issue, but also for your partnership over the last several years. I have no doubt that my successor will enjoy a productive working relationship with the committee and that together we can continue to improve the Nation's cybersecurity and resilience.

I look forward to answering any questions you might have.

Chairman THOMPSON. Thank you very much.

I now ask Ms. Gordon to summarize her statement for 5 minutes.

STATEMENT OF SUSAN M. GORDON, FORMER PRINCIPAL DEPUTY DIRECTOR OF NATIONAL INTELLIGENCE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Ms. GORDON. Good afternoon, Chairman Thompson, Ranking Member Katko, and distinguished Members of the committee. I am absolutely delighted to be here to testify on this issue of utmost National security interest. It is great to see you all again, even as a private citizen and not as your principal deputy director of national intelligence.

There is little more important work we do as a Nation and as a free and open society than that which you are tackling here today and in the days to come.

I am here today to discuss 3 aspects of the issue: The nature of the cyber threats we face and that are emerging, the domains in which those threats manifest, and the imperatives that must drive solutions. My colleagues will discuss the specifics of recent attacks and proffer specific next steps. I hope to put each of those in context.

First, in terms of threat, offensive cyber capability is a global commodity, the means by which every interest of our adversaries and competitors is increasingly achieved. In a digitally-connected world, one need not travel great physical distance or expend great resource to achieve malign outcome.

Fifteen years ago, offensive cyber was the tool only of the great powers, wielded in a largely unconstrained environment with very specific, narrow intention against Governmental targets. Today, while it is especially destructive in the hands of some, like Russia and China, it is a tool of anyone who wants to do harm. While some are more capable than others of achieving strategic impact, all are capable.

In the hands of malign actors, cyber action can have physical, political, military, economic, and societal impact, as we have just witnessed this past year with ransomware attacks, intellectual property theft, theft of PII, disinformation campaigns, intelligence collection, and disruption of service.

We need to stop acting like these attacks are special or rare or somehow beyond our ken or ability to respond because they are happening digitally. This digital activity has physical consequence, and the outcomes that cyber actors are producing threaten our National security, sometimes in isolation, sometimes in aggregate.

In terms of domain, it used to be that governments held all the vital information, the secrets worth stealing, and wielded all the power and made all the decisions worth influencing. No longer. The engine of our great society also lies in our companies and our communities, and the decisions made in boardrooms and voting booths have global impact. As private companies and private citizens have become a threat surface, they, too, must receive National attention.

Threat actors today target whatever and whomever serves their purpose: Government and non-Government, critical infrastructure and private citizens, academic institutions and research centers, huge multinational corporations, and small businesses.

While in some cases the victim is the target, sometimes they are just the transportation and access to the intended quarry. Said differently, if you aren't the target, you may still be targeted. No one—no one—gets off free.

But most of all what we are seeing today are attacks on the most important aspect of free and open societies: Trust, in all its instantiations. We cannot allow that to continue undeterred and unthwarted.

Enough problem-identifying; I am with you. Your purpose, our collective purpose, and one that I know my fellow witnesses and I will commit ourselves to with you is to find a solution. Let me offer a few imperatives or first principles to guide your next steps.

First, solutions cannot be exclusively Federal or exclusively Governmental or exclusively United States. The Cyber Solarium report is a remarkable, important document, and it produced outstanding recommendations, and yet they focused more on Government response than shared responsibility with the private sector or other partners. There is opening here for new.

Second, solutions cannot be exclusively technical. For all our advances in network security, security is most effective when it addresses the entire operating ecosystem. There is no technology magic bullet. The best solutions address personal, physical, and operational security in combination.

Solutions cannot be only for the resource-rich. Since we are all connected, the least of us can affect the whole of us. Solutions cannot focus solely on single entities. Every organization is part of the larger end-to-end system. Did SolarWinds understand the responsibility they carried when they sold their products to the Treasury Department?

On a personal note, intelligence must also be more widely, more openly shared, especially about intent. I know that that is anathema to my former colleagues because knowing an adversary's intent is our most closely guarded advantage. But if we don't share it more broadly, how will a non-Governmental entity ever get ahead of their attackers?

Finally, we need to bring the problem into the light, ruthlessly, because evil can't survive there. There is still too little sharing, for many reasons, none of which are sufficient in light of the exposure we face by not taking advantage of our shared knowledge. Security and trust disproportionately favor the good guys, and we need to press our advantage.

To close out, I offer that we must approach today's rapidly-changing posture with continually-evolving practices. Where we have previously focused on tangible threats, we must now constantly face those that are intertwined and are part of the digital environment.

I look forward to your questions more. I look forward to being a resource for you as we find our way forward and overcome this threat, as we have so many in the course of our history. I look forward to your questions. Thank you so much for the opportunity.

[The prepared statement of Ms. Gordon follows:]

PREPARED STATEMENT OF SUSAN M. GORDON

10 FEBRUARY 2021

Good afternoon, Chairman Thompson, Ranking Member Katko, and distinguished Members of the committee. Thank you for the opportunity to testify on this issue of National security interest—cybersecurity and resilience. It's great to see you again, even as a private citizen not your principal deputy director of national intelligence.

Though my colleagues and I sitting before you all come from different backgrounds and have different perspectives on the issue, I think we all believe there is little more important work we can do as a Nation and as a free and open society than that which you are tackling here today and in the coming days.

I am here to discuss 3 aspects of the issue: The nature of the cyber threats we face and that are emerging, the domains in which those threat manifest, and the imperatives that must drive solution. My colleagues will discuss the specifics of recent attacks and proffer specific next steps, I hope to put those in context.

First, in terms of threat, offensive cyber capability is a global commodity—the means by which every interest of our adversaries and competitors is increasingly achieved. In a digitally connected world, one need not travel great physical distance or expend great resource to achieve malign outcome.

Fifteen years ago, offensive cyber was the tool of the great powers, wielded in a largely unconstrained environment, with very specific, narrow intention against governmental interests. Today, it is the tool of criminals, nation-states, and non-nation-state actors, and while some are more capable than others in achieving strategic impact, all are capable. In the hands of malign actors, it can have physical, political, military, economic, and societal impact, as we have witnessed just this past year with ransomware attacks intellectual property theft, and theft of PII, disinformation campaigns, intelligence collection activity, and disruption of service.

We need to stop acting like it's special, or rare, or somehow beyond our ken or ability to respond because it's happening digitally. This digital activity has physical consequence. The outcomes that cyber actors are producing threaten our National security.

Second, in terms of domain, it used to be that governments held all the vital information (kept the secrets worth stealing) and wielded all the power (made all the decisions worth influencing.) No longer. The engine of our great society lies in our companies and our communities, and the decisions made in board rooms and voting booths can have global impact, so the threat surface includes private companies and private citizens, and their decisions can have direct effect on National security as surely as it would if they held Government position.

Threat actors today target Government and non-Government, critical infrastructure and private citizens, academic institutions and research centers, huge multinational corporations and small businesses. While in some cases the victim is the target, sometimes they are just the transportation and access to the intended quarry. Said differently, if you aren't the target, you might be targeted—no one gets off free. But most of all, what we're seeing today are attacks on the most important aspect of free and open societies—trust—and we cannot allow that to continue.

Success of the opportunistic predator often can be thwarted by the cyber equivalent of locking the front door and putting your valuables in a safe. But in the case of relentless pursuers—most likely nation-states with massive resources and strategic patience—success can only be thwarted by understanding the intention of the actor and committing to whole-of-organization, whole-of-Nation, whole-of-society persistent attention to risk management.

Third, enough problem identifying. Your purpose—our collective purpose—is to find solution. Let me offer some imperatives or "first principles" to guide next steps.

- Solutions cannot be exclusively Federal, or exclusively Governmental, or exclusively United States.
- Solutions cannot be exclusively technical.
- Solutions cannot be only for the resource-rich.
- Solutions cannot focus solely on single entities.
- Intelligence must be more widely, more openly shared, especially about intent.

- Bring the problem into the light, ruthlessly, because evil can't survive there.

To close out with these principles in mind, and in the pursuit of solutions, I offer that we must approach today's rapidly-changing threat posture with continually-evolving defense practices. Where we previously focused on tangible threats, we must now constantly be adapting to the challenges presented by the digital world. To achieve this defensive agility, the intelligence community, Government, industry, and must work closer together.

I look forward to your questions. Thank you.

Chairman THOMPSON. Thank you very much.

I now ask Mr. Daniel to summarize his statement for 5 minutes.

STATEMENT OF MICHAEL DANIEL, PRESIDENT AND CEO, CYBER THREAT ALLIANCE

Mr. DANIEL. Thank you, Mr. Chairman and Ranking Member Katko and other distinguished Members of the committee, many of whom I have worked with before in various capacities, so it is a pleasure to be here before you today.

I appreciate and applaud you for taking the time to actually have this hearing so early in the sequence for this Congress. It shows the importance that you place on this issue.

As our previous 2 witnesses have said, the cyber threats facing this Nation are urgent and they are serious. So I am going to talk about 3 aspects, though, of the cybersecurity issue, of the cyber threats that we face, that should shape how this committee thinks about and how we as a Nation have to think about improving our ability to address this problem.

The first one of which is that, just as important as the urgency and the seriousness of the threat, the threat is getting steadily worse. There are really 5 trends a that are driving this evolution.

First is growth. Cyber space as an environment is literally getting bigger every second, because we keep hooking more and more devices up to the internet. No other domain—land, sea, or air—exhibits this behavior of steady and remarkably almost exponential growth.

But also diversity. The kinds of devices that we are hooking up to the internet are wildly varying now. It is no longer just about wired desktops or laptops, but about watches and cars and industrial control systems like water plants.

It is also about danger. It is no longer that we are talking about simple website defacement or even theft of information, but now effects, physical effects, through cyber space can cause harm and even death.

It is also about numbers. As Sue was just talking about, everybody and their cousin, practically, is now involved in cyber space—terrorists, hacktivists, nation-states, criminals. The numbers are quite staggering. Everyone has discovered that cyber is a good way to carry out their interests and achieve their agenda.

Finally, dependence. We, as a society, as Representative Katko pointed out, are highly digitally dependent. So things and disruptions that would have 25 years ago been minorly annoying are now organizationally catastrophic if they occur.

Another aspect of the nature of cyber space and cybersecurity is how it crosses boundaries and how it crosses silos. There is no other issue that I have looked at in public policy that is as "inter-" anything you want to put in there.

It is interagency. We cannot successfully simply take cyber and make it the responsibility of any one agency in the Federal Government. That simply will not work. Nor can we create an agency that can take all of those different aspects of cybersecurity and have that function either. So it is inherently an interagency issue.

It is also an intergovernmental issue, meaning that it is a State and local issue just as much as it is a Federal issue, as the elections that we just had back in November amply demonstrate.

It is an international issue because it crosses boundaries and borders. As Chris Krebs pointed out, you know, the majority of the malicious activity actually emanates from foreign places.

It is inherently public and private at the same time, because the vast majority of cyber space is owned and operated by the private sector.

Finally, there is also the issue of our mindset. We do not have the right mindset to actually think about cybersecurity correctly. In many ways, we suffer from problems that—of how we approach the problem that hinder our ability to tackle it well.

First of all, as Sue said, it is not just a technical problem, and we want to make it that—one that we can simply buy a gadget to fix. But it is not. It is an economic, it is a business, it is a privacy issue, a National security, law enforcement, psychological problem all rolled into one.

We also want to make it a problem that we can solve. But, as you will hear many of us talk about, you can never solve this problem. We will never achieve 100 percent security. So it is a risk, instead, that we have to manage.

We also tend to think about keeping our adversaries out of networks, but that is not going to work either. We can never keep them out of a network. Instead, we need to think about how we thwart the goals that our adversaries are trying to achieve, rather than simply keeping them out. That will give us many more bites at the apple.

We also tend to try to make cyber space work like the physical world, but it doesn't. The physics and math of cyber space are different. It is a nodal network that operates at light speed, and concepts like borders and distance and proximity all have different meanings.

Finally, we tend to think of cyber space as if it were some sort of global commons, but that is not true. Every bit of cyber space is owned by somebody. Those boxes and computers and laptops and servers all exist on somebody's territory. There is no equivalent to international waters in cyber space.

So, just to conclude this, you might think that, given all that I have laid out, that I am actually a pessimist, but I am not. I actually do believe, as Sue said, that we can make cyber space safer and we can reduce our risk. It will be hard, and it will require us to be innovative not just in technology but in our organizational structures and processes and laws and policies as well, but I believe we can do these things.

I look forward to your questions and working with the committee on this topic. Thank you very much.

[The prepared statement of Mr. Daniel follows:]

PREPARED STATEMENT OF MICHAEL DANIEL

FEBRUARY 10, 2021

Thank you for the opportunity to appear before you today for this hearing on Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience. My name is Michael Daniel, and I am the president & CEO of the Cyber Threat Alliance (CTA)—an information-sharing organization that now includes 32 of the world's leading cybersecurity companies. Prior to CTA, I served for over 20 years in the U.S. Federal Government, including 4½ years as special assistant to President Obama and cybersecurity coordinator at the National Security Council.

Let me begin my testimony by thanking the committee for holding a hearing on this important issue. The cybersecurity threats facing the United States are significant, urgent, and potentially life-threatening—and our Nation must improve its ability to counter them. This committee plays a key role in enabling the Federal Government to meet this challenge. This testimony will lay out the cyber threat landscape the United States faces, the types of adversaries conducting cyber operations, and some long-term goals and principles to address these threats. I will also touch on Federal Government organization, Federal agency cybersecurity, and how to think about cybersecurity in more productive manner.

THE CYBER THREAT LANDSCAPE

We live in a digital age. Digital technologies increase efficiency and productivity, shrink distances, and enable news ways of working and connecting. However, digitization also brings challenges and potential vulnerabilities that—left unchecked—threaten to undermine our National security, economy, and public health and safety. Although the United States faces a myriad of cyber threats, 5 trends are making these threats worse over time:

(1) Cyber space is expanding.—As we connect more devices to the internet, we are making cyber space bigger. It is the only human environment that is continually expanding at a meaningful pace. Land, sea, air, and near-earth orbit are not growing to any appreciable degree, but cyber space is different. While estimates vary, everyone agrees that the growth is enormous. For example, Cisco conservatively estimates that by the end of 2021, 27.1 billion devices will be connected to internet, an increase of 10 billion devices since 2016. That figure translates to 5.5 million devices per day or 60 devices every second.

(2) Cyber space is becoming more heterogenous.—Beyond raw expansion, the variety of devices connected to the internet keeps increasing. These devices are not just desktops, laptops, or smartphones. They are light bulbs, refrigerators, cars, thermostats, sensors, machine tools, dams, water purification plants, oil rigs, toll collectors, and thousands of other "things"—a huge array of different kinds of devices with different functions, protocols, and security features. The combined growth in volume and heterogeneity makes effective cyber defense extremely difficult.

(3) Malicious cyber actors are becoming more numerous.—The number of malicious actors in cyber space continues to grow rapidly as hacktivists, criminals, and nation-states all learn that they can pursue their goals relatively cheaply and effectively through cyber space. The barriers to entry are low and the potential return on investment is high. As a result, the volume and frequency of malicious cyber activity is increasing dramatically.

(4) Cyber threats are becoming more dangerous.—As recently as a decade ago, cyber actors generally limited their malicious activities to stealing money or information, temporary denial-of-service attacks, or website defacements (the digital equivalent of graffiti). But over the last 10 years, malicious actors have shifted to more destructive and disruptive activities. The physical disruption of the Ukrainian power grid, the use of cyber-enabled information operations to influence electoral processes, the release of the destructive NotPetya malware, and the scourge of ransomware are all examples of this trend.

(5) Cyber incidents are becoming more disruptive: as we have become more and more digitally dependent, the potential impacts of a cyber incident have also increased.—It is becoming harder for us to operate without access to the internet; the need for a significant portion of the workforce to work remotely during the pandemic highlights that dependence. What would have been a nuisance a few years ago can now kill people if they cannot get access to timely medical care due to a network outage.

Specific threats

Within these broad trends, I would highlight 2 specific threats:

Ransomware.—Over the last couple of years, one key threat that has emerged is ransomware. This malware encrypts data on a victim's system and in order to regain access to the data, the victim has to pay a ransom. In addition, adversaries are also stealing private information prior to encrypting it and threatens to release the data publicly or onto the dark web if the victim does not pay. This threat has grown to such a degree that it is no longer just an economic nuisance but a National security and public health and safety threat.

Operational Technology malware.—for many years, the computers that run operational processes in manufacturing, power generation, water distribution, and other industrial activities were largely proprietary and difficult to access from the internet. However, these systems are becoming increasingly connected and more standardized. As a result, the ability for adversaries to target and disrupt these systems has increased. A cyber attack against one these systems would have a much higher impact across our digital ecosystem that the typical criminal activity.

CYBER ADVERSARIES

While the number of malicious actors in cyber space can seem almost limitless, these adversaries are typically operating as 1 of 4 types. Each type has different goals, motivations, and resources, and while individuals can operate as different types at different times, this typology is useful for thinking about how to counter the activities of a specific type.

Terrorists.—Many terrorist groups make extensive use of cyber space for recruiting and communication, but fortunately very few are able to undertake disruptive or destructive actions. However, these groups almost certainly have aspirations to conduct visible, spectacular attacks and if a nation-state decides that it is in their interest to train and equip a terrorist group, the result could be a destructive attack.

Hacktivists.—This type of actor has decreased in importance over the last few years, but they can still cause problems. Their motivation is primarily to gain attention for their cause or embarrass their opponents. While they might be OK with harming a "corporation" or a Government agency, they generally are not interested in causing wide-spread, permanent harm.

Criminals.—These actors are by far the most prevalent in cyber space. The motivation for these actors is simple: Money. They can be quite innovative and creative, but money is the driver. They are unlikely to spend time and resources trying to gain access to just one target; if their first few attempts fail, they will move on to the next target, just like in the physical world.

Nation-states.—These actors are pursuing their National security or foreign policy interests through cyber actions. Such interests can include espionage, influence operations, theft of intellectual property and trade secrets, deterrence, low-grade conflict and disruption, or destruction. While some nation-states have less technical capability than some high-end criminal groups, nation-states generally have discipline, patience, personnel, and complementary capability (such as dedicated intelligence agencies) to bring to bear.

LONG-TERM GOALS

Given these trends and malicious actors, the U.S. Government should pursue 3 long-term goals to counter the cyber threats we face. It should seek to raise the level of cybersecurity and resilience across our digital ecosystem; disrupt adversaries at a faster pace and larger scale; and respond more effectively to cyber incidents when they occur.

Raise the level of cybersecurity across the ecosystem.—Despite a growing recognition that cyber threats affect everyone, many organizations still have not implemented basic cybersecurity measures, such as two-factor authentication, and very few have reached a high level of maturity, even those that manage or perform critical National functions. They also have not developed sufficient resilience to cyber incidents. Given this situation, the Federal Government should aim to improve cybersecurity and resilience across the board. Setting such a goal does not require the Government to treat all organizations the same or not prioritize some functions over others; in fact, achieving this goal requires such prioritization. However, given the interconnected and interdependent nature of cyber space, the goal should be that all organizations reach a level of cybersecurity commensurate with their size, industry, and overall function.

Disrupt adversaries at scale.—Since we cannot rely on defense alone, the U.S. Government also needs to increase the pace and scale of its disruption efforts, whether against nation-states, criminals, hacktivists, or terrorists. Disruption should involve all the elements of National power, including diplomatic, economic, law-enforcement, cyber-technical, military, and intelligence tools. It will also require working with private-sector cybersecurity providers and collaborating internationally. While we have made significant progress in these activities over the last decade, we need to impose greater costs on our adversaries.

Respond more effectively to incidents.—No matter how much we improve our defense and offense, our adversaries will sometimes achieve their goals. They will succeed in stealing information or money, causing disruption, or holding a critical function at risk. To deal with those situations, the Federal Government needs to be able to deal with such incidents rapidly and efficiently, enabling private-sector owners and operators to restore functionality expeditiously.

The U.S. Government could achieve these goals in different ways; indeed, whole books have been written on specific aspects of these 3 goals. However, based on my experience both in and out of Government, employing the following principles will increase the chance of success:

1. Focus on comparative advantage.—The Federal Government should not try to replicate the technical capabilities available in the private sector. The technical information available to the cybersecurity industry is extensive, and the Government is unlikely to have technical information the private sector does not. However, the Federal Government does have unique information in the form of attribution, context, and a strategic view point. It also has a comparative advantage in funding basic R&D into cybersecurity, such as how to reduce the exploitable error rate in computer code. While some private-sector entities can disrupt adversaries using a variety of means (such as Microsoft's legal actions), the Federal Government can impose costs on adversaries in ways that the private cannot and should not: Public attribution, law enforcement actions, economic sanctions, diplomatic actions, and other means. Focusing on each sector's comparative advantage will enable the collective whole to be greater than the sum of the parts.

2. Incentivize good cybersecurity behavior.—While at times the Government may need to compel certain actions, the Federal Government should increase the incentives for organizations to implement better cybersecurity:

- *Strategic use of existing regulations*.—The Federal Government should ensure that existing regulations promote good cybersecurity behavior, not inhibit it. Most of the time, new regulation is not required; instead, agencies should focus on implementing regulations that are already on the books.
- *Support and encourage the use of best practices*.—The Federal Government can be a neutral, reliable party in identifying good cybersecurity practices. Two good examples are the National Institute of Standards and Technology's Cybersecurity Framework and the Software Bill of Materials initiative.
- *Drive industries to set standards of care*.—Establishing the generally-accepted level of cybersecurity for organizations within a given industry would have a dramatic impact across the ecosystem. It would remove considerable uncertainty and enable businesses to plan investments. It would address concerns about liability and reduce barriers to collaboration and information sharing.
- *Increase publicly-available information*.—The Government can facilitate disclosure of information that can help customers, clients, shareholders, and other relevant parties take appropriate defensive actions, better assess risk, and advocate for improved security. Examples of such requirements could include data breach reporting, information about material cybersecurity risks on financial statements, and public acknowledgements about how a publicly-traded company is assessing and managing its cyber risk, particularly at the board of directors' level. Such disclosures do not assist criminals or other bad actors—they already know where the weaknesses are; instead, these requirements allow market forces to operate more efficiently. These requirements should be standardized as much as possible at the National level and harmonized at the international level to the extent possible, to reduce burdens on companies and simplify reporting for consumers.

3. Reinforce stability in cyber space.—Governments should strive to make cyber space a stable, reliable environment in which to conduct business. Some key tools include:

- *Transparency*.—The U.S. Government should set the standard for transparency about its offensive cyber capabilities. Not in terms of details about tradecraft or tactics, techniques, or procedures, any more than we are transparent about the technical specifications for military weapon systems. However, we are quite open about the fact that we have attack fighters, submarines, and tanks. We should apply a similar approach to our use of offensive cyber. For example, we should continue to evolve our doctrine, being clear about how and when we would use cyber capabilities as a tool of National power. We should also be transparent about the fact of offensive cyber capabilities, just as we are open about our kinetic capabilities.

- *International norms of behavior*.—Norms can put certain activities "out of bounds." Not all nations will adhere to all the norms all of the time, but norms can help constrain behavior. Of course, we must adhere to the norms we promote—we cannot be "do as we say, not as we do" country. The United States has been effective in this area over the last decade, and we should continue to build on that success.
- *Confidence-building measures*.—Adapting these approaches from arms control and conflict resolution field has promise to reduce the risk of escalation due to accidents or unintended consequences.
- *Coalitions of the willing*.—Given the divergent views among nations regarding cyber space, privacy, and other issues, gaining global consensus on most topics is unlikely. However, this inability to reach consensus should not prevent the United States from assembling coalitions of the willing. Such groups will be far more effective than trying to go it alone or letting the perfect be the enemy of the good.

4. Increase resilience.—If we increase our ability to weather cyber attacks and maintain operations, then the value to our adversaries of conducting attacks decreases. Resilience also enables U.S. leaders to worry less about pre-empting foreign threats and escalating responses.

5. Increase operational collaboration between the public and private sectors.—Unlike in the physical realm, governments do not have a monopoly on cyber "force," and they are not likely to obtain such dominance any time soon. Therefore, the most effective action in cyber space will involve public and private-sector actors working together. Such collaboration goes beyond information sharing to synchronizing activity and it already occurs in certain circumstances. However, we need to vastly expand the scope and scale of these collaborative activities if we want to have a meaningful impact on our adversaries.

FEDERAL GOVERNMENT ORGANIZATION

Given the seriousness of the threats and the broad nature of the long-term goals I have outlined, reviewing the Federal Government's structure, agency roles and missions, and coordination capabilities makes sense. However, traditional policy solutions usually do not work for cybersecurity due to 4 unusual aspects about the issue.

Cybersecurity is inherently interagency

Bureaucracies prefer issues that fit neatly into one organization's mission. Cybersecurity is almost the exact opposite. It is a National security, military, intelligence, economic, public safety, privacy, diplomatic, law enforcement, business continuity, and internal management issue all rolled into one. It touches every Federal department and agency, and many Federal organizations have a legitimate, necessary role in cybersecurity. Thus, cybersecurity far exceeds any current agency's remit. Trying to stuff the whole issue inside one existing department or agency will fail.

Creating a "Department of Cybersecurity," will not work either—in fact, it would be a disaster. Cybersecurity is too integral to too many agencies' missions to centralize those functions in one department. We cannot remove cyber investigations from the FBI, oversight of financial service companies' cybersecurity from Treasury, incident response from DHS, and offensive cyber operations from the Department of Defense and consolidate them inside one department. FBI, Treasury, DHS, and DOD would end up recreating those functions to support their core missions. We would end up with even more complexity.

At the same time, cybersecurity's different aspects are not independent—they interact with each other constantly, sometimes in unexpected ways. Military cyber operations can disrupt intelligence activities or law enforcement investigations. Treasury sanctions could upset diplomatic negotiations. DHS's focus on mitigation could hinder DOJ's ability to prosecute a cyber crime—or vice versa. Network defenders want information from the private sector, but many in the private sector are worried about regulatory action if they share.

As a result, we can employ neither of the standard government approaches to emergent issues—make it one agency's mission or create mutually-exclusive agency siloes for different aspects of the problem. Instead, we must weld these disparate activities together into a single whole through regular, intense, sustained interagency coordination. Such coordination does not occur naturally in any government or large bureaucracy: Personnel have limited incentives to coordinate activities across departmental and agency lines. That is not a moral failure or laziness, but a reality of human psychology. Instead, we must account for this facet of human nature and design our systems accordingly.

Inherently intergovernmental

Cybersecurity also affects governments at all levels, from municipalities to counties to State governments. It does not exclusively belong to the Federal Government. As cybersecurity has become a more pressing issue for organizations of all kinds and the threat of disruptive or destructive activity has grown, the need to incorporate State, local, territorial, and Tribal governments into our cybersecurity activities has grown. For example, State, local, territorial, and Tribal (SLTT) governments play a crucial role in a critical National function, elections. As a matter of democratic principle, we want to maintain SLTT control over elections; on the other hand, expecting an SLTT organization to defend itself against the Russians or Chinese without Federal help is foolish. Therefore, we need to enable the Federal Government to collaborate more effectively with SLTT entities. In particular, the Federal Government will likely need to allocate additional resources to improving SLTT cybersecurity. However, we cannot make cybersecurity exclusively a Federal or SLTT issue.

Inherently international

Cyber threats cross international boundaries quite fluidly. During my time at the White House, virtually no issue was exclusively domestic. If nothing else, much of the cyber crime that afflicts U.S. citizens and businesses has an international connection. On the flip side, what we do domestically has implications abroad. Therefore, countering the threats we face requires significant international collaboration and cooperation.

Further, the international cyber environment is very complex, with many overlapping and intertwined issues. Internationally, cybersecurity involves diplomatic relations, law enforcement cooperation, financial interactions, trade issues, intelligence collaboration, and military operations, not to mention technology and competitiveness concerns. Trying to confine cybersecurity to a specific channel or type of interaction will not work.

Inherently public and private

Finally, cybersecurity forces the Government and the private sector into a different kind of relationship. Traditionally, the Government is either a regulator or a customer for the private sector. While the Government does have those relationships in cybersecurity, the Government and private sector can have a third type of relationship in this area, that of partner or peer. This peer relationship stems from the fact that the private sector owns and operates vast majority of cyber space, has equivalent (or better) technical insight and capability, and can take action that affects much of cyber space without the Government. This type of peer relationship is relatively new and we do not have the necessary laws, policy, procedures, or even vocabulary to fully manage it, other than the overused public-private partnership term. Thus, we need to fully develop the laws, policies, and procedures to govern this type of interaction, so that the relationships remain aligned with our overall sense of equity and appropriate roles for Government versus the private sector.

FEDERAL AGENCY CYBERSECURITY

In December, several private-sector companies identified malicious activity that enabled the Federal Government to unravel an incredibly broad cyber-enabled espionage campaign. This intrusion effectively gave the Russian government unfettered access to numerous unclassified U.S. Government networks for over 9 months. It is difficult to overstate the intelligence value the Russians gained from this access or the likely damage to our National security. That said, based on the publicly-available information, the activity associated with this intrusion appears to consist of espionage, something in which all States engage. As a result, although extremely damaging to our National security, this intrusion is not an "attack."

The fact that the intrusion does not constitute an attack necessarily constrains the U.S. response. "Constrain" does not mean "prohibit." We should respond forcefully to this intrusion through diplomatic channels, such as by expelling Russian diplomats or exacting a cost in other venues. We should also signal that if the incident turns out to involve activities other than espionage, the United States reserves the right to escalate accordingly. But we should carefully calibrate our response with the knowledge that the United States also conducts cyber-enabled espionage.

Regardless of the U.S. response, the intrusion revealed some on-going weaknesses in Federal cybersecurity structure, practices, and funding. While the 2021 National Defense Authorization Act included several provisions that directly address some of these weaknesses (for example, authorizing CISA to conduct threat hunting across

Federal civilian agencies), the Federal Government still needs to aggressively reduce its cyber risk. First, it needs to continue consolidating cybersecurity services within a smaller number of agencies; just as with payroll services, only a small number of agencies should provide cybersecurity services to most Federal agencies. Second, Congress needs to enable agencies to retire their legacy IT systems at a much faster rate. Replacing legacy systems would reduce cyber risk, improve productivity, and enhance service delivery. The $9 billion for cybersecurity originally proposed in the Biden administration's American Rescue Plan would help achieve this goal, especially resources allocated to the Technology Modernization Fund.

WHAT WE CAN EXPECT FROM PRIVATE-SECTOR COMPANIES

This topic is sensitive one. On the one hand, we do not want to re-victimize organizations that have suffered an intrusion, theft, disruption, or destructive attack; moreover, since no organization can prevent all intrusions all of the time, just because a company experiences a breach does not mean it has failed—it might have really excellent cybersecurity. On the other hand, companies have a responsibility to protect customer data or access to other organizations, which means implementing at least some cybersecurity measures, so it is also possible for a company to be negligent in this regard. The question lies in distinguishing which situation a company is in. Threading this needle is one of the key policy challenges for the United States right now.

The solution lies in establishing standards of care for cybersecurity. These standards should vary, depending on factors such as size, industry, function, geography, etc. Standards of care exist in many industries for areas such as safety; sometimes the standards are entirely industry-driven and sometimes they backed up by regulation. These standards should not be static checklists and will need to be flexible enough to evolve as technologies and threats change.

Despite developing and implementing standards of care, the resulting improvements to cybersecurity will still be insufficient to thwart dedicated nation-state intruders. In fact, no amount of cybersecurity investment will prevent a determined nation-state from gaining access all of the time. Therefore, we should not expect individual companies to defend themselves against highly-capable nation-states, such as Russia or China, by themselves. The Federal Government should be able to quickly come to the aid of an organization facing a nation-state threat, whether at the request of the targeted organization or based on its own knowledge.

HOW TO THINK ABOUT CYBERSECURITY IN THE LONG-TERM

This testimony has identified multiple challenges for improving cybersecurity in the United States. While cybersecurity may seem like an impossible task, the truth is that we can improve our cyber defenses. The answer is not purely technological, although technology is certainly required. The primary change we need to make is in our mindset. We need to change how we think about cybersecurity in several ways:

- *Adopt a risk management approach*.—Cyber threats are risks to be managed, not problems to be solved. We will never eliminate cyber threats entirely, nor will we reach a point of 100 percent security. Therefore, we need to think in terms of risk management. Just as a company can never eliminate the risk of bad weather disrupting operations, we need to treat cyber threats as a long-term risk management problem.
- *Use more than technology to counter the threat*.—Managing cyber risk effectively involves more than just employing technical solutions. Technology is necessary but insufficient for addressing cyber threats. Instead, we need to bring economic, psychological, organizational, process, policy, and legal tools to bear on the problem. Only by combining all these tools can organizations manage their cyber risk effectively.
- *Prevent adversaries from achieving their goals*.—If we think about cybersecurity from a "castle and moat" perspective, we will invariably fail. No organization can prevent all adversaries from gaining access to its networks all the time. Instead, if we think of cybersecurity as preventing the adversary from achieving their goals, then we get many more opportunities for success. If we define success as preventing the adversary from achieving their goal at any point along the way, then instead of defenders having to be "right" 100 percent of the time, the adversary has to make zero mistakes at every step. That mindset provides many more opportunities to thwart the adversary than the old castle-and-moat approach.
- *Recognize that cyber space is not a global commons*.—One key barrier to thinking about cybersecurity effectively is that because we cannot "see" cyber space

directly, it feels divorced from the physical world. As a result, we often act as if cyber space is an amorphous domain that resembles the oceans or the atmosphere. In turn, this view leads us to act as if cyber space has large unclaimed, "international" zones equivalent to international waters or air space. But cyber space is intimately tied to territory. It exists due to computers, servers, and other devices that are all owned by a person or organization and residing on someone's territory. This recognition has significant implications for how we should view cyber operations in the international context, and the rules under which we want to conduct them. I want to be clear that in adopting a view that cyber space is tied to territory does not mean the United States has to accede to the Russian and Chinese governments' view that the state should completely dominate cyber space, controlling everything from access to content. This conceptual approach should, however, shape how the U.S. Government and other aligned nations act and operate in cyber space.

CONCLUSION

Based on this testimony, many people might conclude that I am a pessimist when it comes to cybersecurity. It is easy to be overwhelmed by the volume of malicious activity and become fatalistic about cybersecurity threats. However, I reject such fatalism. While we will never eliminate cyber threats entirely as long as we live in a digital world, we can improve our cyber defenses and resilience, disrupt our adversaries, and respond to events when they occur. If we achieve these goals, then we can continue to reap the benefits and minimize the cost of an increasingly connected world. Fundamentally, cyber space is a human-created domain and that means humans can choose to make it safer.

Thank you.

Chairman THOMPSON. Thank you very much for your testimony.

I now ask Mr. Alperovitch to summarize his statement for 5 minutes.

I apologize if I butchered your name, but I did the best I could.

STATEMENT OF DMITRI ALPEROVITCH, EXECUTIVE CHAIRMAN, SILVERADO POLICY ACCELERATOR

Mr. ALPEROVITCH. Thank you, Mr. Chairman.

Chairman Thompson, Ranking Member Katko, distinguished Members of the committee, thank you for inviting me to testify today.

I have spanned my 25-year career working in the cybersecurity industry, including as co-founder of CrowdStrike, now the world's largest cybersecurity firm. Now, as the founder of Silverado Policy Accelerator, a new bipartisan public policy organization focused on National security, foreign policy, and cybersecurity, I am exploring new ways to work with policy makers to strengthen our approach to the challenges that threaten American prosperity and National security.

Almost half a decade ago, I coined the phrase that we do not have a cyber problem; we have a China, Russia, Iran, and North Korea problem. These countries are the 4 primary adversaries whose malignant activity we try to counter in cyber space on a daily basis, just as we do in the physical world. It is also no coincidence that some of the most sophisticated cyber criminal groups in the world operate with impunity from the safety of these very same countries.

The latest supply chain attack, sometimes called the SolarWinds hack, already the most impactful in our history, has drawn attention to serious gaps in the U.S. cyber strategy. However, we now know that SolarWinds was only one of the many supply chain vectors used by the adversary and perhaps not even the largest one. As a result, I, along with other cybersecurity professionals, have begun referring to this hack as the “Holiday Bear” operation to indicate how wide-spread this activity truly is.

This event highlights the need for a broader paradigm shift in our approach to cyber strategy. Both private and Government organizations should adopt what we in the cybersecurity industry call an “assumption of breach” mindset, where defenders actively hunt on their networks for any presence of an adversary, believing that they are already there.

The only safe assumption in cyber is that networks are never safe. This approach to cybersecurity is not fundamentally different from what we do in the physical world, where we expect that foreign spies are already in our Government and have counterintelligence teams to identify them and mitigate the damage that they can do to our National security. We need to adopt the very same strategy in cyber space.

Mr. Chairman and Ranking Member Katko, I have 5 specific recommendations for this committee that can move us forward toward this paradigm shift.

No. 1, Congress should take steps to set CISA on a path to becoming the operational CISO, or chief informational security officer, of the civilian Federal Government. CISA should have the operational responsibility for defending civilian government networks, just as Cyber Command does for DOD networks. Congress could create incentives for Federal agencies to outsource their cybersecurity operations through CISA, such as exemptions for agency heads from FISMA compliance, and turn that responsibility over to CISA.

No. 2, Congress should make agencies adopt speed-based metrics to measure their response to cyber threats. Under an assumption-of-breach approach, the question is not, can we prevent an initial compromise? The much better question is, how long does it take us to find an adversary on the network and eject them?

In the private sector, I developed what I called the “1–10–60 rule” to measure response times to perceived threats. One, detect an intrusion on average within 1 minute, investigate it within 10 minutes, and isolate and remediate the problem within 1 hour—1–10–60.

Through legislation, Congress could require agencies to adopt speed-based metrics by mandating that they collect data on the average time it takes to perform these fundamental defensive actions and to report them to CISA, OMB, and the relevant oversight committees.

No. 3, Congress should pass a comprehensive breach notification law to require certain companies to report technical indicators associated with breach attempts to CISA even when no personal information is actually compromised.

No. 4, Congress should take steps to increase security standards for vendors supplying high-risk software via Government acquisition processes. Congress should compel all Government vendors of high-risk software to undergo annual independent third-party audits of their source code and conduct penetration exercises of their networks. Agencies should be provided the results of these on-going audits as part of their procurement process, increasing transparency and incentivizing companies to quickly patch vulnerabilities in their networks or source code.

Finally, Congress should target the business model of ransomware criminals with stricter know-your-customer, or KYC, rules in cryptocurrency payment systems. Ransomware criminals rely on cryptocurrency, such as Bitcoin, to anonymously collect hundreds of millions of dollars in ransom payments. Congress should evaluate how stronger KYC requirements can be used to effectively stem ransomware threats and support Treasury Department action that achieves these objectives.

Thank you for inviting me to testify before you here today. Silverado is committed to being a long-term partner and resource for this committee. I look forward to your questions.

[The prepared statement of Mr. Alperovitch follows:]

Prepared Statement of Dmitri Alperovitch

February 10, 2021

Chairman Thompson, Ranking Member Katko, Members of the Committee: Thank you for inviting me to testify at today's hearing on cybersecurity. This is the policy arena I have spent my 25-year career in the technology industry exploring as a senior executive working with and advising some of the largest private-sector companies and most sensitive Government agencies in the country. Now, as the founder of the Silverado Policy Accelerator, a new bipartisan public policy organization focused on National security, foreign policy, and cybersecurity, I am looking at ways to build upon my experience in the private sector to work with policy makers and strengthen our approach to new challenges that threaten our critical infrastructure and the backbone of our economy.

Most recently as the co-founder and chief technology officer of CrowdStrike, which I helped to grow from an idea into the world's largest cybersecurity firm, I witnessed the complexity and scope of the challenges that the U.S. Government and businesses face in the cyber domain. Our adversaries in cyber space are sophisticated and numerous, ranging from global criminal groups conducting ransomware attacks and stealing financial and personal data, to nation-states executing complex espionage campaigns, stealing intellectual property, and launching highly destructive and disruptive attacks.

Throughout my years at CrowdStrike, I saw first-hand that cybersecurity represents a growing part of a broader geopolitical struggle between the United States and its adversaries and competitors. This inspired my decision to retire from CrowdStrike last February to launch Silverado to advance American prosperity and global competitiveness in a new era of great power competition. Silverado will use a venture capital approach to accelerate bipartisan policy solutions to pressing challenges in critical areas of economic, strategic, and technological competition. We are set to officially launch next week, and I hope this will just be the first of many occasions for Silverado to engage with this committee to support your important work for the Nation.

As the United States enters a new era of competition, on battlefields old and new, modernizing and further resourcing America's cyber strategy is a necessary precondition for achieving any number of other critical Government objectives. In my testimony today, I will outline a conceptual framework for understanding cybersecurity. I offer 5 recommendations that I believe will meaningfully improve our ability to anticipate and prevent cyber threats and fortify our cyber defenses, building on the recommendations and critical work undertaken by the Cyberspace Solarium Commission:

1. Providing the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. Department of Homeland Security with the authorities and resources to one day become an operational Federal CISO, or chief information security officer, for the civilian Federal Government;
2. Adopting speed-based metrics to measure agencies' response to cyber threats;
3. Passing a comprehensive Federal breach notification law;
4. Increasing security standards for vendors supplying high-risk software through Government acquisition processes; and
5. Targeting the business model of ransomware criminals with mandatory "Know Your Customers" rules in cryptocurrency payment systems.

THREAT LANDSCAPE

Almost half a decade ago, I coined the phrase: "We do not have a cyber problem, we have a China, Russia, Iran, and North Korea problem."

Cyber space is not a separate virtual world, immune from the forces that shape the broader geopolitical landscape. Instead, it is an extension of that landscape, and the threats we face in cyber space are not fundamentally different from the threats we face in the non-cyber realm.

China, Russia, Iran, and North Korea are the 4 primary strategic adversaries whose malignant activities in cyber space we try to counter on a daily basis, as we do their more traditional tactics in the physical world. Oftentimes, these battle lines extend to non-state actors, such as the most well-organized cyber criminals. These actors inflict enormous damage on our economy by launching ransomware attacks and stealing financial data from our businesses and citizens, and it is no coincidence that they operate with impunity from the safety of their homes in these very same countries.

These countries conduct a variety of cyber operations against us on a daily basis, ranging from cyber-enabled espionage against our Government to the theft of intellectual property from our companies to destructive attacks that shutdown business operations to the interference in the foundation of our democracy: Our elections.

The challenges we face were highlighted just over a month ago, in December 2020, when we learned that multiple customers of SolarWinds, a network management company, had been compromised by a sophisticated supply chain attack by a nation-state adversary believed to be affiliated with one of Russia's intelligence services.

The latest supply chain attack has drawn attention to serious gaps in the U.S. cybersecurity strategy. As a threshold matter, I believe that it is misleading to refer to this most recent breach as "the SolarWinds hack." Although SolarWinds was a prominent attack vector that received early attention in the press, we now know that it was only one of many supply chain vectors that the adversary used to gain access to private networks. Because investigations into the scope of the attack are still on-going, we cannot even say with confidence that SolarWinds was one of the largest or most significant vectors. Continuing to refer to the breach as "the SolarWinds attack" distracts from the reality that the breach went far, far beyond a single company. As a result, I, along with other security practitioners, have begun referring to this hack as the "Holiday Bear" operation.

Additionally, as we have learned more about the breach over the past 2 months, I've come to believe that it is also misleading to refer to this incident as a singular attack, or even as a coordinated campaign with a defined end date. Simply put, the sort of sophisticated, long-term cyber-espionage enabled by supply chain vulnerabilities that came to light through this breach is not a discrete or self-contained occurrence; it is the new normal.

It is clear to me that the Russians have learned from their past operations. Throughout 2014–2015, SVR, the Russian foreign intelligence agency believed to be responsible for this most recent activity, launched a broad campaign which gave them access to the networks of the White House, the Joint Chiefs of Staff and the State Department, among others. The success, however, was short-lived, as U.S. defenders quickly detected the noisy campaign and ejected the adversary within weeks. I believe that those original mistakes led the SVR to reevaluate how they conduct new cyber operations and focus on compromising software supply chains in order to gain access to target networks in a much stealthier fashion and to remain in them for weeks, if not years. In some ways, this tradecraft is the cyber equivalent of the Russian illegals program, long practiced in human espionage operations: An extremely patient and long-term effort to gain maximum access to high-value U.S. targets. Since the 1930's, Russia has been sending covert sleeper operatives into our countries under non-official cover to live and work amongst Americans and over years get close to powerful officials in order to steal our secrets. Unlike the illegals program, however, supply chain-based cyber intrusions are much easier and cheaper to scale to hundreds of high-profile victims, all without putting their human intelligence officers at risk.

I believe that this is the Russians' new way of doing business in cyber operations, and I suspect we will continue to see this new approach for years to come. We have also seen China's intelligence services leverage supply chain attacks in the past, and we can expect them to incorporate valuable lessons from this latest Russian action into their own operations.

RECOMMENDATIONS

This Holiday Bear operation further highlights the need for a broader paradigm shift in both the private sector's and the Government's approach to cyber strategy. Across the board, organizations should adopt what we in the cybersecurity industry call an "assumption of breach" approach, where defenders operate on the basis that an adversary has already gained access to their sensitive networks. The premise is simple:

- No cyberdefense system is 100-percent effective at preventing breaches;
- Even with the best training, human error will inevitably foil the smartest defense strategies; and
- Adversaries are constantly adapting to existing defense mechanisms and designing new ways to circumvent them without being detected.

The only safe assumption in the cyber battlespace is to assume that networks are never safe.

The assumption of breach approach is the only appropriate paradigm to govern cybersecurity strategy in this new era of great power competition. Our competitors in this contest are highly sophisticated, well-resourced nation-state actors. We underestimate their capabilities at our own peril.

Incidentally, this is not any different from the approach we already take in the physical world. As a matter of practice, we assume that at any given moment there are people inside our sensitive Government agencies who have been recruited by foreign intelligence services. Our counterintelligence approach is not merely focused on preventing such recruitment. Instead, we explicitly undertake significant efforts to identify spies and limit the damage they may be able to do to our National security. We need to adopt this same approach in cyber space.

This shift in strategic paradigm necessitates a shift in practice. This committee should be commended for its strong leadership in pushing for new and significant resources to support the Federal Government's cyber strategy, most notably by creating CISA in 2018 and strengthening CISA's authorities under the fiscal year 2021 National Defense Authorization Act (NDAA). But, more needs to happen to capitalize on this momentum and deepen these commitments, and in particular, I have 5 recommendations for this committee's consideration:

1. Congress should take steps to set CISA on a path to becoming the operational CISO, or chief information security officer, of the civilian Federal Government.—The majority of the 137 Executive agencies lack the personnel, the knowhow, and the resources to execute a comprehensive cybersecurity strategy. Congress took an important step toward centralizing Federal cybersecurity strategy by creating CISA in DHS in 2018, but the next step is to give CISA both the authority and the resources that it needs to effectively execute its mission.

Ultimately, CISA should have the operational responsibility for defending civilian government networks, just as Cyber Command does for DoD networks. The recent NDAA, which vested CISA with the authority to hunt on agencies' networks without the explicit permission of those agencies, was a critical move in that direction. CISA will now need additional funding to build a 24/7 threat hunting operations center to fulfill the requirements of that mission. Another important step would be to create incentives for Federal agencies to outsource their cybersecurity operations to CISA, turning it into a cybersecurity Shared Service Provider. Such incentives may include exceptions for agency heads from FISMA compliance and turning that responsibility over to CISA, if it is actually being given the authority to secure that agency's network.

2. Congress should make agencies adopt speed-based metrics to measure their response to cyber threats.—In cyber space, the only way to reliably defeat an adversary is to be faster than they are. Under an assumption of breach approach, the question is not, "Can we prevent an initial compromise?" The much better question is, "How long does it take us to find and eject them?" Central to detecting adversaries is the speed with which they leverage the initial resource they have established as their beachhead within the network, move laterally across the environment, and gain access to other sensitive resources. Once adversaries are able to do that, what would have been a minor security event turns into a full breach that requires a lengthy and complex incident response process and that puts defenders' data and operations at risk. Stop the adversary quickly, and you have prevented them from accomplishing their objectives.

With this in mind, Congress should require Federal agencies to adopt speed-metrics that evaluate agencies' response to cyber threats based on the time it takes to begin and complete fundamental defensive tasks. In the private sector, I developed what I called the "1–10–60 rule" to measure response times to perceived threats: Detect an intrusion on average within 1 minute, investigate it within 10 minutes, and isolate or remediate the problem within 1 hour. Through legislation, Congress could require agencies to adopt speed-based metrics by mandating that they collect data on the average time it takes to perform 4 fundamental defensive actions: (1) Detecting an incident; (2) investigating an incident; (3) responding to an incident; and (4) fully mitigating the risk of high-impact vulnerabilities. Over time, these metrics would provide objective and diachronic measurement of an agencies' threat response capabilities that they could report to CISA, OMB, and the relevant oversight committees in Congress. If the metrics prove effective in decreasing agencies' response time to cyber threats, Congress should also consider models to extend their adoption by the private sector.

3. Congress should pass a comprehensive breach notification law.—Such a law would require major private companies, such as those in critical infrastructure, to report technical indicators associated with breach attempts to CISA, including for breaches where no personal information is actually compromised. If there is a single overriding lesson from the recent supply chain attacks, it is that the information sharing between Government and industry remains a serious challenge. Some victims have shared very little information about what took place inside their networks; others have not even publicly acknowledged that they were targeted.

At present, there is no comprehensive Federal breach notification law, and State-level laws are too decentralized, too focused on personal information instead of risk to systemically important critical infrastructure, and sometimes create a perverse incentive for companies not to investigate attacks. In the case of complex supply chain attacks like "Holiday Bear," one company's failure to publicly report a breach can have wide-reaching implications. For example, if cybersecurity company FireEye had not voluntarily and publicly shared evidence of their own compromise and that SolarWinds was the attack vector, the public and the Government may not have known about this highly impactful attack for many months to come. Yet, FireEye had no legal obligation to report this breach under existing law. They should be praised for their courageous decision, but unfortunately, not all other victims have followed their lead in transparency.

4. Congress should take steps to increase security standards for vendors supplying high-risk software via Government acquisition processes.—Government agencies and private-sector businesses currently rely on a number of companies such as SolarWinds whose software runs with high levels of privilege on their networks. Yet these agencies and businesses have little to no sense of the security levels of that software. Borrowing from a widely-used private-sector practice, Congress should compel these vendors to undergo annual, independent third-party audits of their source code and penetration exercises of their networks. The Government could require that companies provide the results of these stress tests as part of the Federal procurement process, or even require companies to publish the results of those audits publicly on their website. Not only would this process increase transparency for their customers, but it would also incentivize companies to quickly and efficiently patch vulnerabilities in their networks or source code and get a clean bill of health, as no one would want to publish a failed audit.

5. Congress should support stricter "Know Your Customer" (KYC) requirements for world-wide cryptocurrency exchanges to target the business model of ransomware criminals.—Dangerous ransomware attacks pose an existential threat to critical infrastructure and many small and medium businesses in this country. For example, criminal attacks on hospital systems—a favorite target of ransomware attacks—put the lives of American citizens in danger, especially during the pandemic, when hospital beds are already in short supply. Ransomware criminals rely on widely available and largely anonymous cryptocurrency, such as Bitcoin, to collect hundreds of millions of dollars in ransom payments without risk of disclosing their identities to victims or law enforcement. It is no coincidence that the explosion of ransomware attacks occurred only after the invention of cryptocurrency platforms, which are the oxygen that fuels the fire of these criminal operations. And while it remains very difficult to purchase goods and services, such as real-estate, cars, and other luxury items that these criminals may want, with cryptocurrency, it is currently easy to anonymously use cryptocurrency exchanges to convert ransom payments into reserve currency like dollars or euros.

The bottom line is that we need stronger tools to undermine the ability of criminals and nation-states to use cryptocurrency to receive and convert ransom payments and purchase illicit goods. The international community has already taken some steps to strengthen KYC requirements. In June 2019, the intergovernmental Financial Action Task Force (FATC) issued guidance recommending that virtual asset service providers, including crypto exchanges, share information about their customers with one another when transferring funds between firms. In December 2020, the U.S. Treasury Department published an advance notice of proposed rulemaking that would require cryptocurrency exchanges to perform and store KYC information on their customers, just like we require banks and other players in the global financial system to do. If designed and implemented properly, these types of tools can starve ransomware threat actors of the oxygen they need to operate.

Congress should undertake an evaluation of how stronger KYC requirements and other safeguards can be used to effectively stem ransomware threats and then propose legislation and support agency action that achieves those objectives.

CONCLUSION

I am grateful for this committee's leadership on cybersecurity issues, and I believe that these recommendations would further advance America's defense by bringing its cybersecurity strategy in line with an assumption of breach approach. As the recent supply chain breach has made abundantly clear, we cannot afford to delay these actions any longer. Every day we fail to act on them is another day that we leave the American government and our people vulnerable to cyber attacks, intellectual property theft, and espionage.

These new steps would also serve to preserve America's competitiveness in this new era of competition between the United States and its adversaries. This contest has reached an inflection point: The nations that present bold, long-term strategies to advance their economic, technological, and strategic interests will shape the future for decades to come, and the Nations that fail to act will fall behind. Modernizing America's cyber strategy is a linchpin that makes all other efforts to ensure continued American leadership possible.

Thank you for inviting me to testify before you here today. Silverado is committed to being a long-term partner and resource for this committee in our shared missions to address these critical challenges facing our Nation.

I look forward to your questions.

Chairman THOMPSON. I thank the witness for his testimony.

I remind each Member that he or she will have 5 minutes to question the witnesses.

I now recognize myself for questions.

This is based on the order of the witnesses' presentation.

All of us are Members of Congress, and although our last witness did a masterful job at the 5 suggestions, I would like to hear from the other 3 witnesses: What do you see as the role of the Federal Government in protecting cyber space from intrusion?

I will start off with Mr. Krebs.

Mr. KREBS. Yes, sir. Thank you for that question.

So there are obviously a range of different authorities within the Federal Government. I would start with the Department of Defense. They have the ability through Cyber Command and the persistent engagement/defend forward philosophy to go out there and figure out what the bad guys are doing and stop them, ideally, so to speak, catch the arrow before it gets here.

There are some side benefits of that, where they can identify targeting lists, like they did in Ukraine and elsewhere, against their elections, that we could bring that back and help inform domestic elections.

You have the intelligence community that also tries to figure out what the incentives are, what the targets are, where the adversary is going, and provide that information to defenders so that they can protect their systems. The law enforcement community has the ability to go out overseas, work with foreign partners, disrupt both state-actor and non-state-actor activities through indictments and other legal actions.

Then, finally, you bring it back home to the domestic civilian agencies that need to broadly work with the private sector, State and local governments, and the Federal Government to help raise awareness, drive smart investment in cybersecurity solutions, and, overall, you know, as you have mentioned in your opening statement, increase the baseline of security.

There is no single approach, though. It does take a team effort of disrupting the adversary, getting inside their head, knowing our risks, and then closing out our risks as aggressively as we can.

Chairman THOMPSON. Thank you.

Ms. Gordon.

Ms. GORDON. I will give you 3, one that Chris touched on, and that is, you can't find a single agency that has all the responsibility.

I actually think CISA's blueprint of attacking election security, to participate with law enforcement, intelligence, and go all the way from the Federal to the State to the local, is a really good model that needs to be codified. Importantly, you ought to look at the authorities to make sure that that joint participation in sharing is easy to effect and that there is someone who's got the con but not all the authority.

No. 2, after the stock market crash in 1929, you saw the rise of the SEC shared responsibility and the introduction of generally accepted accounting principles. They did that because they recognized what was happening in private companies, in public companies, affected our Nation's security. In 2021, is it time for us to consider a bipartisan Government and private-sector approach to looking at generally accepted security principles?

It just isn't satisfying to me that it is up to people's choice of basic-level security, particularly if it is a publicly-traded company and particularly if it is a Government organization. So I think we ought to look at something like that.

The last is, I think in this interconnected world, where the boundaries that we created in the past that were physical between Government and private sector, Federal and State and local have just been obliterated, we are in a place now where the threat surface is disproportionately not in Governmental control. We almost have to change the incentive structure in terms of who is responsible and who is supporting.

So I think what you could do is create incentives both for private companies who accept responsibility to get some benefit, and the Government has an obligation to share more of its information more usefully.

Thank you.

Chairman THOMPSON. Thank you very much.

Mr. Daniel.

Mr. DANIEL. Thank you, Mr. Chairman.

I would identify 4 roles for the Federal Government.

One is enabler. It should be enabling other elements in the economy, other levels of government, to do a better job at their cybersecurity, whether that is through providing resources or by, you know, providing information or, you know, supporting them in a variety of ways.

The Federal Government is also a disrupter, meaning that it should be carrying out actions to disrupt what our adversaries are doing, whether they are criminals or nation-states. That is through using all the tools of National power, whether you are talking economic sanctions, arresting individuals, carrying out technical operations, or even military or intelligence operations.

It is also a regulator and an enforcer, because it should be, you know, in some cases, setting the rules and enforcing those rules, even including in cyber space.

Those 3 are very traditional roles for the Federal Government, but the Federal Government has a fourth one in cyber space that is unusual, which is partner. Because the private sector has much of the technical capability and a lot of the expertise, and, as Sue pointed out, the Government does not have a monopoly on the use of force or technical capability in cyber space. So, therefore, the Federal Government needs to be operating collaboratively, as a partner, as a peer with many organizations in the private sector, such as cybersecurity vendors, telcos, and platform providers, in order to actually disrupt and carry out those other missions that I was talking about the Federal Government having.

Chairman THOMPSON. Thank you very much.

Mr. Alperovitch, you talked about those 5 items, and it looks like everybody is kind-of on the same page. Do you have some comments you would like to make on that, in terms of the role of the Federal Government?

Mr. ALPEROVITCH. Yes, absolutely, especially focusing on the defense of the networks themselves. I believe that CISA should be in charge of defending the civilian government networks and Cyber Command should defend the DOD networks.

Mr. Chairman, I also believe that, as the other speakers have said, we need to go on offense. We need to make it harder for the adversaries to conduct these operations. Law enforcement, in particular, and Cyber Command need to take further actions to disrupt infrastructure of threat actors, both criminal groups and nation-states, and raise the bar.

We need to look at using all the tools of our power to really focus on the 4 primary nation-states—Russia, China, Iran, and North Korea—and what we can do to deter their malignant activity in cyber space.

Chairman THOMPSON. Thank you very much.

The Chair yields to the Ranking Member for questioning.

Mr. KATKO. Thank you, Mr. Chairman.

I appreciate the comments that I have heard so far. As I said in my opening statement, it seems, at least in a dot-gov domain, that our efforts for dot-gov security are too confederated and too clunky and ultimately inadequate.

You know, Mr. Alperovitch, what you said with respect to CISA being the quarterback, if you will, that you think it should be designated as such, that is 1 of the 5 recommendations I had. I wanted to drill down a little bit more on that and see what you envision CISA's role to be as that quarterback in the dot-gov domain.

Mr. ALPEROVITCH. Absolutely. Thank you very much for that question, Mr. Katko, and thank you for your leadership on this issue.

I believe that CISA needs to become a shared service provider for cybersecurity for agencies. The fact of the matter is, when you look at over 130 different Executive branch agencies, the vast majority of them will never have the talent, the expertise, the resources to defend themselves against the most sophisticated nation-states out there, such as Russia and China, that are trying to break into their networks.

Certainly, you have the large agencies, the intelligence community, the DOD, law enforcement agencies like the FBI, that do have that capacity, but many small ones will never do that. As a result, I think that they need to start thinking about outsourcing certain cybersecurity tasks to CISA.

Chris Krebs, when he was director, set up a great set of shared services, such as shared email services that are secure, that CISA can deliver to agencies. They need to start adopting those.

We need to start thinking about incentives to encourage agency heads to start outsourcing that capacity. I think looking at FISMA and reducing the overhead of FISMA compliance for agencies that turn over that capability to CISA is one way that can encourage them to do so.

Mr. KATKO. OK.

With respect to OMB's role in this, do you believe that CISA should, over OMB, play more of a role in that area?

Mr. ALPEROVITCH. Absolutely. I think it is important to set standards so that agencies can look at what works and what doesn't work in individual agencies when it comes to cybersecurity. And OMB has a role to play to share the standards across the Government and try to get agencies to adopt similar types of technologies and approaches that have already been proven to work.

That is why I also believe that metrics, particularly speed-based metrics, are really effective at getting visibility for both CISA and OMB into what agencies are doing to be faster than the adversaries, to detect them, investigate, and remediate breaches as quickly as possible. Then you can learn from, sort-of, the best of the best in Government and try to make sure that everyone else adopts the same strategies.

Mr. KATKO. All right. Thank you very much.

Mr. Krebs, it is nice to see you again, and I appreciate your service during your time at CISA. Obviously, you have some expertise there, and I am going to kind-of ask you a similar question as I did Mr. Alperovitch.

Do you believe CISA should be playing that centralized authority as he described it? If so, what would you do if you were king and could shape that for them?

Mr. KREBS. Yes, sir. Thank you. I agree with pretty much everything Dmitri said. I can't take exception with anything, in fact.

Look, the approach we have taken over the last decade-plus due to some of the oversight mechanisms that are in place, in part by Congress, has taken us a half-step forward. We need to take that full step. The 101 Federal civilian agencies are simply not in a position to secure themselves all by themselves. The reason for that is the lack of resources, the lack of personnel, and the lack of follow-through.

So, you know, I have thought for some time now that, No. 1, we need a comprehensive Federal civilian agency cybersecurity strategy. We have to pull that together. We need the requirements to put in place for the agencies to meet. Those requirements will likely be very onerous and very expensive, and I can think of maybe a handful of agencies that would be able to comply.

So give them the opportunity to comply, or give them an option, as Dmitri said, an incentive, where the CIO in the CISO shop can just turn the keys over the CISA, and CISA can build those services through the quality service management office, like a hardened, secure, cloud-based email instance, and pull everyone in.

As of now, there are 101 different instances of email across the civilian agencies. That is just not a defensive posture. We have to bring it all into one hardened, single ring, so to speak, to make it most defensible. That is going to require authorities to compel, and it is going to require resources, but it is also going to take some time to implement.

Mr. KATKO. Well, I appreciate it. Basically, what we are asking is to do on the dot-gov side what they have already done on the dot-mil side with DOD. I dearly hope we can get that moving.

Now, Mr. Alperovitch, quickly, with respect to SolarWinds, from your perspective in the private sector, cyber espionage campaigns, where does CISA need to be focusing its attention going forward?

Mr. ALPEROVITCH. So I actually believe, Congressman Katko, that SolarWinds really represents a new normal for Russian intelligence.

If you look at what they were doing prior to SolarWinds, they were trying to be very noisy when they were breaking in and to be detected very, very quickly. I believe that they reevaluated post-their original compromises of the White House, State Department, and the Joint Chiefs of Staff back in 2014 and 2015 and realized that the supply chain vector, being able to compromise, sort-of, these high-risk software, enterprise software, like SolarWinds, and using that to gain access to high-value networks is really the way to go if you want to have long-term access to these networks and remain undetected for months, if not years.

In some ways, this mirrors exactly what they are doing in human intelligence with their illegals program, where they are sending spies over to this country to implant themselves for decades in our society and get close to people in power so that they can steal secrets. They are now trying to do the very same thing in cyber through the supply chain compromises, and I think this is going to continue on for many years to come.

China, I am sure, is looking at this very carefully and trying to adopt the same practices.

So I think the Government, CISA in particular, needs to take a really hard look at supply chain vulnerabilities. As I suggested in my testimony, we need to start looking at elevating standards for providers of this high-risk software to the Government. Requiring them to perform annual audits of their source code and of their networks, I think, is one way to do so.

Mr. KATKO. OK. Thank you very much.

I have so much more I could ask, Mr. Chairman, but I am out of time, and I yield back.

Chairman THOMPSON. The Chair will now recognize other Members for questions they may wish to ask the witnesses. I will recognize Members in order of seniority, alternating between Majority and Minority.

Members are reminded to unmute themselves when recognized for questioning and to then mute themselves once they have finished speaking and to leave their camera on so they may be visible to the Chair.

The Chair now recognizes for 5 minutes the gentlelady from Texas, Ms. Jackson Lee.

It appears we have a technical issue. We will fix that. We will go to——

Ms. JACKSON LEE. I am here, Mr. Chairman. Mr. Chairman.

Chairman THOMPSON. OK.

Ms. JACKSON LEE. Can you hear me?

Chairman THOMPSON. Yes.

Ms. JACKSON LEE. All right. Thank you so very much. First of all, thank you for this hearing.

Thank you to the witnesses.

Let me go with Mr. Alperovitch.

I believe you gave the 5-point agenda, if I am not mistaken?

Mr. Alperovitch.

Mr. ALPEROVITCH. Yes, I did.

Ms. JACKSON LEE. Yes. Could you give a little bit more of substance to the idea, I am going to call it the cyber czar, and the extent of that individual's authority? Would they be able to interface with agencies across the landscape, Federal agencies? Would they be able to cite them for their failings, or would they be instructed in what they need to do? Would they provide oversight internally? Obviously, Congress has the other part of oversight. What would that individual be responsible for doing?

Mr. ALPEROVITCH. Thank you for that question, Congresswoman Lee. I think it is a great question.

In some ways, I think the Biden administration has already resolved part of that issue by appointing an incredible individual, Anne Neuberger, as Deputy National Security Advisor for Cyber. I have known Ms. Neuberger for many years. She has done tremendous work at NSA and Department of Defense for over a decade on this issue, so there is literally no better expert in Government to work these issues.

I think, within the National Security Council, she will have the authority to coordinate strategy and policy for the U.S. Government, working together with the director of CISA. So I think we are on the path to getting the Government organized for success here.

Ms. JACKSON LEE. Thank you very much.

Let me move to Ms. Gordon.

Obviously, we are in a different climate where cyber may even be the tool for bad actors—Proud Boys, Boogaloo Bois, the Oath Keepers. How, in your capacity dealing with intelligence, would you see a new group of domestic terrorists being able to utilize cyber to interfere with the Government workings?

Let me just follow up with a question to Director Krebs.

Thank you for your service, as I do all.

The issue with SolarWinds, we had this problem with Mr. Snowden—a contractor, unvetted, and had a great deal of—how should I say it?—confidence and comfort. I would be interested in you following up on Ms. Gordon on how do you put the firewall up for these third-party contracts that we seem to be completely immersed in in the Federal Government.

Ms. Gordon, on the idea of cyber being a tool of destructiveness and bad acts.

Ms. GORDON. Yes. Thank you so much for the question. It is a great one.

I think that our domestic extremists and terrorists got a pretty good look at the playbook. No. 1 is, disinformation is incredibly powerful, the ability to overwhelm airwaves with any sort of messaging. We haven't talked much about disinformation as a part of the cyber threat, but it surely is and we learned it. They learned a lot of the tool kits that have been reused over the past 2 or 3 years. So I think that is No. 1, is how can they use their voice.

Then second is, I think you would expect them to use tools to disrupt normal business processes, the normal functioning of society, the normal ability of people to carry out functions that are much more even in order to be able to shape activities.

I think both of those are well within their ken. There are tools available to do it. It will take the kinds of things we have talked about from a Governmental level to be able to attack those.

We are going to have to look at how intelligence can support that. Because it is a little bit of a slippery slope with intelligence on domestic, but I think there is some craft that the intelligence community has, particularly born of their time in the counterterrorism fight, that can be applied to this problem.

Thank you so much.

Ms. JACKSON LEE. Thank you. I would like to work with this committee and you on these issues.

Let me quickly ask Mr. Krebs—and, Mr. Daniel, maybe you will be able to follow up in my short time and respond to this issue of the water systems being violated and what kind of cyber weaknesses do we have when that happens.

Mr. Krebs on the SolarWinds? Maybe there will be a second or so for Mr. Daniel.

Mr. Krebs.

Mr. KREBS. Yes, ma'am. I will try to do this quickly.

I actually think Dmitri did a pretty good job of laying out a few of the requirements that need to be in place, particularly for Federal Government contractors. That includes increased transparency and attestations to the security, not in a compliance-based way, which is just a checklist, but actually demonstrated security improvements.

But to get there, we have to have a better understanding of what enterprise software and services are systemically important. That is a lot of the work that I think CISA and the National Risk Management Center should be doing.

Ms. JACKSON LEE. Mr. Daniel, on the violation of the water system and the cyber impact? Mr. Daniel.

Mr. DANIEL. Sure. So I think what that shows is that our adversaries are willing to go beyond simply stealing information or even holding systems at ransom, but are willing to move toward destructive acts—acts that could cause physical harm.

I think what it also shows is that, you know, it is—you know, water systems are not something that, sort-of, immediately spring to a lot of people's minds. People have thought about the power grid or the financial system, but it is almost any system that is connected to the internet, which is essentially almost anything today, can be a target. So we need to be thinking very broadly in terms of our cyber defenses.

Ms. JACKSON LEE. Thank you, Mr. Chairman. I yield back.

Mr. BISHOP. Well, I may have lost—Mr. Chairman, did you just speak? I lost audio, I think, or couldn't hear you, sir.

Chairman THOMPSON. Well, we are recognizing you for 5 minutes.

Mr. BISHOP. I thought so, sir, but I just couldn't hear. Thank you very much, Mr. Chair.

As I was taking notes over the testimony—Mr. Daniel, I think I would come to you first—I noticed both you and Mr. Alperovitch focused on something that seemed instinctively accurate to me as a layperson that—you said it, I think—that we can't keep the adversary out of networks, and that instead, we need to thwart their objectives. It does seem to me that Government and private enterprise have spent inordinate resources to keep people out of networks, and so it makes sense to me to finally come to the conclusion that you can't.

But what does that mean—Mr. Alperovitch, I will come to him in a minute, because he talked about maybe substituting speed metrics, I believe, to find and eject intruders. I think there might be problems with that idea too, but how do you thwart their objectives, Mr. Daniel?

Mr. DANIEL. Well, so what I mean by that is that the adversary is gaining access to networks for a purpose. They are not simply gaining access to gain access. They are looking to steal information. They are looking to steal money. They are looking to——

Mr. BISHOP. Do damage.

Mr. DANIEL [continuing]. Cause—yes, do damage. They are looking to cause disruption. They are looking to achieve some objective. So if you change your mind-set to one of, I want to look at all of the different actions that the adversary has to do to achieve that objective, look at all of the different steps that they have got to get through to achieve that end goal and focus on where do I have the greatest comparative advantage to break that chain, to disrupt their operations, then suddenly, instead of the defender having to be right all of the time because you are trying to keep the adversary out, the adversary has to be right a hundred percent of the way through their efforts.

So you get many more bites at the apple to try to disrupt them. So if we start thinking about it in terms of, we succeed if they don't get to their end objective. To my mind, that is a much more effective way to think about cybersecurity.

Mr. BISHOP. So, again, as a layperson, it seems to me, that, for example, when we are worried about avoiding information theft, maybe we ought to think in terms of making a lot more information public so that we are not worried about it being stolen, particularly if it is lower sensitivity. Would that be a possible way to think?

Mr. DANIEL. That is certainly one way to think about it. You could also think about storing more of that data in encrypted form, so that even if the adversary gets it, they can't do anything with it.

Mr. BISHOP. If you are concerned about damage being done to data, then you can build in redundancy and have multiple copies of stuff to avoid damage. Would that be another way to go?

Mr. DANIEL. That would be another way to go. You try to think of all the different ways that you could thwart what the adversary is doing.

Mr. BISHOP. Speaking—Ms. Jackson Lee just made reference to the water system thing, I saw that story, and I wonder, is it necessary that things like that, where you can do damage, why is that connected to the internet? Why can somebody change the way a chemical is put into the water supply over the internet? Wouldn't there be a way to defend against the possibility of intrusion if you say networks are not impenetrable, period?

Mr. DANIEL. Well, certainly, Representative, it is certainly one of the principles in industrial control systems that you should minimize the number of systems that are connected to the internet, and there are best practices for how to do that in a way that is more secure.

But, certainly, you also want to build in multiple layers of defenses. Like in the case of the water system, they do have them. There are other alarms and things that might have detected that change that was made even after it was made.

But I think you raise a good point about really looking at and understanding your network and understanding why you are connecting what you are connecting and not just assuming that connecting it is a good thing.

Mr. BISHOP. Thank you, sir.

Mr. Alperovitch, you talked about this same issue and said that we need to adopt speed metrics in detecting and ejecting intruders. Doesn't the SolarWinds experience suggest that we might not be really able to do that either?

Mr. ALPEROVITCH. Well, I think—and thank you for that question, Congressman Bishop. I think SolarWinds' operation actually highlights some of the failures but also some of the successes. I know of a number of major companies that actually detected the intrusion quickly—Palo Alto Networks was one of them—and contained it before any damage was done. So it was certainly possible. Not everyone was successful at doing so, but you do have time.

When I was in the private sector, I coined this concept of breakout time, the time that it takes for an attacker once they get in, once they establish a beachhead within the network, to actually accomplish their objective, to get off that beachhead, to get to other resources within the network, elevate their privileges, get access to valuable data, ultimately steal that data or destroy it, whatever their objective may have been.

What I found is that, on average, it took adversaries from nation-state criminal groups over 4 hours to accomplish that objective. That may not seem like a lot, but actually, if the defenders are quick enough to detect, investigate, and remediate breaches within 1 hour, then you can stop them dead in their tracks, they can't get off that beachhead, and you eject them before they are able to be successful.

So if we start measuring every agency on their ability to detect, investigate, and remediate breaches quickly, we can start holding them to account and make sure that they are focusing on what truly matters, which is how they become faster than the adversary.

Mr. BISHOP. Mr. Alperovitch, I mean, isn't—and I don't think we have had a full accounting of the SolarWinds thing, but weren't they undetected for months?

Chairman THOMPSON. His time has expired.

Mr. BISHOP. All right.

Chairman THOMPSON. The Chair recognizes the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you for holding this hearing. I want to thank our witnesses for your testimony today and thank you for all you have done to better protect the country on a whole host of National security fronts and issues, especially on cyber.

I think almost all of you have referenced the Solarium Commission and its findings at one point or another. Thank you for recognizing that. As a commissioner on the Cyber Solarium Commission, I was very pleased with our final report and the findings in it, and hopefully it is going to be a great blueprint going forward for better protecting the country in cyber space.

Mr. Krebs, let me start with you, if I could. In the fiscal year 2021 NDAA, we codified the roles and responsibilities of sector risk management agencies with respect to their sectors and to CISA. The Solarium Commission recommends tying this to a 5-year National risk management cycle to get a holistic sense of where key investments need to be made across the National critical functions.

Do you agree with the Solarium Commission's recommendations or assessments?

Mr. KREBS. Thank you for that question, sir. Yes, I do, in fact, agree with the evolved approach to risk management across the National critical functions and the fact that it does take—it takes all the agencies that have relationships and expertise in a specific sector or subsector to play along with CISA and the intelligence community.

Mr. LANGEVIN. Thanks for that insight. I appreciate the feedback. By the way, thank you for the integrity you showed when you were director at CISA in securing elections and doing everything you can to make sure, as you said, they were the most secure in U.S. history.

Mr. Daniel, in one of your—and I have learned a lot from you over the years in our discussions, both when you were at the White House as cyber coordinator and since you left now to be in the private sector. In one of your valedictions as cybersecurity coordinator just before the end of the Obama administration, you spoke of the need to go beyond information sharing and do operational collaboration. I have to tell you, I think about that phrase all the time.

The Solarium Commission recommends creating a common toolset for joint collaborative environment for interagency and public-private joint analysis of cyber threat data. Do you agree with this recommendation? Any comments you have in that respect?

Mr. DANIEL. Yes, Congressman. Thank you very much for that. I agree that the Solarium Commission did just some tremendous work in this area to really highlight some key efforts that will really improve the cybersecurity of the Nation as a whole.

I think that this idea of operational collaboration in a collaborative environment is absolutely critical. Information sharing is important. I mean, I run an information-sharing organization, but you share information with a purpose, and that is to take action.

As Dmitri was saying, we actually need to be able to go on the offensive with all of our capabilities, and the only way to do that is to do that in a collaborative fashion. So when I use the term "operational collaboration," what I mean is that we need to move beyond just sharing information back and forth between the Government and the private sector, but actually enable multiple elements of the Government—law enforcement, intelligence, CISA, diplomatic, economic—to be lined up and synchronized in time with actions that the private sector can take, so that the actions of the Government and the actions of the private sector are mutually reinforcing and have a strategic impact on the adversary. So that is what I mean by "operational collaboration."

Mr. LANGEVIN. Well said. Thank you.

Mr. Krebs, let me go back to you. The fiscal year 2021 NDAA also contains a force-structure assessment for CISA to determine personnel and facilities needed going forward. How would you describe CISA's resourcing versus its mission? Let me ask you this also, in your time at CISA, were there times that you had to forego important projects due to resource constraints?

Mr. KREBS. Yes, sir. Thank you for that question. So at the top line, the budget at CISA, at least as I was director, was about $2.2 billion, which seems to be a pretty significant and it is, in fact, a significant amount. About $1.2 billion of that was focused on cybersecurity investments, cybersecurity programs.

However, of that $1.2 billion, about $800 million is focused on 2 programs—the National Cyber Protection System and the Continuous Diagnostics and Mitigation Program. So that leaves, you know, several hundred million dollars on the end for incident response, and actually very little, frankly, for broader engagement with the critical infrastructure community.

That was my biggest concern. My biggest regret was that we were not able to plow additional resources into the ability to get out there into the field and engage more critical infrastructure and State and local partners. However, the State-wide Cybersecurity Coordinator Act that was passed as well in the NDAA and some of the additional funding has given us more capability to get out in the field.

That is the one distinctive advantage of CISA, is that they operate primarily in the unclassified space. In COVID, when you can work remotely, you can follow the trends that the cybersecurity industry have done as well and actually employ people, not in the National capital region, but out in the field where you don't actually have to be tied to a Secure Compartmented Information Facility.

Mr. LANGEVIN. Right. I definitely agree that for CISA to effectively do its job, it is going to have to be properly resourced, and we are not quite there yet. But thank you for the work that you did there at CISA, and I look forward to staying in contact.

Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. [Inaudible.]

Mr. LANGEVIN. I don't know if we can hear you, Mr. Chairman.

VOICE. You are muted, Mr. Chairman, I think.

Mr. LANGEVIN. Mr. Chairman, we didn't hear you. I think you were muted. Something is wrong on that communication side.

Chairman THOMPSON. OK. Mr. Higgins, the gentleman from Louisiana, for 5 minutes.

Mr. HIGGINS. Thank you, Mr. Chairman. I think you are doing just fine with the technology we are dealing with right now. It is a challenge for all of us.

Mr. Alperovitch, we know that foreign actors are continuously looking for flaws in our Nation's cybersecurity programs with efforts to threaten our data integrity, our public health, our safety. China is our biggest global competitor, actively engaged in horrible things in their own country, stealing our Nation's economic and National security secrets, and vacuuming up large swaths of American data for nefarious purposes or for their own design. China works overtime to get themselves embedded into our information and communications technology supply chain.

Russia had and may still have total access to our unclassified Federal networks. It has been reported Iran was heavily involved in a misinformation campaign surrounding the 2020 election.

Congress is constantly talking about a deterrent strategy regarding cyber campaigns. It is critical that the United States imposes real costs on these cyber adversaries to attempt to defer future attacks.

Personally, I think we should strike back in the cyber realm. I would like your opinion on that, good sir. In your professional opinion, what is the best way to respond to foreign cyber attacks?

Mr. ALPEROVITCH. Thank you, Congressman Higgins. I think you hit the nail on the head in terms of the threat environment. All of the threat actors—and I would also add North Korea—are constantly hitting our networks, they are stealing our intellectual property, they are performing disruptive attacks, and in some cases, harboring criminal groups that are engaged in ransomware operations against our hospital networks and small businesses all over this country.

So we absolutely have to respond. I think we absolutely have to strike back, but I think we need to look at the full toolkit of our power. Sometimes cyber may be the right tool. Sometimes it may be something we do in the physical world, whether it be sanctions, diplomatic efforts, or sometimes even supporting with military capabilities opponents of those regimes, such as, for example, providing military aid to Ukraine that we have done to confront what Vladimir Putin is doing in that country.

So I think what we need to do is step back and try to figure out what is the best way we can influence the particular adversary, and the strategy will be different for each of the 4 countries that we are dealing with. Sometimes cyber will play a role. Sometimes it will be something else, but we shouldn't necessarily jump at the tool. We should focus on the overall strategy and then figure out which tool works best for it.

Mr. HIGGINS. OK. Let me ask you to clarify. How would we—if we are going to respond in the cyber realm, let's say, if we identify a cyber actor, we don't know who that sponsor is, how can we tell if it is a nation-state? Do you have confidence that with our current technologies and cyber infrastructure and the American men and women that are in charge of knowing these things, do you have confidence that we can tell the difference between a criminal actor operating from within a nation-state versus a nation-state-sponsored cyber attack? Do you have confidence we can tell the difference?

If so, why would a solution like a responding cyber attack—I have heard it referred to as a cyber bullet—if it is going to hit the bad guy, then it hits the bad guy, whether it is a nation-state or not, whereas if it is a criminal actor and you put sanctions on the entire nation-state, that unnecessarily injures our diplomatic relationship with some nation-states. In my remaining time, would you respond to that, please?

Mr. ALPEROVITCH. Absolutely, sir. On the first question, I do have confidence in the capability of our intelligence community. I have worked with them closely over many years, and the fact of the matter is, we have better capabilities to attribute cyber attack than we have ever had in our Nation's history.

Over the last 10 years, I can't think of a single major consequential cyber attack that was not attributed. Many of them have been attributed publicly, and the Justice Department, the last 4 years in particular, have indicted all of the 4 major countries—Russia, China, Iran, and North Korea—for their malicious cyber activity.

But even when we don't attribute things publicly, the U.S. intelligence community usually knows very, very rapidly, within days if not hours, who is responsible, because of the phenomenal capabilities we have on tracking cyber adversaries and infiltrating their own networks to understand what they may be planning to do.

So I think we do know who they are very well in most of these cases, and I think we can craft the right strategies to influence their behavior, including in cyber.

Mr. HIGGINS. All right. Listen, it is a very important subject. I thank the Chairman for holding this meeting, and Ranking Member, my colleagues on the committee. We are dedicated to addressing this in a bipartisan manner.

Mr. Chairman, I yield.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from New Jersey for 5 minutes, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman. Thank you, for once again being on top of these issues for a decade prior to it coming to fruition here.

Mr. Krebs, during your time at CISA, you launched the Rumor Control program. Could you discuss why CISA began the Rumor Control program and why it is important?

Mr. KREBS. Yes, sir. Thank you for that question. So the predicate for Rumor Control actually goes back 3½ years or so. In the preparation for the 2020 election, the CISA team, the Election Security Initiative, working with our State and local partners, spent a significant amount of time threat modeling how any actor, whether state actor or non-state actor, like a ransomware crew, could target and disrupt an election.

So we had dozens of scenarios that we subsequently deconstructed into their component pieces and were able to develop defensive strategies, where we could invest, where we could increase awareness and training and capacity. Toward the end, though, it became clear that in many ways, an actual hack was not the greatest concern. Instead, we were thinking about perception hacks, where an adversary could claim that they had either access to a machine or a minor cybersecurity event could be blown out of proportion.

Rumor Control was intended to provide factual information to the public on how elections actually work and the controls that are in place, and that software or hardware is not a single point of failure in any election and that there are controls, like paper-based ballots, in place to ensure the security of the election.

Mr. PAYNE. Thank you. During the 2020 cycle, we saw a significant increase in lies and conspiracy theories during the following election. What are the risk of political leaders amplifying election misinformation?

Mr. KREBS. Well, of course any time you have election-related misinformation, it can undermine the public's confidence in the election itself, the democratic process, regardless of the source, whether it is domestic or foreign interference.

Again, that was the concept behind Rumor Control in the rapid, real-time debunking of some of these themes, like the hammer and scorecard machine algorithm that was being manipulated by a foreign deceased dictator.

The point is, we have to get out in front of these rumors, this disinformation and misinformation, as quickly as possible and inform the American people on how these processes, these machines, elections themselves, actually work.

Mr. PAYNE. OK, thank you.

Ms. Gordon, we are still trying to understand the long-term damage that Trump's false, incendiary rhetoric around the election, coupled with the physical attack he incited at the Capitol, will have on the public's faith in our democratic processes.

Ms. Gordon, was there a noticeable spike in chatter to echo and amplify ex-President Trump's disinformation narratives?

Ms. GORDON. Thank you for the question, Congressman Payne. So I have been out of the intelligence community since 2019. So I am not tracking the information, but let me give you a little bit of perspective.

We know that our adversaries, particularly Russia, but not exclusively Russia, have as their strategic imperative to undermine democracy, to use any means that they can since the Cold War to be able to insinuate themselves into any rift that they see to exacerbate that problem.

So there will be—our adversaries will use that moment to do 2 things. No. 1, amplify messages that are destructive. Then the second is to take those images and hold them up globally to suggest that what we have long said we were is, in fact, not as good as what they have.

So the global impact is also present in addition to their using those events to try and further create risk. That is why this notion of protecting the digital space has to include disinformation, because what we saw was that——

Mr. PAYNE. Yes.

Ms. GORDON [continuing]. Is as dangerous as anything else. Thank you for your question.

Mr. PAYNE. Thank you. So, basically, the treasonous insurrection that we saw on the 6th plays right into our opponents' hands, correct?

Ms. GORDON. The activities that we have seen where we turn on ourselves are very useful to our adversaries.

Mr. PAYNE. Thank you, Mr. Chairman. I yield back.

Chairman THOMPSON. Thank you. The gentleman yields back.

The Chair recognizes the gentleman from Mississippi for 5 minutes, Mr. Guest.

The Chair will recognize the gentleman from California, Mr. Correa, for 5 minutes.

Mr. CORREA. Thank you, Mr. Chairman. Can you hear me OK?

Chairman THOMPSON. Yes, we can.

Mr. CORREA. I wanted to thank you and Mr. Katko for holding this most important hearing. I wanted to essentially say that just listening to our witnesses speak today, I ask myself, how did these folks acquire the weapons, the tools to such, with ease, penetrate our defenses in terms of cyber?

You know, as I think back at the history of this country, as we dealt with the Soviet Union, we used to have this concept called mutually assured destruction, which is, you attack us—you won't attack us because we can attack you back, and the cost is just too expensive.

Today, like Mr. Alperovitch said, you got China, Russia, Iran, North Korea, that essentially attack us, and essentially their folks in their area attack us with impunity. So my question is, what is it that we can do to essentially establish a policy of deterrence?

Because, in my opinion, these attacks should, in all sense and purposes, constitute a declaration of war on the United States. What are we doing? What can we do to stop these attacks? What is the deterrence that we can develop, can use, to have these folks that are essentially operating out of countries like Russia from attacking us?

I will start out by asking Ms. Gordon to answer that question or any comments you may have.

Ms. GORDON. I think it is the perfect question. Thank you for asking. I will give a start, and I will let my colleagues add on.

I think we have already given you some of the groundwork. No. 1, you can't stop all activity. You can't. So here is what you can do. You can increase the cost of attack by doing the simple things to make yourselves more secure, so you don't get nuisance activity.

The second is, you can understand—I hate the use of the word "red line," but you can understand what the impacts are to our society that we cannot tolerate and build policy around if those lines are crossed, we will respond.

Then the third is—and I think everyone has said the same thing—don't think of cyber action requiring exclusively cyber response. Once you have said what your National interests are and that those must be protected, you can find a whole range of solution. Cyber may be one of them, but that can't be the only one.

I yield to my friends.

Mr. CORREA. Mr. Krebs.

Mr. KREBS. Yes, sir. Well, just to build on a little bit of what Ms. Gordon said, you know, particularly emanating from those 4 countries—China, Russia, Iran, North Korea—the behavior will continue until the leadership has decided that it cannot tolerate further behavior.

I think there are still options on the table for more destructive attacks and more brazen attacks, particularly for Russia. I don't think we have hit the upper limit of their pain threshold. For instance, working, I think, with our allies, with the United Kingdom and elsewhere, where there are Russian ex-pats, Russian oligarchs, that have a significant amount of money, you start turning the screws on those individuals, and they will go back to the Kremlin and you may see some behaviors change.

Mr. CORREA. Mr. Krebs, we have heard this suggestion a number of years ago in this committee. You go after their pocketbook, you go after the oligarchs. Yet this has not been used. What has been deterring our country from using those kinds of weapons, which is, you hit them at the pocketbook? Excellent solution. Why do you think we haven't used that?

Mr. KREBS. I think that we have used some significant amount of sanctions, penalties against Russian actors, but this is not a single country effort. We have many allies and many friends that we need to partner with. I already mentioned the United Kingdom and the significant amount of Russian capital that has flowed into London and elsewhere.

We have got to go shoulder-to-shoulder with our adversaries, but at the same time, recognize that there are certain behaviors that, unfortunately, are within the realm of acceptable cyber behavior, and to a certain extent, that is going to continue to be espionage targeting, for instance, Federal agencies, not that it is OK, but those are the rules of the road right now.

Mr. CORREA. Thank you.

Mr. Daniel.

Mr. DANIEL. Well, I would say that to some degree, we actually have achieved some degree of deterrence, meaning that we have not seen wide-spread destructive attacks carried out against the U.S. power grid and other systems. So we have achieved a level of deterrence. But I think what you are referring to, Congressman, is that we—the level of activity that we have not been able to deter is still too high.

So I think that the way that I would frame it up is that we have to continue both increasing the costs from deterrence by denial, meaning that—and this was something the Solarium Commission talked a lot about—of, you know, making our systems harder, but also in figuring out creative ways to disrupt what the adversaries are doing. Maybe that is, you know—in the criminal networks, that may be going after the money flows, particularly going after cryptocurrencies, like Dmitri was talking about. Or in the nation-state context, we have to put it into that geostrategic context that

Dmitri was talking about and figure out how to raise the cost on our adversaries in a way that causes them to change their behavior.

Mr. CORREA. Mr. Daniel, excuse me. You talked about cryptocurrencies——

Chairman THOMPSON. Mr. Correa, your 5 minutes are up. I am sorry.

Mr. CORREA. Thank you very much, Mr. Chairman. I yield.

Chairman THOMPSON. The Chair recognizes the gentleman from New Jersey, Mr. Van Drew, for 5 minutes.

Mr. VAN DREW. Thank you, Chairman and Ranking Member. I think it is good that you put this meeting and discussion together.

Cyber threats pose a great risk to our Nation, whether attacks on State and Federal Governments, businesses, or even our hospitals. America is the focal point of the attacks. Our adversaries are more capable than ever to cause damage to our country. This poses a significant threat to our critical infrastructure, supply chains, and even elections.

Every day we face attacks from Russia, China, Iran, and North Korea. In our last election, we were victims of cyber attacks from some of the world's most dangerous adversaries. Just a few days ago, hackers infiltrated a water treatment plant in Florida and temporarily increased lye ratios to lethal levels.

In the third quarter of 2020, the world saw a 50 percent increase in the average daily number of ransomware attacks compared to the first half of the year. That is unacceptable.

As it relates to election security, the cybersecurity and infrastructure of CISA has become increasingly important in protecting our institutions. As the many bad actors in the global landscape continue to adapt in their attacks, we need to evolve in our response. We must remain one step ahead of our enemies, especially as it relates to election security.

If we do not have faith in our process, we cannot have faith in our country. CISA's role, working with State and localities, must continue to grow, so that Americans can have confidence in our democracy and assurance that the Federal Government is doing all that it possibly can do to protect its citizens.

So I have some questions. One is for Christopher Krebs, and you know I always talk about the Coast Guard because we have the only training center. Every single individual that is in the Coast Guard at some point goes through my district in Cape May. How does CISA coordinate with the Coast Guard to promote cybersecurity of maritime critical infrastructure? That is for Christopher Krebs.

Mr. KREBS. Yes, sir. Thank you for that question. The last administration issued a National maritime cybersecurity strategy last year. CISA coordinates very closely with the Coast Guard. In fact, Coast Guard service members actually sit with CISA and actually support our Hunt and Incident Response mission.

It is a very collaborative relationship between CISA and the Coast Guard. The relationship in terms of going out and working in the maritime sector at ports, on facilities, and then coastwise is a budding relationship that I would suggest, again, we need to put more resources against.

Mr. VAN DREW. OK. Which makes sense. But it has been fruitful to this point.

Mr. KREBS. Yes, sir, I think so. If I could just make one example based on what Sue Gordon, Ms. Gordon, mentioned earlier about our election security efforts. What worked so well there is that we brought all of the relevant stakeholders together and created almost, as I called it, a mini CISA. So we had all elements of CISA, with our stakeholders, really intensely focused on the mission.

But elections is just one of the National critical functions. We have to identify that top slice, 15 to 20 top National critical functions, highest risk, and create little mini CISAs around each and every one of those functions. We can make rapid, rapid progress in securing those sectors and functions if we take that approach.

Mr. VAN DREW. Good. Thank you.

For Michael Daniel, the recent incident at the Florida water treatment facility shows how vulnerable we are to attacks from hackers. What can and should be done to prepare for and combat the cyber threat to critical infrastructure?

Mr. DANIEL. Well, thank you, Congressman. I think that when you really think about it, there is kind-of, I would say, 3 things that we need to be doing, one of which is very much hardening those systems and raising the level of cybersecurity across the ecosystem. That is everything from really thinking about cybersecurity in different ways that I was talking about, but also employing things like the NIST Cybersecurity Framework to do that risk management to those systems. But then also going on the offense to find those adversaries and to disrupt them and to prevent them from doing what they are trying to do.

Then also being able to know that sometimes both of those things will fail and know that we need to be ready to respond and recover. This is where what Dmitri was talking about, those time-based metrics of how we need to get better at responding rapidly, identifying the malicious activity, containing it, and then removing it from those networks, so that we can minimize the amount of damage that we take.

I think—and we need to be doing that, as Chris was just saying, across, thinking about that from a National, critical function perspective about what is important to our economy and to the functioning of this country as a whole. Sometimes that will not be obvious from the outside, and it requires thought and analysis to arrive at some of those critical functions and where they are vulnerable.

Mr. VAN DREW. Thank you. I appreciate all, and I thank you for your work.

I yield back.

Chairman THOMPSON. Thank you.

The Chair recognizes the gentlelady from Michigan, Ms. Slotkin, for 5 minutes.

The Chair will recognize the gentleman from Missouri for 5 minutes, Mr. Cleaver.

Mr. CLEAVER. Thank you, Mr. Chairman.

You know, I am going to express appreciation, first of all, for you doing this hearing because I think it is right on time. I thank all of our very knowledgeable witnesses and articulate witnesses.

I want to thank you, Mr. Krebs, for your integrity. It is good for the whole country to see what integrity looks like.

You know, my concern right now is global versus domestic terrorism. You know, we are told by the FBI that the greatest threats to our country are coming from within, which one of the witnesses has already talked about being one of the goals of Russia. So I am concerned, frankly, about whether or not there is enough intelligence or data that would allow us to know whether the domestic threats coming from various groups around the country—around the country are also a cyber threat to the country.

So, Mr. Krebs—I would like to hear all of our witnesses just briefly hit on that, the domestic threat and whether I am overthinking it to believe that that could eventually become one of the greatest threats to us, if not already the greatest threat.

Mr. KREBS. Thank you, sir, for that question. It is not in the top, you know, 5, probably, of cyber threats that I am concerned about right now. I would actually put at the top of my list ransomware, targeting State and local and small and medium businesses.

Part of the reason why domestic cyber threats, from a pure sophistication perspective, is that they are not given time to root. That is because law enforcement, the FBI, has greater authorities here to actually go and grab the bad guy and do a perp walk, which is different from how some of those ransomware gangs that operate in Russia and Eastern Europe and elsewhere. The law enforcement community cannot always reach out and touch them.

So that is a distinct deterrence advantage that we have here at home to push back on larger-scale cyber activity. Yes, there is always going to be identity fraud and, you know, lower-level criminal activity, but really truly National security- and economic security impact-level of cyber threat domestic, I don't believe that is an immediate threat.

Mr. CLEAVER. Do the other witnesses pretty much agree with that or do you have anything to add?

Ms. GORDON. Congressman Cleaver, I will just add a little too. I think Chris is right, but I do think in terms of National security threats to the Nation, our own extremism is problematic. They may not have any particular advantage in cyber right now, but the tools they would need are not elusive. As I mentioned before, there are foreign actors who may be very willing to provide either their expertise or their resources.

I absolutely believe that there is hope in what Chris said about our natural advantages dealing with our problems domestically, but this is a concerning threat and it can use cyber capabilities in the same way some of our other adversaries can.

Mr. CLEAVER. Well, I don't want my time to run out, so I will do this very quickly. I have read that 95 percent of cybersecurity breaches are the result of human error, and so—and this may be horrible-sounding. I genuinely don't mean for it to sound this way—but in hearing many of the individuals who have been arrested for the January 6 attempted coup d'etat, you know, and maybe they were good at science and just not good at other things, because none of them have come across, you know, like, you know, brain surgeons. I don't know what else to say.

So I am just wondering, if we got 95 percent from human error, which is not very much, frankly, you know, in terms of how far it could go, I am assuming we only have—it is close to zero—zero from them. Mr. Chairman, I will listen to the answer and I am out. Thank you for the indulgence.

Mr. KREBS. Sir, I think that is a fair point that I would expand upon my earlier answers, that, yes, there is the potential for insider threat, disgruntled employees. When you think about what happened down in Florida earlier this week, it is very likely that that was, in fact, a disgruntled employee that conducted that operation. I think we would leave the investigation to finalize that.

That is why it is so important to have visibility over the network, controls in place. To Dmitri's point, you know, if you are planning for a broader, you know, assumption of breach perspective, you will be able to defend against a range of different actors.

Mr. CLEAVER. Thank you, Mr. Chairman.

Mr. KREBS. But that is a good clarifying point, sir.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from Iowa, Mrs. Miller-Meeks, for 5 minutes.

Mrs. MILLER-MEEKS. Thank you so much, Mr. Chair, Ranking Member Katko, and all of the witnesses who are presenting here today. Extraordinarily important topic, and I appreciate the ability to both listen and learn.

Before coming to Washington at the beginning of this year, I served as a State senator in my home State of Iowa. Last year, the Iowa legislature recognized the importance of cybersecurity, and we voted to increase funding for cybersecurity initiatives to our DCI.

All of you in your testimony today have recognized and brought up and addressed the importance of a combined effort, not solely a Government effort, but also State and private.

Ms. Gordon, in your testimony, you discussed the importance of cybersecurity at the State and the private industry level, and I am wondering what Federal resources currently exist to help States that want to strengthen their cybersecurity.

Ms. GORDON. So I think what CISA has done and what Chris has done in the context of election security has given a great blueprint for State and local to be able to use their resources but the wisdom of the Federal to put those 2 things together.

I think there is probably more we can do. One of the thoughts that I have is, as the intelligence community got more and more securing itself against this, one of the great advantages we had was when we went to cloud computing and away from all the small infrastructure that is really hard to keep up with and patch.

I think there is an interesting question to be said with whether there is some ability to provide for less advantaged localities, some sort of access to broader cloud computing that could offer that advantage in the same way. Thank you very much.

Mrs. MILLER-MEEKS. Thank you so much.

You all had mentioned seeing boundaries and silos, and, Mr. Krebs, you had mentioned—talking about ransomware. We certainly have had ransomware attacks in Iowa and, again, put legislation to deal with that. So if a State is working to prevent ransomware attacks or if they are currently experiencing a ransomware attack, what assistance or guidance is the State able to receive from the Federal Government, should the Federal Government provide assistance, and what does the process look like for a State seeking guidance?

Mr. KREBS. Yes, ma'am. Thank you for that. Ransomware is a—I think we are on the verge of a global emergency. The rate at which we are seeing State and local governments get hit is truly frightening.

CISA, over the last 2 years, working with the FBI and other law enforcement partners, has kicked off a ransomware awareness campaign. I think we actually need to do more, though. I think we need to have a joint public-private sector initiative, like the Institute of Security and Technology's Ransomware Task Force, where everyone comes together across technology sector and Government to make things better.

But to start, we have to improve defenses. State and local governments simply cannot protect themselves. There is too much legacy infrastructure out there, still too much reliance on single-factor authentication like passwords.

We have to make that generational leap in technology. The Federal Government has to help here. I think we have to either match what the Homeland Security grant programs have done for counterterrorism or we have to go even further. I think with COVID, remote work force, digital transformation, in a subsequent funding stimulus bill, I think we have an opportunity to put a lot of really meaningful, impactful resources into the hands of State and locals, to upgrade their systems, to improve citizen services, and ultimately secure against this on-going scourge of ransomware.

Mrs. MILLER-MEEKS. Mr. Daniel, would you have anything to add to that?

Mr. DANIEL. I think it is absolutely right that State and local governments, not only in dealing with ransomware, which I completely agree with Chris, that we—I think, you know, that has moved into the realm of National security and public health and safety threat, that we very much have to deal with. We need to provide a lot more resources to State and local governments for them to both defend themselves and to remediate and have options other than paying the ransom if they do get hit with ransomware. They really need to have that option.

But I also think we need to be looking at how we work with State and local governments to be ready to respond to other kinds of disruptive and potentially destructive attacks to our critical infrastructure. There is some work being done by a group called the New York Cyber Task Force that will be coming out later this spring that will look exactly at that topic.

Mrs. MILLER-MEEKS. Great. Thank you so much. I appreciate all of the testimony from the witnesses, and again, very important topic and very timely.

Thank you, Mr. Chair. I yield back my time.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from New York for 5 minutes, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. Let me thank our witnesses for their expert testimony here today.

Let me just say that the Federal Government is really making up for lost time.

I am sorry, Mr. Chairman, my—somehow I—my technology just failed on me. Would you give me 1 minute?

Chairman THOMPSON. We can hear you loud and clear.

Ms. CLARKE. OK. One moment, sir.

Chairman THOMPSON. We can actually hear and see you.

Ms. CLARKE. OK, very well. Just I am trying to actually return to my questions.

I am sorry, Mr. Chairman. I just—my technology is failing me today.

Chairman THOMPSON. Well, I tell you, if the gentlelady from Nevada will step in, we will come back to you.

Ms. CLARKE. That will be fine, Mr. Chairman.

Chairman THOMPSON. The Chair recognizes the gentlelady from Nevada for 5 minutes, Ms. Titus.

Ms. TITUS. Thank you, Mr. Chairman. I could never fill the shoes of my predecessor there, but thank you for letting me go ahead.

I would just like to shift the attention a little to work force needs. If you covered this when I was in T&I markup, I apologize, but I don't think so.

You know, this is one of those areas where the need outraces the supply in the case of people who are qualified to do this work. There was a study that was released last fall that showed that 880,000 professionals work in cybersecurity, but there is a work force gap of about 350,000. I know here in Nevada, we have approximately 2,700 unfilled cybersecurity jobs.

We are seeing more colleges and universities get involved in this kind of training. In fact, UNLV has a new partnership with what they call HackerU to start training some of these folks and fill in this skills gap.

I wonder if our panelists, starting with Mr. Krebs, could address this shortage and what we might be able to do to help fill it at the Federal Government assistance or encouragement or information that will help us find the people who can do these very important jobs that y'all have been discussing.

Mr. KREBS. Yes, ma'am. Thank you for the question. I think about that as a today problem as well as a tomorrow problem. Starting with the tomorrow problem, we have to continue increasing digital literacy and supporting K–12 education, STEM education, including thinking in security principles.

You know, I have 5 kids. I have talked about this in numerous hearings before. In the public school system, I see that they need more science, technology, engineering, mathematics education.

To the today problem, though, I think the people are there, the potential work force is there. We just need to make it more accessible. I do think, though, that the pandemic and the remote work force has actually given us—or at least a glimmer of hope.

Traditionally, in the information security community, there are annual conferences all over the place, all over the country. They cost money to attend, to fly to, all those things. Most of them have gone on-line, and many of them have been free and open to the public. That has been a significant barrier reduction to opening up access to education, training, and awareness. So we need to keep that going.

We also need to, through the Federal Government, provide pathways to cybersecurity positions. I know at CISA, we were trying to expand our recent graduates and current students internships and hiring. That is a—working with the Scholarship for Service Program, we can actually help augment tuition assistance. That, to me, is a great opportunity to bring people in to the government, train them up for 3 or 4 years, and then give them the opportunity to go back out into the private sector.

That actually gives us a couple advantages. One is that we have a degree of standardized training, but we also now at CISA, we have an alumni network. So if they go out into the critical infrastructure community, they know how to work with CISA, and they have actually a preference to work with CISA. Those are just a couple examples right now that I think that we can do more of.

Ms. TITUS. I would think this would be an area where veterans might play a role, that we might take advantage of some of their skills and knowledge.

Mr. KREBS. Yes, ma'am. In fact, CISA hired a significant number of veterans, but also there are private-sector programs. There is the Cyber Talent Initiative, the CTI, that a number of private-sector corporations have participated in, as well as Microsoft has a dedicated military veteran program, where they train up over a course of weeks and offer interview for positions those that finish the program.

Ms. TITUS. Well, thank you.

Anybody else want to add to that?

Ms. GORDON. Yes. Representative Titus, great question. To add on 2 ends of what Chris shared, totally agree with the educational aspect, starting in K–12.

I also think we need to add to that just the realities of operating in a digital world. So remember the D.A.R.E. Program we had countering drugs in the schools? Where is that, to have people understand what is happening to them in a connected world and the social responsibility?

So I think there is a piece of that education of—kind-of like ethics of being in and protecting yourself in a digital environment that would be a good add.

The sec is, I think we are missing at the top end of organization, so not just the workers but the top end, a digital literacy that allows leaders and decision makers to understand what is at risk and what their responsibility to devote resources.

So instead of just leaving it to their technical teams, I think we need an educational effort focused at leaders. So I can bracket the education.

Then I think there is a real opportunity, as the Federal Government doesn't just throw knowledge and requirements of the transom to localities, if we start engaging with local and regional activities to bring capability in and spawn regional capability, that is going to be an attractant for developing the jobs that will keep people locally, not just suck them all in to a Federal, centralized thing. So I think there are some really good opportunities for us to incentivize those sets of things.

Ms. TITUS. Well, thank you. I would like to work with you on that, and I appreciate it.

Thank you, Mr. Chairman, and I will yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from Georgia for 5 minutes, Mr. Clyde.

Mr. CLYDE. Thank you, Mr. Chairman, for having this very important hearing.

You know, we discussed already about the attempt on the water supply facility in Florida, and then also in March 2018, the Trump administration accused Russia of orchestrating a series of cyber attacks that targeted the U.S. power grid.

My question for Mr. Krebs is, could you estimate how many times a day or estimate the scope of how many attempts bad actors try when they attempt to breach U.S. critical infrastructure networks?

Mr. KREBS. My dog upstairs is trying to answer the question right now. I apologize for that.

Mr. CLYDE. Would you like me to repeat it?

Mr. KREBS. Would you mind coming back to me?

Mr. CLYDE. Sure, sure, sure, no problem. Could you estimate how many times a day a bad actor attempts to breach a U.S. critical infrastructure network in our country? Could you give us an idea of the scope?

Mr. KREBS. I will try over the dog's barking. Clearly, somebody that is walking dogs on the street.

It is—when I say try, it is actually really hard to make any sort of meaningful quantification. There are both automated tools that run on a regular basis looking for vulnerable systems connected to the internet, and then there are focused, human-powered initiatives or efforts. We are talking—I would even, I would hesitate, millions and millions and millions. I mean, we are talking just massive numbers of scanning attempts on a regular basis. That is just the noise of the internet. The more sophisticated, capable efforts are going to be fewer in number, going after the bigger fish to catch.

Mr. CLYDE. OK. Thank you very much. I appreciate that.

My next question is to Mr. Alperovitch. You mentioned in your opening statement ransomware. So the best way to reduce the threat of an adversary, in my opinion, is to remove the incentive. You know, as a small businessman, I called it the economic sword.

I understand that bitcoin is a primary way that many ransomware bad actors want to get paid. So could you tell me, is there a way to minimize or eliminate simply the ransomware bad actors' ability to get paid?

Mr. ALPEROVITCH. Congressman, that is an excellent question. It is no coincidence that the explosion of these ransomware attacks occurred about 10 years ago when we saw the emergence of these cryptocurrency platforms like Bitcoin, which enabled these criminal actors to collect ransom anonymously.

So, previously, before the emergence of cryptocurrency, to get a ransom, you literally had to provide the wire instructions for your bank to get the ransom or a place where someone could send you a check. As you can imagine, law enforcement could easily track that down and get that criminal arrested.

Mr. CLYDE. Exactly.

Mr. ALPEROVITCH. With cryptocurrency, they could do it anonymously.

So I believe that de-anonymizing these types of transactions through know-your-customer regulations that the Treasury Department can implement can absolutely take the oxygen out of this ransomware fire and totally disrupt their business ecosystem.

I think Congress should absolutely be looking at that. I know Treasury has put out regulations back in December, proposed regulations, in this sphere. I think Congress should be supportive of that.

Mr. CLYDE. So you think that would be a very important aspect of the cybersecurity solution.

Mr. ALPEROVITCH. I think that can totally disrupt the business ecosystem for these criminal operations and can significantly dampen the number of attacks we are seeing against our small businesses and hospitals and the like.

Mr. CLYDE. Right. OK. Thank you very much. I appreciate that.

Mr. Chairman, with that, I yield back.

Chairman THOMPSON. Thank you very much.

The gentleman yields back.

The Chair recognizes the gentlelady from New York, Ms. Clarke, for 5 minutes.

Ms. CLARKE. Thank you, Mr. Chairman. I think I have got it this time. I want to once again thank our expert witnesses.

I think what we have heard today is that in the 21st Century the line between the physical world and the digital world just keeps growing slimmer. When it comes to homeland security, malware can disrupt our critical infrastructure as effectively as a bomb, and hacked data can be a more effective tool of espionage than a human source.

There is a reason that this is one of the very first hearings that we have held this Congress. It is because cyber threats are no longer a risk for tomorrow. Our day of reckoning has arrived. The SolarWinds breach was far from an isolated incident. From the OPM hack to relentless attacks against the private sector, IP networks are the new battlefields and have been for some time.

As Chairwoman of the Cybersecurity Subcommittee, I believe we are overdue to reimagine DHS and make it reflect this reality. It is time to stop spending money on walls that divide us and more money on firewalls that protect us.

Fortunately, President Biden has made it clear from the start that he is taking a different approach, nominating seasoned experts to National security positions across the Federal Government and the White House who recognize the need for a whole-of-Government approach to cybersecurity.

I look forward to working with him to defend American networks and not just at the Federal level but also, as has been stated by numerous of my colleagues, at the State and local level and in the private sector. Nothing less than our National security depends on it.

With that, I want to turn to my questions.

As a Nation, we have no way of knowing how much of our critical infrastructure has been compromised by hostile nation-states like Russia through cyber hacks like SolarWinds unless individual companies decide to come forward voluntarily.

As Chairwoman of the Cybersecurity Committee, I have been following the conversation about requiring critical infrastructure owners and operators to report when they experience major cybersecurity incidents, as the Cyber Solarium Commission recommended last year.

So, Mr. Krebs, would you have been better equipped to carry out our mission as CISA director if you had access to detailed, thorough data on successful cyber intrusions targeting critical infrastructure?

Mr. KREBS. Yes, ma'am. Thank you for that question.

I certainly think it would be helpful to have, or at least in terms of significant cyber compromises, an after-action process that is, you know, almost a no-fault exercise and not constrained by litigation concerns and things of that nature, where you could actually get to the root cause of what happened and then share findings, even maybe in an unattributed way, with the rest of the private sector.

We have to learn from our past mistakes, or we are going to keep repeating them. We also have to really, really emphasize knowledge transfer from the haves that have invested to the have-nots that are either yet to invest or, you know, beginning to realize where they fit in the ecosystem and they want to be better corporate citizens and understand their responsibilities to the economy.

Ms. CLARKE. Thank you.

Mr. Daniel, you mentioned the need to create standards of care for private-sector critical infrastructure. Can you elaborate upon what those standards should look like?

Mr. DANIEL. Yes. Thank you, Representative Clarke.

I think those standards are going to vary depending on the industry, depending on the size of the company, depending on what functions it performs and their criticality to the overall infrastructure.

But we have these standards in many other kinds of areas, like safety and how you treat customer data and things like that in other areas. What we need to start doing is extending that into cybersecurity so that companies know what their responsibilities are.

That will also help cut down on that litigation that Chris just referenced. Because if they know that they are reaching that level of standard of care and they are exercising that as due diligence, then they won't be as worried about reporting and communicating with the Government.

Ms. CLARKE. Thank you.

Mr. Krebs, I just want to take the opportunity to thank you for doing the right thing during your tenure at CISA and refuting Donald Trump's lies and disinformation about the 2020 election.

Do you believe you were fired because you created the "Rumor Control" blog and made public statements affirming the integrity of the election?

Mr. KREBS. Thank you for the question, ma'am, and thank you for your kind words. I, you know, can't attribute any specific motivation to my firing other than what was in the 2 tweets and the fact that the President seemed to believe that the statement that it was a secure election was, in fact, inaccurate.

Ms. CLARKE. Well, thank you, Mr. Krebs.

Mr. Chairman, I yield back. Thank you very much.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from Texas for 5 minutes, Mr. Pfluger.

Mr. PFLUGER. Mr. Chairman, thank you very much for this hearing, and Mr. Ranking Member. I appreciate the opportunity.

For the witnesses, thank you for taking the time in a very important time.

You know, cybersecurity and the cyber world affect every single American. As somebody who spent 20 years in the military flying the most advanced piece of weaponry, we don't fight our wars without cyber help, without, as has been mentioned, the comparative advantage.

What I would like to kind-of focus on right now is the word "competitive" advantage.

Ms. Gordon, I appreciated hearing your thoughts on how there is not just one solution, you know, for us as a country to remain secure in the cyber world, and it is going to take State and local, international partners, our Federal Government, private industry. These partnerships are extremely important.

In my district, Angelo State University is seeking to become a cyber center of excellence. This is a Hispanic-serving institution, in academic year 2021 and 2022 should be a minority-serving institution. We are in a rural area. So the uniqueness of Angelo State University in the seeking of being a cyber center of excellence is one of those pieces of the solution and that layered defense, that model.

When it comes to competitive advantages, just like the gentlelady from Nevada, I am worried about our education system and the lack of preparing. As somebody who graduated from a military academy, studying military tactics is extremely important.

Ms. Gordon, I would like to hear your thoughts on what can be done at the university level to really empower these universities and higher education to focus on STEM. As one report shows, our students in math and science are ranked in the bottom 50 percentile, you know, for STEM education. I know this has been mentioned, but what can we do to empower these universities to continue to improve the quality of education?

Ms. Gordon, to you.

Ms. GORDON. Well, thank you, Congressman. That is a great question.

I love hearing what is going on at your university. A good friend of mine is Dr. Heather Wilson at UTEP, and she makes the exact same point about the remarkable opportunity we have at several institutions if we put our focus, give them some resources, inspire them with need. I think we have the raw material; we just have to apply it to the problem.

So I think there are 3 things you need to do—we need to do.

No. 1, I think we are already starting to do it, and that is to talk about these things as Nationally important, not just a question of economics, not just something elusive, but actually how important this is to our Nation. So, be expansive about the threats we have, the threats to and through information, and what can be done. Let's get people wanting to participate in that.

No. 2, I think we see a whole bunch of private-sector companies who are recognizing their social responsibility. Let's do some things to inspire them to continue to invest not only in products and services but in the humans that are going to make them run.

No. 3, I think that, as the Federal Government, as you all consider what can be done to couple National wherewithal to local action—and with what we have learned about COVID, about distance learning, I think we have the opportunity to not have to have everyone move to one place to participate but you can participate where you are.

I think the United States has tremendous advantage. Open systems, competitiveness, innovation—those are all watchwords. Get it applied to this problem, and I think we will be all right.

Mr. PFLUGER. Thank you, Ms. Gordon.

Mr. Alperovitch, quickly in the remaining time, when it comes to critical infrastructure, critical vulnerabilities, I am very worried about not only the water system, as we have heard, but also the delivery of our energy—in my case, oil and natural gas and the delivery systems.

How do we harden those systems? How do we protect those systems?

Mr. ALPEROVITCH. I think we absolutely have to focus on this. I am actually on the board of a company called Dragos that focuses on these very issues.

I think that, when you look at the oil sector, you look at our manufacturing sector, frankly, industrial control systems are very vulnerable. We have not focused on protecting those systems.

We need a different approach to the one that protects the enterprise networks, sort of our laptops and servers, to the way we protect our systems that interact with the physical world, and this absolutely needs to be a Government focus, sir.

Mr. PFLUGER. Thank you.

Again, to all of you, thank you for thinking outside of the box. This is a huge issue.

Mr. Chairman, Ranking Member, thanks for the time to focus on something that will keep all Americans safe, especially those things that are providing services and educating our children.

With that, I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from Nevada—I am sorry—New Jersey for 5 minutes, Mrs. Watson Coleman.

Mrs. WATSON COLEMAN. Thank you, Mr. Chairman. Thank you for having this hearing.

To each of the individuals who have participated, thank you for the information you shared. I am learning a lot. I have a lot to digest. This is really quite extensive, quite concerning on so many different levels, and quite new to me, actually.

Mr. Krebs, let me just say to you also, I thank you for your integrity as well.

Mr. Krebs, let me ask you the first question. There was a proposal that was offered today to make the CISA director the chief information officer or the chief of the information sharing for all of the agencies. Do you think that that is a good idea?

Mr. KREBS. Yes, ma'am. There is a Federal chief information security officer that resides within the Office of Management and Budget. That function really is a policy-setting role, and then CISA is in a policy-enforcement role.

I think if we can expand the resources, capabilities, and ability to actually—well, frankly, get agencies to improve their security through resources and capabilities, then I think we are going to be in a much better place.

Mrs. WATSON COLEMAN. So do we still have an issue with agencies feeling very proprietary over information in their jurisdiction and not sharing it in an interagency capacity?

Mr. KREBS. I think there are a couple issues here.

One is that privity of contract between agencies and their vendors prohibit CISA, for instance, from getting information on incidents. In some cases, particularly in some of the recent hacks, I had heard—because they happened after I left—that when CISA tried to ask a vendor for information, the vendor would say, "I am sorry, I can't give you that, that is up to the agency to give you that," and then the agencies don't always turn that over. So we need to change that and put CISA as a part of the contractual relationship.

But any way you cut it, when an agency is responsible for their networks, they are always going to have a sense of ownership and proprietary responsibility. We have to change that model. We have to make it easier for them, where they don't have to hire, where they don't have to invest their own, where it is already provided for and it is a turnkey solution. That should free up the chief information officers to focus more on citizen services and actually delivering value to the American people.

Mrs. WATSON COLEMAN. OK. Thank you.

I think this is to Mr. Alperovitch.

You talk about accelerating the detection, investigation, and mitigation by increasing the metrics. Is anything needed in that regard other than additional resources? Is the capability for the agencies to do that already in existence? Is that a resource issue?

Mr. ALPEROVITCH. I think it is a resource issue, but it is also policy issue.

I think Congress should absolutely require agencies to start tracking those metrics every single year, report them to CISA, report them to OMB, report them to oversight committees, so that you actually would have the information needed to understand how well are agencies doing in detecting and investigating and responding to sophisticated adversaries and what more needs to be done.

Also borrow from examples of agencies that are doing really well and trying to make sure that everyone else adopts those types of strategies broadly.

Mrs. WATSON COLEMAN. Uh-huh. Thank you very much.

Mr. Daniel, can you walk the committee through the problems with the security patches? Those are the updates that you see from time to time. Can you talk to us about the frequency of them and whether or not this is the best way to have this take place?

Mr. DANIEL. Well, certainly.

So all software comes with vulnerabilities and bugs and errors in it. It is just the nature of writing software code. So companies that manufacture and write that code are going to have to update it. So we certainly want the ability to update and manage that code, and we want to do that in a fashion that is as easy for the customers to do that as possible.

One of the problems that we have, though, is that there are hundreds of these patches that come out very frequently. Different companies and different providers are providing these patches on a very regular basis. So the challenge for a company is to actually figure out how to implement those patches and do so in a way that does not disrupt their business operations.

So patch management and managing those updates to your software is actually a very critical problem for many enterprises. We need to work toward making that patch management and software management as easy and as transparent as possible.

Mrs. WATSON COLEMAN. Can a trickster encourage you to do something that will have a negative impact on your device, and you are thinking that is the company telling you to update it? Can a hackster or a trickster or whatever do that to you? If so, is there something that we should be doing, looking at it from a Government perspective, as a standard, as a modus operandi?

Mr. DANIEL. Well, certainly, Representative, there is always a possibility that an actor will try to trick you, to try to scam you into clicking a link that takes you to someplace that is not legitimate—that is called phishing—that will try to misdirect you and get you to download malicious software. But what I would say is that, you know, relying on trusted vendors that you know and are relying on the normal update process, that is the best way to go.

Even though we know that there are opportunities, like what happened to SolarWinds, for that to be compromised, that is far from the most common route, and it is much more common for a scammer to try to phish you or trick you in that manner. So I still think it is critically important that companies and individuals and organizations regularly patch and update their software.

Mrs. WATSON COLEMAN. Thank you.

Thank you, Mr. Chairman. I have a lot of other questions. I know my time is up. I yield back.

You are muted, Mr. Chairman.

Chairman THOMPSON. That is technology for you. It said I was not.

But, Mr. LaTurner, if you can hear me——

Mr. LATURNER. I can.

Chairman THOMPSON [continuing]. I will recognize you for 5 minutes. Thank you.

Mr. LATURNER. Thank you, Mr. Chairman. I appreciate it. I appreciate you putting this panel together.

I have appreciated all of your testimony.

I want to focus primarily on ransomware and specifically on its impact on small and medium-size businesses. This is a major issue that people are struggling with. I could name several just in recent history of businesses that have been dealing with this. The ransom was huge sums of money. They felt like there were almost no resources, no response, no help—a very powerless feeling about how to deal with this.

So, clearly, we have so much work to do at the Federal, State, and local level with governmental institutions. But, specifically, Mr. Alperovitch, you talk about passing breach notification laws, which make some sense. What else can we do to partner with and be a better resource to these small and medium-size businesses that don't have the resources and really feel helpless in the environment that we are in right now?

Mr. ALPEROVITCH. Thank you, Congressman LaTurner. I think this is a great question, because we really have the haves and the have-nots in cyber today, where the big organizations, the Fortune 500 companies, are doing just fine, spending resources and trying to defend themselves against the sophisticated attacks, but the same criminals, the same nation-state actors that are going after them are also going after the small and medium businesses that really have no capacity, no talent to defend themselves against these sorts of issues.

We need to look very seriously at this problem. I think the right way to think about this for small and medium business is to try to outsource that capability to a cloud provider or another manner of service provider that can be responsible for their defense.

But, as I mentioned previously in my testimony, I think in ransomware in particular, which is the No. 1 plague that is hitting small businesses, as you mentioned, sir, every single day, we need to go after these criminals, we need to shut down the ways that they can collect these payments anonymously, and prosecute them to the full extent of the law. That is the only way that we can get a handle on this problem.

Mr. LATURNER. I appreciate that answer.

Mr. Krebs, you talk in your testimony—talk about disrupting the business model, which clearly we need to do. So if you would talk about that just a little bit.

But then focus more, if you could, on the section where you talk about more aggressive action against ransomware actors. You say you are not suggesting extrajudicial kinetic actions against ransomware gangs, but authorities available to law enforcement and military should be on the table.

So talk a little bit about the business model disruption and then about that, if you don't mind.

Mr. KREBS. Yes, sir. Thank you.

On the disrupting the business model, I mean, the simple fact right now is that ransomware is a business, and business is good. I have said that before; I said it in my testimony.

Mr. LATURNER. Yes.

Mr. KREBS. It is simply too easy for criminals to extract value. As Dmitri mentioned, it is primarily driven by the ubiquity of cryptocurrencies and the ability to anonymously transact illicit activities.

So I think, in part, what Treasury did last year with the OFAC notice that it is, in fact, a possible sanctions violation to pay ransom to a sanctioned entity, like Ryuk, the Ryuk gang, that should have a chilling effect.

I think there are other mechanisms that we can take a harder look at. If I said—I meant—I think I said last year.

So there are some other things—you know, how we facilitate the payment beyond cryptocurrency. Should it be legal to pay ransoms? When you think about terrorism and ransom of terrorists, that is typically unlawful. So I think we need to have a policy conversation about whether it is in fact legal to pay criminal gangs a ransom.

So, to your last point of additional action, we have already seen a couple cases over the last year, most recently in the last month or so, targeted action by law enforcement against the Emotet malware infrastructure. Last year, we saw Microsoft go after Trickbot and their infrastructure.

We need to have coordinated activities—law enforcement, informed by the intelligence community—to go after the actual infrastructure and the people that are conducting these activities.

Again, to the extent we can put hands on them and arrest them, that is a good thing. That takes an exceptional length of time. So, if we can take down the processes and the infrastructure by which they conduct these activities, that has to hold the ground until we can lock them up.

Mr. LaTurner. Thank you, Mr. Krebs, Mr. Alperovitch, and all the conferees.

Thank you, Mr. Chairman. I yield back.

Chairman Thompson. Thank you very much.

The Chair recognizes the gentlelady from California for 5 minutes, Ms. Barragán.

Ms. Barragán. Thank you, Mr. Chairman.

Thank you to our witnesses.

In 2018, the maritime sector saw 2 massive ransomware and malware attacks on the maritime industry, impacting the ports of Barcelona, Spain, and San Diego, California.

These attacks seem to be focused and potentially made increasingly easier as the convergence of information technology, or IT, and operational technology, OT, systems become more integrated. According to varying industry reports, the number of maritime-focused cyber threats and incidents have risen by as much as 900 percent.

These cyber attacks have great economic impact to maritime ports, especially those that are integrated into our transportation networks. These attacks can cause reputational harm, financial loss, and even physical damage, especially in the cases of compromised dockside equipment or vessel.

The Port of Los Angeles, in my district, has invested to create a cybersecurity operation center and has a dedicated cybersecurity team whose role is to protect the cyber aspects of the port. To create additional centers and resources will require investment by Federal, State, local, and private industry partners. Without such investments, this will greatly cripple and potentially hinder American supply chains and response efforts to catastrophic events like the COVID pandemic.

Mr. Krebs, if I can come back to you on this, what can ports be doing right now to ensure their maritime cybersecurity preparedness?

Mr. KREBS. Yes, ma'am. Thank you for that.

So, partly, they can work with companies, like Dmitri mentioned, Dragos and some other vendors, that can help them understand what their environment looks like, the controls they need to put in place to secure their systems, to lock them down, to disconnect if at all possible. But that is not always possible, because you need, a lot of times, remote access.

The bigger issue, though, here is that, you know, we have to have this balance of stopping the adversary as best we can alongside improving defenses. So it is not a, you know, just invest in defenses, and it is not just an invest in offense; it has to be a more equitable balance.

I think, historically, we have over-invested or, at least, principally invested in offense, and we have to ramp up defensive investments going forward.

Ms. BARRAGÁN. So, just to follow up on that, should operation centers like the one at the Port of Los Angeles be considered for Federal grant funding, such as, like, State homeland security grant programs, emergency preparedness grant programs?

Mr. KREBS. Yes, ma'am. I know that L.A. city cyber fusion or cyber intelligence center was funded by Federal grant, and I thought the port center was as well. But I think that is a fantastic innovation, in terms of pulling all the stakeholders together enterprise-wide to be able to manage risk to environments.

Ms. BARRAGÁN. Great. Thank you very much for that.

It is clear from recent events that the United States must improve its ability to respond and recover from a significant cyber event. Part of that effort must focus on partnering with private-sector owners and operators of critical infrastructure. In the aftermath of a cyber event targeting the electric grid, for example, there is a real question about whether there are sufficient laws in place to allow a grid operator to cooperate with the Federal Government to prioritize power restoration to a critical facility such as a military base.

Last year's U.S. Cyberspace Solarium Commission report recommends that, to address this concern, Congress should pass a law specifying that entities taking or refraining from taking action at the direction of any agency head should be insulated from legal liability.

Mr. Krebs, would this type of Congressional action help reduce barriers to cooperation between the Federal Government and the private sector during a cyber event? Are there any steps that you recommend Congress should take?

Mr. KREBS. So, as I recall, that recommendation was based on the Federal Government asking a company, for instance, to take certain action or allow an adversary to continue their activities for observation or for their monitoring purposes, and that could result in downstream damages to customers or people.

So I think that is a balance of equities, of trying to understand and stop the adversary versus protection. So I think that is a nuanced approach. I think we have to be very careful with that approach. But I think, again, going forward, we have to have a better understanding of where the riskiest bits of our Nation's economy, our infrastructure are.

One of the aspects of the Solarium that I really liked was the continuity-of-the-economy effort. That was built, in part, on the National critical function work out of the National Risk Management Center.

We don't have an in-depth enough understanding of how our economy truly works. Until we get there, we are not going to be able to invest smartly enough in terms of how we are organizing collectively for security.

Ms. BARRAGÁN. Great. Thank you for that.

With that, Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentleman from Michigan, Mr. Meijer, for 5 minutes.

Mr. MEIJER. Thank you, Chairman and Ranking Member.

Thank you to all our distinguished guests who are on the call right now.

I want to touch upon briefly some of the conversations that we have been having around cyber hygiene and, specifically, an analogy that came up in some of the prepared statements and that I think is just broadly in the ether around a cyber Pearl Harbor.

Now, I guess my specific question—and I would like if Mr. Krebs could look at this first. When I think of the analogy of cyber Pearl Harbor, you know, we think of just kind of, like, a massive attack. But, you know, if you are going to face an attack, you know, our military is able to prepare itself—you can have radar installations, you can send out advanced forces, you can figure out how to preempt.

But I think it was Mr. Daniel who mentioned that we are really facing a panoply of problems, right? We have everything from nation-states to criminal enterprises, the line between which can oftentimes be blurred, to individuals, you know, who may be domestic and working in some capacity.

I guess the analogy that I have just been working with and I would love to get some reactions on is more of, how do we preempt a cyber Chicago fire? You know, after the Chicago fire, you had changes in building codes, you had, you know, investments in fire departments, everything from the installation of sprinkler systems to, later, smoke detectors.

You know, although a cyber attack is obviously much more intentional, you know, we saw with the breach at the Oldsmar water facility, you know, that it was an outdated version of TeamViewer that was left on the computers—you know, obviously an example of just very poor cyber hygiene and a failure to have basic defenses.

You know, how can we change our thinking on the resiliency side to not just be focused on the catastrophic but all of the ways in which, short of catastrophe, we can incrementally be increasing our overall resiliency?

I don't know, Mr. Krebs, I would love for you to touch upon that and just within the idea of CISA as running point within all of those nodes.

Mr. KREBS. So I think this is an interesting question, and it is one that I think has probably been asked in hearings like this now for going on 10 years-plus, you know, when are we going to see the cyber Pearl Harbor. I am not sure we are ever going to see it.

I think what has happened to date has been sufficient to reinforce, you know, the perilous nature of where we are right now. I am hoping that, to quote Dmitri, that the Holiday Bear campaign, the Russian espionage campaign, is enough for Congress to take bold action and change the way that the Federal Government does business to secure its own networks—centralize authorities, provide capabilities that are hardened and more defensible, rather than leaving it up to the 101 different agencies. We have to change the way we act.

I also hope that the private sector now has had its awakening, that there are software companies, enterprise software and enterprise services, out there that have all of a sudden realized that, "Oh, my goodness, I am systemically important. I have a significant part of whatever segment or market that I am in, and if I am going to have a bad day, there are hundreds and thousands of people that are going to have bad days too. So what do I need to do about that?"

You need to implement better internal controls and transparency on what you are doing to secure your products. But you also have to engage in a meaningful way, to Dmitri and Michael's point, on operational partnerships, getting together to study a discrete, specific problem, contribute your resources, alongside your peers, in an open information-sharing environment where you can actually take real action.

Again, this is what we did for elections. We brought a range of stakeholders in, we were very open about the problems that were out there, and then we put collective action against that problem and dramatically improved security.

Mr. MEIJER. Mr. Krebs, just as a follow-on, you know, you mentioned CISA's budget. I mean, where do you think it needs to go to be able to provide that adequate level of security?

Mr. KREBS. So I think that is in part what I hope we can figure out through the NDAA's, kind of, force structure analysis. The Department of Defense does this exceptionally well. They can tell you exactly what return on investment you get from a single unit, and you can do unit-type costing from there. This is how DOD works.

The civilian agencies, DHS in particular, do not take that approach. We have to adopt that mindset. That will get us to a spot where, whether the budget should be $2 billion, it should be $4 billion or $8 billion, we will get there through that process.

But we need more resources, more modern infrastructure. We need to implement more modern security controls, like protective domain name system, a recursive system that is out for bid right now. Those are the sorts of things that we have to continue pushing forward.

I will tell you this right now: We are only going to have to spend more. We are only going to have to do more and more and more. It is not a one-shot deal. This is going to be the rest of our lifetimes.

Mr. MEIJER. Thank you, Mr. Krebs.

Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the gentlelady from Florida, Mrs. Demings, for 5 minutes.

Mrs. DEMINGS. Mr. Chairman, thank you so very much. I hope you can hear me. My connection has not been that great.

Chairman THOMPSON. We can hear you right now.

Mrs. DEMINGS. OK. Thank you so very much.

Thank you to our witnesses for joining us today. I also want to thank each of you for your just absolutely outstanding service.

Several of my colleagues have talked a bit about the attack on the water system in my home State of Florida. I know there are going to be investigations into that. There are a lot of unanswered questions for that because there are multiple independent systems that could be a part of the issue.

But what I would like to ask—and Mr. Krebs or anyone who would want to answer this question—do you feel like—I do believe this is just the beginning. I think we have been quite lucky. Do you think, like, that this attack was more of a—we liken it to a burglar trying a doorknob to see how easy it was, how quickly they could do it, in preparation for greater attacks?

Anyone who—Ms. Gordon or Mr. Krebs or anyone who would like to answer. Thank you.

Mr. KREBS. Yes, ma'am. Thank you. Yes, I touched on this briefly before. I will maybe clarify my earlier comment.

I think it is possible that this was an insider or a disgruntled employee. It is also possible that it was a foreign actor. This is why we do investigations. But we should not immediately jump to a conclusion that it is a sophisticated foreign adversary. The nature of the technology deployment in Florida, it is, frankly, not—certainly not where anybody, I think, any information security or operational technology security professional would like for that security posture to be.

I will also say that Oldsmar is probably the rule rather than the exception. That is not their fault. That is absolutely not their fault. These are municipal utilities that do not have sufficient resources to have robust security programs. That is just the way it goes. They don't have the ability to collect revenue at a rate enough to secure their deployments.

As I mentioned earlier, you know, when you have the internet, it is supposed to make things easier, it is supposed to make things more manageable. So, now that all of a sudden it is a security threat, it is almost counterintuitive.

Also, look, you have to be able to manage this stuff efficiently, so we need to have more security controls in place. I think there are at least 3 things that we need to do.

The first is we need to have more Federal funding available to get these tens of thousands of water facilities and other municipal operational technology systems up to speed with better security, more updated systems. Windows 7, if that is what they had, we should be on Windows 10. It is those sorts of things that we have to do.

The second is we need more training available. We have to bring the training to the systems where they are. So whether it is working with private sector or CISA working with the EPA, we can't expect these vendors to go to Idaho National Labs or travel. We have to bring the training to them.

Third, to Ms. Gordon's point, we have to have regional approaches to better IT technology. We have to have consortia that allow for upgrades and maintenance that are available with better price, with better cost efficiencies and economies of scale. You can pull that together at a State or regional level. I think that is going to have to be the future of IT deployments for systems like this.

Mr. DANIEL. Just to build on what Chris said, I would say that we very much need to keep an open mind until the investigation gets further down the road as to who the perpetrators behind this might be.

It could be a nation-state. Iran has shown itself very interested in water systems in other countries like Israel and even in the United States in former situations. It could be a lone actor. It could be a disgruntled employee.

There is just a wide array of possibilities at this point, and we really need to keep an open mind until the investigation concludes.

Mrs. DEMINGS. Right. I appreciate you saying that, because relaxing too soon, we know the consequences of that.

My last question, and I would like to address it to Mr. Daniel: You know, cyber attacks, we all know now, is the new weapon of choice, whether it is to rob you blind from your bank account or to have a major attack. But it does not seem to me that we are really prepared for this new weapon of choice.

Could you just talk a little bit about, you know, historically where we are, where we need to go, and did it just kind-of sneak up on us, this new weapon of choice, cyber attack?

Mr. DANIEL. Thank you, Representative. That is a very good question.

You know, if you actually look at how the internet developed and the way that people thought about the internet, Chris is absolutely right; it was supposed to be this new utopia. It was supposed to bring all these benefits. We didn't really think through how it made us more vulnerable.

We have seen this over and over again, of how the tools that were originally built to do good things also turned out to enable the bad guys to do malicious things. I think that it has taken us a while to sort-of shed that sort-of initial sort-of purely optimistic view of everything about the internet being good and start to realize that it can also be used for harm.

In many ways, though, this technology has developed incredibly rapidly. You know, it has only really existed in its current form for about 25 to 30 years. In policy terms and in legal terms and in, you know, sort-of, sociological terms, that is actually a very short amount of time. So it shouldn't really be a surprise to anyone that we are still trying to figure out how to organize and prepare to defend ourselves against the threats in this new environment that doesn't act like most of the rest of the physical world that we are used to.

So, yes, in some ways it did sneak up on us, but I think the good news is that now we are very much aware of the problem. We have committees like this that are focusing on it, and we have had a good policy foundation built over the last 10, 15 years. Now I think we can really start to do a much better job of getting our arms around the problem.

Mrs. DEMINGS. Thank you so much.

Ms. GORDON. I would add just one more thing——

Mrs. DEMINGS. Oh, go ahead.

Ms. GORDON. Yes, I would just add one thing——

Mrs. DEMINGS. Do I have time?

OK. Go ahead, Ms. Gordon.

Chairman THOMPSON. Go ahead.

Ms. GORDON. Yes, just one sentence, is that I also think that, for too long, we left it to be part of the support function and support functions infrastructure. We tend to make organizational choices about where we spend our resources, and when mission needs dominate, we take money away from those they support.

I think, with these recent events, we have the chance to make it a leadership issue. I think the Congress has a chance to put this in the forefront of the leadership, not have it be a second- and third-order effect that happens in local choice about implementation.

Thank you.

Mrs. DEMINGS. Again, thank you all so much.

Mr. Chairman, thank you for your leadership on this. Thank you for your patience, and yield back.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the next gentlelady from Florida, Mrs. Cammack, for 5 minutes.

Mrs. CAMMACK. Thank you, Mr. Chairman.

Good afternoon to everybody. I would like to thank the witnesses for appearing here today before the committee.

I know that, in a lot of ways, we are beating a dead horse here. I think we can all agree on the importance of cybersecurity and what lies ahead and the challenges we have. I know that our witnesses have explicitly stated or alluded to the fact that the interests of the United States, from National and homeland security all the way to economic prosperity, rely on our cyber capabilities, coordination, and resilience, particularly with our critical infrastructure.

As we have discussed in the hearing here today, cybersecurity threats are not only present for large corporations or Federal agencies, but these threats exist for both large and small businesses; Federal, State, and local governments; academic institutions; U.S. critical infrastructure; and private citizens across the country.

I am particularly excited about the hearing today, as I have spent 3 years getting my master's at the United States Naval War College on this very subject and have been identifying and looking for ways that Congress can more efficiently address these challenges. So I am very grateful for everyone's testimony here today.

Our witnesses and some of my colleagues on the committee have already touched on the recent discovery of the SolarWinds intrusion, which officials have confirmed is likely of Russian origin and may possibly be the worst intrusion in U.S. Government and private networks in our history. I am deeply concerned about this attack and plan to work with my colleagues on both sides of the aisle of this committee to better understand the full scope of this cyber espionage campaign.

So, turning now, as we look toward cybersecurity challenges in the Government and private sector, I believe that our future work force development should be a top priority as we reinforce and harden our critical infrastructure.

So, to Mr. Krebs, one of my first and primary concerns is our Nation's cybersecurity work force and this shortage that exists. In fact, it is what I wrote my master's thesis on. Think tanks, publications that all track our cybersecurity work force have been discussing this issue for years, yet we have a major shortage that remains today.

I would like to throw this idea out to you and get your input on establishing an academy of sorts, much like how we have our traditional service academies, like the Naval Academy, West Point, something like a U.S. Cyber Academy Corps, which would be dedicated and devoted to educating and training future cybersecurity professionals to defend our homeland and National security.

I would like to personally see an emphasis on joint operability not just among services but across Federal agencies, and would open up doors for non-traditional students who may have accessibility or disability challenges that would prohibit them from entering a traditional service academy like West Point or the Naval Academy or the Air Force Academy.

So do you see this being a feasible undertaking, something that is much needed, something that Congress should look to incorporate in future NDAA language? I would love to get your input on that.

Then I have a follow-up question to the remaining panelists.

So I will let you take it away.

Mr. KREBS. Thank you. First off, I would like to read your thesis. It sounds like you have a lot of really good ideas that could be implemented.

To your point of an academy, a cyber academy, I think that is certainly an option. But, ultimately, to your closing point, it takes all kinds.

Congress has previously appropriated for CISA—I forget at this point the amount, but to set up a network of institutes and training academies and college and university programs that would range all the way from post-grad to 4-year colleges to 2-year colleges to technical institutes, you know, trades. We have to make it more accessible to everyone to get technology-based education to put them in a position to enter the work force.

The last thing I will mention on this was, you know, I am a firm believer that we have the opportunity and the inherent advantages in the United States of America, because of our diversity, to bring the fight back to—the defensive fight, certainly—back to the adversary that tend to be monocultural and homogenous. I think that, based on our diversity of opinions, backgrounds, experiences, thought processes, that this gives us a distinct advantage.

We have to harness that. We have to work through all sorts of different educational platforms to bring more people into the work force. So we would love to work with you and think more about this.

Mrs. CAMMACK. Mr. Krebs, I know I am short on time. I did want to pose a question, if the Chairman would allow me, for the panelists, Mr. Daniel, Ms. Gordon.

If you could maybe touch on the "Tallinn Manual" and——

Chairman THOMPSON. One question. One question.

Mrs. CAMMACK. I appreciate it. Thanks for giving a little bit of grace to a freshman. I appreciate that.

I would like to get some input from our experts here on the "Tallinn Manual" that has really kind-of been the guide internationally as we have looked to address and respond to cyber attacks, both from lone-wolf-type actors to state-on-state attacks.

Do you see the "Tallinn Manual" as something that has been effective? Do we need to really subscribe to some of the guidelines and framework that they have outlined particularly in the second edition?

I will kick it to Ms. Gordon first.

Ms. GORDON. I am sorry. I made it through the whole hearing without staying on mute.

I don't think there is any one—I am with Chris. I think we ought to look at your thesis and see what we have.

I think there is nothing perfect. I do think we are going to have to explore standards and standards beyond our borders. So I think it is a fine place to begin. I don't think it is a panacea. I think we always have to look at it to make sure it doesn't disproportionately limit our freedoms, but I think it is a fine place to begin.

Mrs. CAMMACK. Thank you.

Mr. DANIEL. I would concur with Sue's point. I think the level of thought and the degree of, sort-of, analysis that went into creating the "Tallinn Manual" is really an excellent foundation in the international space.

You know, clearly, just given the amount of fussing that the Russians and the Chinese do about the "Tallinn Manual," anything that they dislike that much says that I probably ought to really like it. So I will also use that as a benchmark as well.

Mrs. CAMMACK. Excellent. Thank you.

Thank you, Mr. Chairman.

Mr. KATKO. Mr. Chairman, just a point of privilege just for one moment?

Chairman THOMPSON. The Ranking Member is recognized.

Mr. KATKO. Thank you.

I have a hard stop at 5 that I cannot get out of, and I just wanted to thank you for having this hearing and bringing such a critical issue to light.

I want to commend all of the witnesses, and I want to commend all of my fellow members. Excellent questions, excellent preparation. I am proud to be a part of this, and I know we are going to have a lot more hearings on cybersecurity going forward. But I appreciate your leadership, Mr. Chairman.

I yield back. Thank you.

Chairman THOMPSON. Thank you.

The Chair recognizes the patient gentlelady from Virginia for 5 minutes, Mrs. Luria.

Mrs. LURIA. Thank you, Mr. Chair.

Thank you again to all the witnesses who have joined us today for this very informative discussion.

You know, I wanted to just bring up a couple incidents that have happened recently in my district here in southeastern Virginia.

In November 2020, malware infected the Hampton Roads Sanitation District, and that led to delays in billing. This was basically caught and stopped before, you know, it spread throughout their whole network, and the damage could have been much worse. The perpetrator has not been identified.

But, you know, I think that these instances of attacks on, you know, local or regional utilities are perhaps more common than we recognize.

So I wanted to know, you know, from the Federal level, what level of coordination, of establishing of trends, identifying these vulnerabilities, and, you know, how we can help, you know, across the board from them being replicated, you know, kind-of just that coordination effort between Federal or State and local governments relative to these public utilities. Like, what more should we do?

I know Mr. Krebs brought up, you know, this coordination between different levels of government. If you could comment on that, from the Federal level, what other resources could help these local utilities?

Mr. KREBS. Yes, ma'am.

So, to your point of vulnerability disclosure, vulnerability discovery, CISA sits at a point where they manage the National Vulnerability Database, or at least they support it for NIST. That is a process by which I think 13,000 or so vulnerabilities were disclosed and managed by CISA last year.

So CISA certainly sits in a trend analysis position. I think what CISA needs to do more of is that over-the-top analysis of where things are going, where is the most effective investment of that last dollar.

This is a conversation that Dmitri and I have had several times, of the value of investing in patching and the value of investing in hunting. There is a balance you have to strike. You don't want to over-rotate one way, or you are going to throw the entire approach out of balance.

But I think we have to do more trend analysis on, you know, for instance, the top 5 areas that you can make the most meaningful vulnerability management investment in your operational technology. That is something I have talked with a number of different OT security companies about.

So where I am really going with this is, we need more insight. We can do the technical coordination piece, but we need more insight. That requires people, and it requires communication, and it requires engagement with the community. At that point, leadership will understand. If you give them the resources to smartly invest, then you will actually see, at the endpoint, improved security behaviors.

Mrs. LURIA. Well, thank you. I would love to continue this conversation separately about, you know, how we are allocating resources and what resources have been allocated; you know, can they meet that improved goal of analyzing the data writ large.

Another thing that came up in my district—and I am sure any Member of Congress who, you know, would speak on these issues would have examples from at home—is that we had a ransomware attack at one of our local universities, at Virginia Wesleyan University in my district. They were affected by a ransomware attack in 2019.

So I was wondering, for, you know, the institutions of higher learning—this is, you know, a private higher educational institution—are there any resources from the Federal Government or could we do more to protect them?

Then, also, to follow on to that, are there requirements for reporting of these types of attacks by institutions of higher learning and specifically private institutions of higher learning?

Either Mr. Krebs or maybe Mr. Daniel could respond to this one.

Mr. KREBS. So I mentioned earlier the CISA ransomware awareness campaign. Institutes of higher learning, K–12 education are actually in the top 3 of ransomware attacks, along with public health as well as Government agencies. So we have to do more, but, again, you know, some of these institutions just don't have the resources to secure. So we have to push more resources out there to them.

CISA, as I understand it, is working now with the Department of Education to have a more targeted approach to K–12 and college and post-grad.

I will defer to Mr. Daniel on anything else he wants to add there.

Mr. DANIEL. Well, thanks.

It is a good question, Representative. I think, there are no general reporting requirements for most private institutions with respect to [inaudible] ransomware.

Now, there are resources available from various places, in terms of expertise to—you know, how you want to make that decision about whether or not to pay and then how to remediate your systems. But it is often very difficult to access, and it is not typically in one centralized location.

I think one of the efforts that is on-going—Chris made a reference to the ransomware task force that has been put together. That is one of the issues that very much that task force is looking at, is how to make those resources more easily accessible to, you know, things like private universities and others that don't have the resources to call in, you know, an incident responder in the same way that, you know, a big private-sector company might.

Mrs. LURIA. Well, thank you for that.

I am sorry, I think my time has expired.

I yield back, Mr. Chairman.

Chairman THOMPSON. Thank you very much.

The gentlelady's time has expired.

The Chair recognizes the gentleman from Mississippi, Mr. Guest, for 5 minutes.

Mr. GUEST. Thank you, Mr. Chairman.

Since the creation of the internet, we have been battling cyber attacks. New cyber attacks, as we know, have been highlighted by the recent actions involving SolarWinds. We have discussed that in great detail.

You mentioned that particularly, Mr. Daniel, in your report. On page 9 of your written testimony, you say, "In December, several private-sector companies identified malicious activity that enabled the Federal Government to unravel an incredibly broad cyber-enabled espionage campaign. This intrusion effectively gave the Russian Government unfettered access to numerous unclassified U.S. Government networks for over 9 months. It is difficult to overstate the intelligence value the Russians gained from this access or the likely damage to our National security."

So my question—and I will start with you, Mr. Daniel—is, what should the response be?

I see that you come down in the following paragraph and you say, "We should respond forcibly to this intrusion through diplomatic channels, such as by expelling Russian diplomats or exacting a cost in other venues."

I want to see if you can expand on that answer, particularly what you are talking about when you say "exacting a cost in other venues."

Mr. DANIEL. Sure. Thank you, Representative. So I think that, you know, this actually—this kind of intrusion poses an interesting problem for the U.S. Government in responding, and we absolutely should respond.

But, so far, all of the information that is available about this intrusion indicates that it is espionage, and espionage is something that the United States carries out itself against our foreign adversaries. So that has to shape and constrain how we think about our response.

Now, during the Cold War, we very much had, you know, an understanding with the Russians that, occasionally, espionage operations went beyond the bounds and they got too big and they got out of hand. So when that happened, there was a response, and that often involved expelling diplomats, for example, sort-of the typical term for that is PNG-ing, persona non grata, you know, so you remove those diplomats and suspected Russian agents from the country.

But what I mean by the other options are, there are things that the Russians want in the United Nations and in other diplomatic areas. We can slow that down. We can use our influence with our—you know, both ourselves and with our allies to cause them problems in the diplomatic realm. There are things that the Russians want that we can say no to or that we can slow-roll for a while to make it clear our displeasure at the scope and scale of this operation.

So while I think that the options for retaliation for us have to be constrained by the fact that we also carry out espionage, that does not mean we have to simply, you know, accept this behavior sort-of meekly and not express our concerns with it.

Mr. GUEST. Let me change gears with the panel just very quickly. What efforts are being made to leverage technical expertise that exists in many of our universities across the country?

Both myself and Chairman Thompson have universities, major universities, here in Mississippi that are both doing great work in the area of cyber research. So my question to the entire panel is, how can we incorporate this work being done at our academic institutions into our National strategy to combat cyber attacks?

Ms. GORDON. I will start and be brief and so we can see the whole perspective. No. 1, I think in many instances, the Government does and has relied on the work going in our academic universities, particularly in the research that is going to allow us to be prepared in the future.

But what we really need is what you all are talking about here. We need some sort of quest, some problem that is clear, to unleash and put Government money behind it, to really drive people both to those programs and those programs to drive the solutions that we need.

So I think we already do tactically. I think we have used it historically, but I think you all are on the threshold of being able to set a flag in the ground and say we have got to go there, and universities are a great place to be driving that forward.

Mr. GUEST. Any other Members care to comment on the use of the universities to incorporate them into our National strategy?

Mr. KREBS. I will simply add that student—current students and recent graduates are going to be key to building out any program. I know at CISA, we use the Scholarship for Service I already mentioned. We had a number, you know, I think 2 dozen interns, paid interns in place that were able to help. In fact, a number of interns were actually on our Election Security Initiative. So, you know, this is a great way to help boost the work force now and in the future.

Mr. GUEST. To all our witnesses today, I want to thank you.

Mr. Chairman, I yield back.

Chairman THOMPSON. Thank you very much.

I would like to recognize the vice chair of the Homeland Security Committee, Mr. Torres of New York, for 5 minutes.

Mr. TORRES. I thank you, Mr. Chair.

I read recently in *The New York Times* that a man by the name of David Evenden, a former hacker for the National Security Agency, essentially went on to become a cyber mercenary, for CyberPoint, an American contractor that had business with the United Arab Emirates and has an office in Dubai, where Mr. Evenden was stationed.

According to this report, on behalf of his client, the United Arab Emirates, Mr. Evenden was tasked with hacking into Qatar, and in the process of doing so, he eventually eavesdropped on the private communications between the Government of Qatar and the then First Lady, Michelle Obama.

So when I read this anecdote, I was horrified, and I asked myself, how could an American contractor and how could a hacker from our National Security Agency be allowed to eavesdrop on the private communications of the First Lady and be allowed to engage in cyber operations against either the United States or an ally of the United States like Qatar?

So 2 questions: How can this be allowed to happen, and how do we ensure that this never happens again? This question can either go to Mr. Daniel or Ms. Gordon.

Ms. GORDON. Mike, I will take it to start.

It is a horrifying scenario. It is a slippery slope. People with expertise developed at Government, in Government institutions, will leave periodically, and we don't want their knowledge to not be used. So, you know, prohibiting them from doing anything or from advancing the state-of-the-art is not something that would be in our interest.

But I also believe that when you engage in something that would be antithetical to the laws of this country, to the standard that you had lived under before, you are still bound to that, and you are smart enough to know what you are engaged in.

We have lots of sorts of nondisclosure protection of Classified information, ethical restrictions. I think it is worth considering applying those, but we will have to be very mindful, because that expertise is also the expertise that keeps the United States ahead in being a global leader.

Mike.

Mr. TORRES. Well, to be clear, I am not proposing to prohibit the use of the expertise. I am proposing prohibiting cyber mercenaries from engaging in cyber operations against their own country or against an ally of the United States. That is a——

Ms. GORDON. Yes, you and I see it the same way. I am just saying that as we figure out how to prohibit that, we are going to have to be really mindful of the other side.

Mr. TORRES. In the interest of time, I want to move on to SolarWinds. You know, well before the breach of the U.S. Government, there were early warning signs that SolarWinds was complacent about its own cybersecurity.

According to Reuters in 2017, Mark Arena, the chief executive of a cyber crime intelligence firm, informed the U.S. Government that there was an FBI-wanted cyber criminal offering to sell access to SolarWinds' computers on underground forums.

In 2019, Vinoth Kumar, a security expert, warned SolarWinds that anyone could access the company's update server with the password SolarWinds123. Even though SolarWinds broadly serves both the U.S. Government and corporate America, SolarWinds did not even have a chief information security officer.

I am curious to know, why would the Government, the Federal Government, do business with a vendor that was so glaringly complacent about its own cybersecurity? The sloppiness of one supply chain vendor like SolarWinds can create systemic risk for the rest of us.

So the question is: Do we have a process in place for ensuring that the supply chain vendors with which we do business have sufficient cybersecurity protection? This question, Mr. Krebs.

Mr. KREBS. So I think I will pick up where Dmitri opened up in his opening remarks about some of the measures we need to put in place with Federal Government contracting. I have already talked about adding CISA as a—with some degree of privity of contract, or at least information sharing based on individual contracts. But we also have to know where the systemically important software is in the Federal Government, what has elevated privileges, you know, what sort of data is being touched in the cloud environment, you know, who is touching source code, what are the controls in place. Dmitri has a range of recommendations that I think are important.

They are just not there yet. So we need to update the Federal acquisition regulation and we need to get deeper into contracts. I think in part what the Department of Defense has done with the CMMC program is a good start.

Mr. TORRES. Mr. Chair, how much time do I have left? I don't actually see the timer.

Chairman THOMPSON. Well, Mr. Chair, I will be gracious to you. Take as much time as you need.

Mr. TORRES. OK. I will end on this note. I have a question about cyber strategy. You know, suppose the United States, our cybersecurity apparatus finds a vulnerability, it seems to me we have 2 options. We can either correct the vulnerability and thereby strengthen our cyber defensive capabilities or we can exploit the vulnerability and thereby strengthen our cyber offensive capabilities.

It seems to me historically the United States has chosen to prioritize playing defense rather than playing offense, has chosen to exploit vulnerabilities rather than correct them.

In light of the SolarWinds breach, did we as a country make a strategic miscalculation in prioritizing cyber offense at the expense of cyber defense? That will be my last question, and I will direct that toward Ms. Gordon.

Ms. GORDON. Boy, it has been a continuum, and I think we have moved in the direction that you so clearly articulated, that on the early days, we were looking for advantage in terms of offense.

In the days we have seen since, we recognize that advantage is the ability to withstand the kinds of attacks we see. So I think it is always a choice, but I think that the pendulum has swung more in the direction that you articulate, and SolarWinds certainly hammered that home in terms of how to achieve it. Thank you.

Mr. TORRES. Thank you so much, Mr. Chair. I appreciate your courtesy extended toward me.

Chairman THOMPSON. Thank you very much.

The Chair recognizes the other gentleman from New York, Mr. Garbarino.

Mr. GARBARINO. Garbarino, Mr. Chairman.

Chairman THOMPSON. All right.

Mr. GARBARINO. Garbarino.

Chairman THOMPSON. Thank you.

Mr. GARBARINO. Thank you very much, Mr. Chairman, Ranking Member Katko, for putting this hearing together, as well as for the witnesses for their testimony.

As Ranking Member for the Subcommittee of Cybersecurity, Infrastructure Protection, and Innovation, I am looking forward to working with Chairwoman Clarke to implement some of the recommendations that we heard today.

I have just, like, 1 or 2 questions. You know, we heard about SolarWind and how it was the largest cyber attack on the country up to date. It exposed that we were unprepared, that we were underresourced to deal with the attack.

President Biden has recommended a multibillion-dollar infusion for Federal IT modernization and cybersecurity to respond to the SolarWinds breach.

I will start with Mr. Krebs, and maybe if somebody else wants to jump in and answer as well. Mr. Krebs, what is your opinion of CISA's Continuous Diagnostics and Mitigation Program? What do we ultimately want it to do? Is it a lot more funding, or is it, you know, better to force aggregate visibility from CDM deployment or a combination of both?

Mr. KREBS. So I think we need to invest more in CDM. I think we need to invest more aggressively, and we need to get more organizations onboarded through the various levels of the program.

Ultimately, CDM is about knowing what is on the network, who is on the network, and what data is transiting the network. We are still, based on some of the investments to date, taking too slow of an approach, and we need to accelerate that investment. We need to add additional investment for the proactive hunt capabilities, and that is what is going to, as Dmitri mentioned, give us the ability to take that assumption of breach mentality.

But as I see it, CDM is going to be the future of the program.

Mr. GARBARINO. OK.

Mr. KREBS. Of Federal cybersecurity.

Mr. GARBARINO. Any other witnesses want to touch on that? Or I am going to move on.

Mr. ALPEROVITCH. Yes, Congressman. I would just like to echo what Chris has said, but the assumption of breach mentality, I think, is most steep. We need to stop pretending that we can stop adversaries from getting to our networks. They will always be able to get in, sometimes through insiders, sometimes through spies that they will be able to insert into our Government.

But we need to assume that they are there, we need to hunt for them actively, 24/7, on all of our networks, and kick them out as quickly as possible. That is the winning strategy. I have seen it work in the private sector. I believe it absolutely can work in the Government.

Mr. KREBS. This is—if I can just add one little coda on top of that. I have been asked the question a couple times, you know, when are we going to know if the Russians are finally out of the network. You should have always assumed they were there the whole time. That is not the mentality that you want to take. It is continuous hunting. Assume that they are there.

Mr. DANIEL. Yes. I will just add on top of that, I think the proposals also need to retire a vast amount of the technological debt that the Federal Government has incurred, that there are systems out there that we can't even get continuous diagnostics monitoring on because they are so old. So we need to retire those—we need to retire those systems and modernize much of the Federal Government's IT.

Mr. GARBARINO. That was actually my follow-up question, Mr. Daniel, about whether or not everybody should be required to update, every Federal agency. So I imagine everybody here feels the same way.

Mr. KREBS. So I would—one of the things I think a missed opportunity we had, both through earlier steps of CARES Act but also the more recent COVID-related package of that $10 billion, that $9 billion for Federal agencies to upgrade and modernize their systems is absolutely critical. It is really, really tough right now to secure, as Michael pointed out.

We have to upgrade these systems. So whatever the next opportunity is, whether it is some Capitol Police-related legislative package, I really encourage Congress to think hard about what additional funding is required to secure the Executive branch.

Mr. GARBARINO. Mr. Chairman, I have to run to another hearing. I did have another question, but I do have to go to another hearing, so I yield back. I definitely thank the Chairman and the witnesses for their testimony today.

Chairman THOMPSON. Thank you very much.

Let me also thank the witnesses for their testimony. The accolades you have already received from my coworkers on the committee speaks volumes for their appreciation for your response to their questions.

The Members of the committee may have additional questions——

Ms. JACKSON LEE. Mr. Chairman? Mr. Chairman, if I might be yielded to for just a moment? This is Sheila Jackson Lee.

Chairman THOMPSON. The lady from Texas is recognized.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman.

What an enriching and very powerful discussion. One of the agencies that has been on the forefront of cybersecurity is obviously our Defense Department—and when I say on the forefront, they have a infrastructure dealing with this.

I think what we have gleaned from this meeting, that there needs to be a coming together on the domestic security and the vulnerabilities that we experience. I think this committee hearing, Mr. Chairman, has been singular in highlighting those issues.

I join with my colleagues—I have heard a number of ideas—I join with my colleagues that we should be on the offensive and not the defensive. I have just heard Director Krebs talk about shoring up the Executive. So I am hoping that our leadership will recognize that we probably, as swiftly as you are, Mr. Chairman, by having this hearing, that we need to move swiftly.

I will conclude by saying, even before SolarWinds, we wrote legislation dealing with a zero-day event, which now sets enormous panic for me, because it is more than a viable possibility, and that is when all of our systems are at a level of—a diminishing level.

So I hope that what we have gotten out of this hearing is a sense of urgency and the ability to work with you, Mr. Chairman, and all the Chairs on the number of committees. I am glad to be on one of the subcommittees to really say to the administration and say to the Nation that cybersecurity has to be, from the domestic security perspective, a heightened and enlightened defense effort, if you will. I can see that we can do it in this committee.

So thank you very much. I just wanted to thank you for the hearing and thank the witnesses for the hearing as well. I have been through this a lot, and to hear your representation gives us a great road map for us to proceed on. So thank you each and every one of you.

Chairman THOMPSON. Thank you very much.

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

Without objection, the committee's record shall be kept open for 10 days.

Hearing no further business, the committee stands adjourned.

[Whereupon, at 5:22 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM HONORABLE MICHAEL T. MCCAUL FOR CHRISTOPHER C. KREBS

Question 1. What role do State and local government IT infrastructures play in ensuring the security of our Nation? What specific steps can State/local entities take to improve their IT infrastructure, what resources can we provide them, and can you speak to the increased funding that you proposed in your testimony?

Answer. Response was not received at the time of publication.

Question 2. Are there any gaps where you think the Legislative branch might step in to protect the United States against cybersecurity threats, including misinformation? Moving forward, how can Congress help CISA in their efforts?

Answer. Response was not received at the time of publication.

Question 3. What are some common misconceptions about the security of our elections? What can we do to promote transparency regarding the administration of our elections?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE JAKE LATURNER FOR CHRISTOPHER C. KREBS

Question. With the perpetrators of the Solarwinds hack likely still lurking in our systems, monitoring unencrypted communications, gathering valuable information on how we respond, would you agree the Federal Government needs to prioritize operational security by leveraging secure communications as a critical first line of defense?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE JAKE LATURNER FOR SUSAN M. GORDON

Question. With the perpetrators of the Solarwinds hack likely still lurking in our systems, monitoring unencrypted communications, gathering valuable information on how we respond, would you agree the Federal Government needs to prioritize operational security by leveraging secure communications as a critical first line of defense?

Answer. Response was not received at the time of publication.

QUESTION FROM HONORABLE JAKE LATURNER FOR MICHAEL DANIEL

Question. Now that there are unified communications capabilities available in establishing a strong, resilient crisis response plans to prevent and mitigate future intrusions, what role does end-to-end encryption play and should the Government place priority on communications that allows for global federation so that Government agencies are able to communicate securely with external parties?

Answer. Secure communications are critical to almost all Government activities, including policy development, service provision, cybersecurity, and crisis response, and these activities must involve interactions between the Government and the private sector to be effective. Given the capabilities of our adversaries, making communications secure requires strong end-to-end encryption, but such encryption also poses a challenge to law enforcement in preventing or disrupting crimes. As a result, the encryption debate is a security-versus-security debate. There is no single "right" answer to this debate.

Societies must decide how much security of the first kind they are willing to trade for the second and vice-versa.

○