DEFENDING AGAINST FUTURE CYBER ATTACKS: EVALUATING THE CYBER SPACE SOLARIUM COMMISSION RECOMMENDATIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JULY 17, 2020

Serial No. 116–79

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

43–867 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
CEDRIC L. RICHMOND, Louisiana
DONALD M. PAYNE, JR., New Jersey
KATHLEEN M. RICE, New York
J. LUIS CORREA, California
XOCHITL TORRES SMALL, New Mexico
MAX ROSE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
NANETTE DIAZ BARRAGÁN, California
VAL BUTLER DEMINGS, Florida

MIKE ROGERS, Alabama
PETER T. KING, New York
MICHAEL T. MCCAUL, Texas
JOHN KATKO, New York
MARK WALKER, North Carolina
CLAY HIGGINS, Louisiana
DEBBIE LESKO, Arizona
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
DAN CRENSHAW, Texas
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, Texas

HOPE GOINS, *Staff Director*
CHRIS VIESON, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

CEDRIC L. RICHMOND, Louisiana, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
KATHLEEN M. RICE, New York
LAUREN UNDERWOOD, Illinois
ELISSA SLOTKIN, Michigan
BENNIE G. THOMPSON, Mississippi *(ex officio)*

JOHN KATKO, New York, *Ranking Member*
MARK WALKER, North Carolina
MARK GREEN, Tennessee
JOHN JOYCE, Pennsylvania
MIKE ROGERS, Alabama *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
SARAH MOXLEY, *Minority Subcommittee Staff Director*

CONTENTS

DEFENDING AGAINST FUTURE CYBER ATTACKS: EVALUATING THE CYBER SPACE SOLARIUM COMMISSION RECOMMENDATIONS

Friday, July 17, 2020

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 12:30 p.m., via Webex, Hon. James R. Langevin [Member of the subcommittee] presiding.

Present: Representatives Jackson Lee, Langevin, Rice, Underwood, Slotkin, Thompson; Katko, and Joyce.

Mr. LANGEVIN. Good afternoon. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order.

Good afternoon, everyone. I want to thank the co-chairs of the Cyberspace Solarium Commission and Commissioners Spaulding and Ravich for participating in today's hearing. I would also like to thank the gentleman from Louisiana, Mr. Richmond, for allowing me the honor of chairing this subcommittee in his absence.

I have the privilege of serving on the Solarium Commission with the witnesses testifying here today. I can honestly say that working on a report was one of the highlights of my Congressional career—research, outreach, and deliberation was a testament to our 2 co-chairs, Senator King—here today to testify this afternoon. I hope our subcommittee will take full advantage of the wealth of knowledge of the virtual witnesses at the witness table.

The commission's report outlines a strategy of layered cyber deterrence, and includes 82 recommendations on how the Government can implement the strategy. I am looking forward to discussing those recommendations with my colleagues today, particularly those that would strengthen the cybersecurity—the Cybersecurity and Infrastructure Security Agency by increasing its capabilities and clarifying its relationship with the intelligence community and sector-specific agencies.

I am also looking forward to covering the essential role of Congress in implementing our Nation's cybersecurity posture. From the outset of the—and thanks to the work of our dedicated executive director, Mark Montgomery, we deliberated with a bias toward action. After all, as the Members of the subcommittee know full well, the status quo in cyber space sees us making—status quo in cyber

space sees us making steady progress, while the threat increases exponentially.

We need to act, and act now, to change that dynamic and get ahead of the curve. I am proud to report that leaders of this subcommittee, including Chairman Richmond, Ranking Member Katko, and Representatives Jackson Lee, Rice, Slotkin, Green, and Joyce all have recommendations to the forthcoming National Defense Authorization Act and impending—and to implement aspects of the Solarium report.

It is an honor to share the virtual dais with Members committed to addressing this quintessential information-age challenge, and I am sure the committee and this subcommittee will continue to play a vital role in implementing the report.

I encourage our witnesses to discuss why Congress is so important to moving the conversation forward on cybersecurity, and I encourage my colleagues to probe the decision making behind the strategy and recommendations.

The events of this year provide an interesting context in which to review the Solarium recommendations. The COVID–19 pandemic has amended and altered the way we live, the way we work, and the way we govern. Overnight, nearly half of employed adults became teleworkers, putting added stresses on our infrastructure, and creating new opportunities for hackers to wreak havoc.

Now Congress is holding remote hearings, and State and local governments have become e-governments with little time to transition. Many State and local governments are also finding that, due to the antiquated IT systems and the fact that their data aren't in the cloud, that they are unable to scale and secure vital programs like unemployment insurance, highlighting the need for modernization as part of the security push.

Our adversaries have noticed the broader attacks surface. Just yesterday, CISA, in conjunction with allies in the UK and Canada, announced that Russian operatives are targeting health care organizations doing research on the virus.

[Audio malfunction.]

Mr. LANGEVIN [continuing]. The breach of Twitter that saw many prominent accounts linking to a Bitcoin scam. It doesn't take much imagination to see what chaos one could sow with such access on Election Day if a bad actor was pushing out disinformation.

The realities of 2020 make clear that a comprehensive whole-of-Nation approach to cybersecurity is necessary, but—is a necessity, but we do not yet have one. So we lack a clear leader in the White House whose mission it is to focus on cybersecurity. We lack clear understanding of roles and responsibilities, both within Government and—between Government and the private sector. We lack clear metrics to measure our progress.

The Cyberspace Solarium Commission report cannot fix all of the challenges that we face in cyber space. But it does chart a bold course, and it does not shy away from the trade-offs we will need to make to decisively improve our cybersecurity posture.

The report makes clear that everyone, from Government, to private-sector companies, to Congress itself needs to make meaningful changes. We need to expect more from Government: Closer coordination across agencies; stronger collaboration with critical infra-

structure; and a—and critically, a greater emphasis on planning. We need to strengthen Government agencies—in particular, CISA—to do so.

We also need to expect more from the private sector. We need companies to truly accept the risk that they take in cyber space by accepting the consequences of failing to protect their data and networks.

We also need technology companies, what the report calls "cybersecurity enablers," to do more to make the secure choice the default choice. Too often we see a rush to be first to market, not secure in a market. Too often we see entities like the ISPs not protecting the small and medium-sized customers, because they don't believe it is their job. More importantly, where the public and private interests at—the nexus of critical infrastructure that this committee is charged with protecting. We need to ensure the private sector is doing its part to protect itself, while acknowledging that they can't go it alone.

So this is part of the end-state we desire in the Solarium report, a state where we are resilient enough to deter our adversaries and agile enough to push back when they insist on testing our defenses. To that end, to end—to—that end-state is in reach, but it will require the work of this subcommittee and of the experts that we have invited before us if we are to achieve that goal.

So I look forward to beginning what I am sure will be a fruitful series of discussions on how to implement the Solarium report.

I again thank our witnesses who are here today. I am grateful that the co-chairs of the Cyber Solarium Commission could be here, Senator Angus King and Congressman Mike Gallagher.

I am honored that Suzanne Spaulding could be here, as well, and I look forward to all of our witnesses' testimony today.

[The statement of Mr. Langevin follows:]

STATEMENT OF HON. JAMES R. LANGEVIN

JULY 17, 2020

I had the privilege of serving on the Solarium Commission with the witnesses testifying here today, and I can honestly say that working on our report was one of the highlights of my Congressional career. Our thoughtful research, outreach, and deliberation was a testament to our two co-chairs, Senator King and Congressman Gallagher, and I hope our subcommittee takes full advantage of the wealth of knowledge at the virtual witness table.

The commission's report outlines a strategy of layered cyber deterrence and includes 82 recommendations on how the Government can implement that strategy. I am looking forward to discussing those recommendations with my colleagues today—particularly those that would strengthen the Cybersecurity and Infrastructure Security Agency by increasing its capabilities and clarifying its relationship with the intelligence community and sector-specific agencies.

I am also looking forward to covering the essential role of Congress in improving our Nation's cybersecurity posture. From the outset of the commission—and thanks to the work of our dedicated executive director, Mark Montgomery—we deliberated with a bias toward action. After all, as the Members of this subcommittee know full well, the status quo in cyber space sees us making steady progress while the threat increases exponentially.

We need to act, and act now, to change that dynamic and get ahead of the curve. I am proud to report that leaders on this subcommittee, including Chairman Richmond, Ranking Member Katko, and Representatives Jackson Lee, Rice, Slotkin, Green and Joyce all have amendments to the forthcoming National Defense Authorization Act to implement aspects of the Solarium report. It is an honor to share the (virtual) dais with Members committed to addressing this quintessential Informa-

tion Age challenge, and I am sure the committee—and this subcommittee—will continue to play a vital role in implementing the report.

I encourage our witnesses to discuss why Congress is so important to moving the conversation forward on cybersecurity. I encourage my colleagues to probe the decision making behind the strategy and the recommendations.

The events of this year provide an interesting context in which to review the Solarium Commission's recommendations. The COVID–19 pandemic has upended and altered the way we live, the way we work, and the way we govern. Almost overnight, nearly half of employed adults became teleworkers, putting added stress on our infrastructure and creating new opportunities for hackers to wreak havoc.

Now Congress is holding remote hearings, and State and local governments have become e-governments with little time to transition. Many State and local governments are also finding, that due to antiquated IT systems and the fact that their data aren't in the cloud, they are unable to scale and secure vital programs like unemployment insurance, highlighting the need for modernization as part of the security push.

Our adversaries have noticed the broader attack surface. Just yesterday, CISA—in conjunction with allies in the United Kingdom and Canada—announced that Russian operatives are targeting health care organizations doing research on the virus. And 2 days ago, we saw a major breach of Twitter that saw many prominent accounts linking to a Bitcoin scam. It doesn't take much imagination to see what chaos one could sow with such access on Election Day if a bad actor was pushing out disinformation.

The realities of 2020 make clear that a comprehensive, whole-of-Nation approach to cybersecurity is a necessity, but we do not yet have one. We lack a clear leader in the White House whose mission it is to focus on cybersecurity. We lack clear understanding of roles and responsibilities, both within Government and between Government and the private sector. We lack clear metrics to measure our progress.

The Cyberspace Solarium Commission report cannot fix all the challenges we have in cyber space. But it does chart a bold course, and it does not shy away from the trade-offs we will need to make to decisively improve our cybersecurity posture. The report makes clear that everyone—from Government to private-sector companies to Congress itself—needs to make meaningful changes.

We need to expect more from Government: Closer coordination across agencies, stronger collaboration with critical infrastructure, and, critically, a greater emphasis on planning. And we need to strengthen Government agencies—in particular CISA—to do so.

We also need to expect more from the private sector. We need companies to truly accept the risks they take in cyber space by accepting the consequences of failing to protect their data and networks. We also need technology companies—what the report calls "cybersecurity enablers"—to do more to make the secure choice the default choice. Too often, we see a rush to be first to market, not secure to market. Too often, we see entities like ISPs not protecting their small and medium-sized customers because they don't believe it's their job.

Most importantly, where the public and private intersect, at the nexus of critical infrastructure that this committee is charged with protecting, we need to ensure the private sector is doing its part to protect itself while acknowledging that they can't go it alone.

This is part of the end-state we desire in the Solarium report, a state where we are resilient enough to deter our adversaries and agile enough to push back when they insist on testing our defenses. That end-state is in reach, but it will require the work of this subcommittee—and of the experts we have invited before us—if we are to achieve that goal.

Mr. LANGEVIN. With that, I am now proud to yield to Mr. Katko for his opening remarks.

Mr. KATKO. Thank you, Mr. Chairman, I appreciate your comments. Before I begin I want to congratulate one of the Solarium members on the birth of his first child, Representative Gallagher.

Grace Ellen Gallagher came to this world not too long ago, and we welcome her in. You—I will raise—I will hoist a pint in her honor soon.

I want to thank all the commissioners for their work on the Cyberspace Solarium Commission, and congratulate them on producing a truly game-changing report and recommendations that ac-

company that report that take a bold step in the direction of reinventing our Nation's cybersecurity policy and architecture. The commission's legislative proposals accompanying the recommendations are enabling Congress to act quickly and decisively on these urgent measures.

I am interested in all the recommendations in the report, and I have gone through all of them, but I am really focused on several of them today, and they are as follows: Strengthening the Cybersecurity and Infrastructure Agency, or CISA, and its work force; evaluating CISA's facilities needs; strengthening the CISA director position, and making the assistant directors clear positions—the National cyber director; authorizing CISA to threat hunt on the gov domain, .gov domain; developing a strategy to secure email; and modernizing the digital infrastructure of State and local governments, and small and mid-sized businesses.

As Ranking Member on the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, my top priority among the commission's recommendations is strengthening and clarifying CISA's authority, and vastly increasing its funding to allow it to carry out its role as the Nation's risk manager, coordinating the protection of critical infrastructure and Federal agencies and departments from cyber threats.

I introduced this recommendation as a bill, together with Mr. Ruppersberger, and cosponsored his amendment to the NDAA, which requires CISA to assess what additional resources are necessary to fulfill its mission. This assessment should examine CISA's work force composition and future demands, and report to Congress on the findings.

Under this bill, CISA would also evaluate its current facilities and future needs, including accommodating integration of personnel, critical infrastructure partners, and other Department and agency personnel, and make recommendations to GSA. GSA must evaluate CISA's recommendations and report to Congress within 30 days on how best to accommodate CISA's missions and goals with commensurate facilities.

The facilities evaluation dovetails with the commission's recommendation for an integrated cyber center within CISA. That is critically important.

In conjunction with Chairman Richmond's CISA director amendment to the NDAA bill that I cosponsored, I reintroduced my CISA director bill. The bill and amendment elevate and strengthen the CISA director position to reflect the significant role that it plays, and making the position the equivalent of an assistant secretary or military service secretary. They limit the term of the CISA director to 2 5-year terms, which ensure the agency has stable leadership, and de-politicizes the assistant director positions by making them career positions.

A related amendment that my fellow colleague, Mr. Green, cosponsored and I cosponsored, clarifies CISA's authority to conduct continuous threat hunting across the .gov domain. This will increase CISA's ability to protect Federal networks, and allow CISA to provide relevant threat information to critical infrastructure.

Finally, the recommendation to establish a National cyber director within the White House, offered as an amendment to the NDAA

by my colleague and friend, Mr. Langevin, is another legislative proposal I am cosponsoring. This Presidentially-nominated and Senate-confirmed National cyber director would be the principal cybersecurity adviser to the President, tasked with developing, counseling the President on, and supervising implementation of a National cyber strategy, which is sorely needed. This leadership will bring focus to our Nation's cybersecurity as a top strategic priority.

I look forward to hearing from our witnesses today about these Solarium recommendations and many others that fall under the jurisdiction of our subcommittee, as well as working with my colleagues to attach many of the commission's recommendations as possible to the NDAA, another must-pass vehicle, or pass as standalone bills.

I want to thank the Chairman for holding this important hearing. I look forward again to convening in person with my committee colleagues. But I want to take a moment before I close to really command the members of the Solarium Commission: Mr. King, Mr. Gallagher, Ms. Spaulding, Mr. Langevin, and all the others.

I think that what you did is what they did after 9/11 with respect to terrorism. You are anticipating the issues before we have a catastrophic attack. I commend all of you for doing that. That is why I think this is such an important hearing we are having today.

So the bipartisanship that has been shown on this, the lack of politics, and understanding the issues, and understanding the threat and attacking it, it is exactly what we should be doing. I commend everyone for that.

With that, Mr. Chairman, I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Mr. Chairman.

I want to thank all of the commissioners for their work on the Cyberspace Solarium Commission and congratulate them on producing a game-changing report and recommendations that take a bold step in the direction of reinventing our Nation's cybersecurity policy architecture. The commission's legislative proposals accompanying the recommendations are enabling Congress to act quickly and decisively on these urgent measures.

The recommendations I am most interested in hearing about today are, strengthening the Cybersecurity and Infrastructure Security Agency (CISA) and its workforce, evaluating CISA's facilities needs, strengthening the CISA director position and making the assistant directors career, the National cyber director, authorizing CISA to threat hunt on the .gov domain, securing email, developing a strategy to secure email, and modernizing the digital infrastructure of State and local governments and small and mid-sized businesses.

As Ranking Member on the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, my top priority among the commission's recommendations is strengthening and clarifying the Cybersecurity Infrastructure Security Agency's (CISA) authority and vastly increasing its funding to allow it to carry out its role as the Nation's risk manager coordinating the protection of critical infrastructure and Federal agencies and departments from cyber threats. I introduced this recommendation as a bill, which requires CISA to assess what additional resources are necessary to fulfill its mission. This assessment should examine CISA's workforce composition and future demands and report to Congress on the findings.

Under the bill, CISA would also evaluate its current facilities and future needs including accommodating integration of personnel, critical infrastructure partners, and other Department and agency personnel and make recommendations to GSA. GSA must evaluate CISA's recommendations and report to Congress within 30 days on how best to accommodate CISA's mission and goals with commensurate facilities. The facilities evaluation dovetails with the commission's recommendation for an integrated cyber center within CISA.

I reintroduced my bill elevating and strengthening the CISA director position to reflect the significance of the role, making the position the equivalent of an assistant secretary or military service secretary. My bill limits the term of the CISA director to 2, 5-year terms, which ensures the agency has stable leadership. It also depoliticizes the assistant director positions by making them a career.

A related legislative proposal that I am working with colleagues to pass, clarifies CISA's authority to conduct continuous threat hunting across the .gov domain. This will increase CISA's ability to protect Federal networks and allow CISA to provide relevant threat information to critical infrastructure.

Finally, the recommendation to establish a National cyber director within the White House is another legislative proposal I am cosponsoring. This Presidentially-nominated and Senate-confirmed National cyber director would be the principle cybersecurity advisor of the President, tasked with developing, counseling the President on, and supervising the implementation of a National cyber strategy. This leadership will bring focus to our Nation's cybersecurity as a top strategic priority.

I look forward to hearing from our witnesses today about these Solarium recommendations and the many others that fall under the jurisdiction of our subcommittee as well as working with my colleagues to attach many of the commission's recommendations to the National Defense Authorization Act (NDAA), another must-pass vehicle or pass as stand-alone bills.

In closing, I want to thank the Chairman for holding this important hearing and I look forward to again convening in person with my committee colleagues.

[Pause.]

Mr. KATKO. I can't hear anything, Jim——

Mr. LANGEVIN. I was muted, sorry about that. I thank the Ranking Member for his comments, and I want to join with him.

First of all, I want to thank you, Ranking Member, for your leadership on cybersecurity issues, as well as I have been honored to join with the Ranking Member on these cybersecurity issues that are before us, and that are moving their way through the Congress.

I also want to join the Ranking Member in congratulating the newest father in the House, Mr. Gallagher, on the birth of his baby girl, Grace, and wish all the best to your entire family. My congratulations.

Also, I should mention not—when I mentioned Senator King as co-chair along with Congressman Gallagher and Suzanne Spaulding, I glossed over and unintentionally didn't mention Dr. Samantha Ravich's name, but I am going to read bios on each of them in a minute. But I welcome, obviously, Dr. Ravich, and thank her for her participation and valuable contribution that she made to this Solarium Commission report, as well.

So with that, I thank the Ranking Member again.

Members are reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member in their July 8 colloquy.

With that, I ask unanimous consent to waive the committee rule 8(a)(2) for the subcommittee during remote proceedings under the covered period designated by the Speaker under the House Resolution 965.

Without objection, so ordered.

The Chair now recognizes the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chair and Ranking Member, and our witnesses today.

As you know, the Solarium Commission is very forward-thinking, something—I compliment our witnesses for their brilliant work

that they have done on it. I compliment you personally, being a Member of our committee, having served on it.

I have a written testimony for the record. In the interest of time and, again—forward, I will submit it for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JULY 17, 2020

At the outset, I want to acknowledge how fortunate we are, as Members of Congress, to have before us a whole-of-Government, public/private-sector blueprint for defending the Nation against future cyber attacks. Too often, thoughtful documents like this are the product of Monday morning quarterbacking that takes place after a catastrophic event has occurred.

After the September 11 attacks, the 9/11 Commission studied how the organization and policies of the Federal Government led to its failure to predict, prevent, and prepare for the attacks, and made a series of recommendations to reorganize the Government and build lacking capabilities.

After Hurricane Katrina, Congress identified critical deficiencies in Federal emergency management policy and overhauled it in the Post-Katrina Emergency Management Reform Act. After the Russian government attempted to meddle in our elections in 2016, I co-led a Task Force on Election Security to understand vulnerabilities in our election infrastructure, and we issued a report and recommendations to address them. Soon, I expect we will establish a commission to study the failures of the Federal Government that have led to its inept response to the COVID–19 pandemic.

We are lucky we are here today not to discuss a tragedy, but rather, how to organize the Federal Government to effectively avoid one. At this time, the responsibility for leadership on Federal cybersecurity policy rests with Congress.

Although there are many well-intentioned, capable people working hard to advance sound cybersecurity policy throughout the Executive branch, the lack of consistent leadership from the White House has stunted progress. Over 2 years ago, for example, the White House green-lighted the elimination of its Cyber Security Coordinator. The result is a lack of effective coordination among Federal agencies who compete for cybersecurity authorities, responsibilities, and associated budgets—and Federal agencies approaching Congress with conflicting priorities. The time has come for that to stop.

Toward that end, I appreciate and support the commission's recommendation that Congress establish a National cyber director. I understand Congressman Langevin has authored legislation to implement that recommendation and has also submitted it as an amendment to the NDAA. I fully support both efforts.

I similarly appreciate the commission's recommendations regarding strengthening the Cybersecurity and Infrastructure Security Agency and more clearly defining the roles and responsibilities of CISA and sector risk management agencies. Right-sizing CISA's budget and equipping it with the authorities necessary to carry out its mission to secure Federal networks, while also supporting critical infrastructure, has been a bipartisan priority of committee Members.

I am particularly interested in hearing Ms. Spaulding's thoughts on these recommendations given her perspective as the former under secretary of the National Protection and Programs Directorate.

Additionally, I am interested in discussing commission recommendations related to implementing a "carrot and stick" approach to encourage private-sector collaboration with the Federal Government's cybersecurity and defense efforts, particularly the proposed codification of "systemically important critical infrastructure."

Finally, I would be remiss if I did not address the commission's observation that Congress' fractured jurisdiction over cybersecurity frustrates efforts to achieve a comprehensive, cohesive approach to cybersecurity. I agree. While I disagree with the commission's recommendation on that point, rest assured that I am working to address the underlying problem.

Mr. LANGEVIN. I thank you, Chairman Thompson, and I thank you for your leadership, both of the full committee on a whole host of issues, but for your leadership and support on cybersecurity, in particular. You have been incredible, and I thank you for that, your leadership there.

I understand that Mr. Rogers is not able to join us. Is that correct?

OK, I believe that is the case. So if Mr. Rogers is not here, then with that, again, I thank the Chairman, and I now welcome our panel of witnesses.

First I would again like to welcome Senator Angus King, the former Governor of Maine, who served as co-chair of the Solarium Commission. Senator King currently sits on the Senate Armed Services Committee and the Senate Committee on Intelligence, among others, and has been a vocal leader on cybersecurity throughout his tenure. I welcome the Senator here.

Next, Representative Mike Gallagher, co-chair of the Cyberspace Solarium Commission and current Member of the House of Representatives for the 8th district of Wisconsin. Mr. Gallagher is a Member of the House Armed Services Committee, and a former Member of this committee. I would also like to welcome Mr. Gallagher back to the committee again, back to Congress after his paternity leave, and I thank him for interrupting his paternity leave, being here with us.

Again, Mr. Gallagher, congratulations on your daughter, Grace. In addition to being a huge Packers fan, I know they will be incredibly very proud of their father for the work that you have done with the commission.

Next we will hear from Suzanne Spaulding, a commissioner for the Cyber Solarium Commission and senior adviser at the Center for Strategic and International Studies. Before that Ms. Spaulding served as the under secretary for the National Protection and Programs Directorate at the Department of Homeland Security, which is now the Cybersecurity and Infrastructure Security Agency, or CISA. So I look forward to hearing her unique perspective and her emphasis on how civics education is an essential component of resiliency.

Finally, we have Dr. Samantha Ravich, a commissioner of the Cyber Solarium Commission, and former deputy national security adviser during the Bush administration. Dr. Ravich is currently serving as the chair of the Foundation for Defense of Democracy's Center for Cyber and Technology Innovation. I deeply appreciate her coming to speak with us today, and for her incredible contributions to, I think, a continuity of the economy.

With that, without objection, the witnesses' full statements will be inserted into the record. I now ask each witness to summarize their statements for 5 minutes, beginning with Senator King.

Senator King, it was a pleasure serving with you on the Solarium Commission, and I look forward to hearing your comments here today. You are now recognized.

STATEMENT OF HON. ANGUS KING, A UNITED STATES SENATOR FROM THE STATE OF MAINE, AND CO-CHAIR, CYBERSPACE SOLARIUM COMMISSION

Senator KING. Mr. Chairman, thank you very much for holding this hearing. It really means a lot to the work of the commission to be taking this next step.

I would say that I use this technology every Wednesday morning for the Senate Prayer Breakfast, and it seems to work very effec-

tively, except when we try to sing hymns. So I think, as long as we don't sing any hymns today, we will be OK.

I appreciate your time. I also appreciate the involvement and engagement of Representative Katko, who has—who outlined a series of bills, all of which we think are important, and I really want to thank him for his work.

I want to give a little bit of background. The first thing to observe is that, in the last 6 months, we have learned that the unthinkable can happen. The unthinkable can happen. In the last 48 hours, we have learned that cyber is an ever-present threat.

As the Chairman mentioned in his opening statement, the attack on Twitter, which was a commercial one, but also the apparent attack by the Russians on the security of our pursuit of a vaccine, it is just a reminder that this is not an academic question, but it is something that is really a—front and center in threats that this country is facing.

The commission that you mentioned several times, and that Mike Gallagher and I were privileged to co-chair, was set up in the 2019 National Defense Act. It had a unique structure. It had 4 sitting Members of Congress, 4 members from the Executive, and 6 members from the private sector. I can honestly say that, throughout our deliberations—and we had over 30 meetings, had 400 interviews, thousands of pages of documents—there was not a single moment of partisanship or of partisan discussion. In fact, I have no idea the party affiliation of the other 10 members of the commission who aren't Members of Congress. That, it seems to me, speaks to the importance and overriding power of this issue that really must unite us.

So that was the work of the commission. We went through, as I mentioned, 30 meetings together. We had stress tests. We had a sort-of contest of ideas in the middle of last summer, and we really tried to approach this with fresh eyes to look at, really, 2 basic questions: What should our strategy be, and what should our organizational structure be to—both to protect, to prepare, and to prevent cyber attacks?

As you mentioned, there are 82 recommendations in the report, 54 of which have been converted into legislative recommendations and presented to the various committees of both the House and the Senate in the form of fully-drafted legislative proposals.

What we are talking about is what is called layered cyber deterrence, and that means resilience so that our adversaries feel that there is not much to be gained by attacking us because of our security and our protection of our systems, but also a declaratory policy that, if attacked, we will respond.

One of the deficiencies in our cyber posture over the last several decades has been we have a deterrence strategy for a major sort-of threshold of use of force, but we haven't had a strategy, and we haven't articulated a doctrine that would provide a deterrent for less than use-of-force kind of cyber attacks.

For that reason, as I have said many times, we are a cheap date. Our adversaries don't—they don't compute the cost of attacking us. That has to change. That is the strategic picture.

The organizational picture is that cyber is scattered throughout the Federal Government. It is in the Defense Department, it is in

the intelligence community, it is in DHS, it is in the FBI. We really need to try to straighten out the organizational structure.

One of my observations has been that messy structure equals messy policy. That leaves with the creation of a National cyber director in the White House, appointed by the President, confirmed by the Senate, which will give continuity to this important interest. We want somebody in the Federal Government who wakes up every morning with the mission of protecting this country in cyber space.

Finally, one of the crucial elements that we tried to address in the report—and frankly, it is a difficult one—is the relationship between the Government and the private sector. Eighty-five percent of the target space in cyber is in the private sector. The private-sector computers, whether they are in the financial sector, or energy, or transportation, or telecommunications, they are the front line troops in this battle. Yet it is the Federal Government that often has the resources and the expertise and the ability to pull together this information in order to protect our country.

So I will go back to—I think one of you stated—I think Mr. Katko, Representative Katko, stated and Mike Gallagher said this was our mission from the beginning. We wanted to be the 9/11 Commission report without 9/11. That is really what we have tried to focus upon in this project.

So I want to thank the committee. Now is the time to put these recommendations into law, into practice, if we are going to protect our country in the way that we all believe—it can be done, and certainly it should be done. The unthinkable can happen. But we can be prepared, we can prevent, and we can protect this country.

Thank you, Mr. Chairman.

[The joint prepared statement of Sen. King, Hon. Gallagher, Ms. Ravich and Ms. Spaulding follows:]

JOINT PREPARED STATEMENT OF SENATOR ANGUS KING, HONORABLE MIKE GALLAGHER, SAMANTHA RAVICH, AND SUZANNE SPAULDING

JULY 17, 2020

The Cyberspace Solarium Commission (CSC) was established by the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyber space against cyber attacks of significant consequences."

The Cyberspace Solarium Commission consists of 14 commissioners, including 4 currently-serving legislators, 4 Executive branch leaders, and 6 recognized experts with backgrounds in industry, academia, and Government service. Senator Angus King and Representative Mike Gallagher serve as the co-chairmen. The commissioners spent the past 13 months studying the issues, investigating solutions, and deliberating on courses of action to produce a comprehensive report. Our commissioners convened nearly every Monday that Congress was in session for over a year, achieving an impressive benchmark of 30 meetings. The staff conducted nearly 400 interviews with industry, Federal, State, and local governments, academia, non-Governmental organizations, and international partners. The commissioners also recruited our Nation's leading cybersecurity professionals and academic minds to vigorously stress test the findings and red-teamed the different policy options in an effort to distill the optimal approach to securing the United States in cyber space. The final report was presented to the public on March 11, 2020 and identified 82 specific recommendations. These bi-partisan recommendations were then subsequently turned into 52 legislative proposals that have been shared with the appropriate committees in the Senate and House of Representatives.

Ultimately, the commission developed a strategic approach of "layered cyber deterrence" with the objectives of actively shaping behavior in cyber space, denying

benefits to adversaries who exploit this domain, and imposing real costs against those who target America's economic and democratic institutions in and through cyber space. Our critical infrastructure—the systems, assets, and entities that underpin our National security, economic security, and public health and safety—are increasingly threatened by malicious cyber actors. Effective critical infrastructure security and resilience requires reducing the consequences of disruption, minimizing vulnerability, and disrupting adversary operations that seek to hold our assets at risk. We believe the future of the U.S. economy and our National security requires both the Executive branch and Congress work in tandem to prioritize and grant the following recommendations.

First and foremost, the commission found that the Federal Government lacks consistent and institutionalized leadership, as well as a cohesive, clear strategic vision on cybersecurity. As a result, we recommend that Congress establish a National cyber director in the Executive Office of the President to centralize and coordinate the cybersecurity mission at the National level. The National cyber director would work with Federal departments and agencies to bring coherence in the development of cybersecurity policy and strategy and in its execution. The position would provide clear leadership in the White House and signal cybersecurity as an enduring priority in U.S. National security strategy.

Second, the Government must continue to improve the resourcing, authorities, and organization of the Cybersecurity and Infrastructure Security Agency (CISA) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience. We recommend empowering CISA with tools to strengthen public-private partnership. Of particular value would be the authorities needed to aid in responding to attempted attacks on critical infrastructure from a variety of actors ranging from nation-states to criminals. Currently, the U.S. Government's authorities are limited exclusively to certain criminal contexts, where evidence of a compromise exists, and do not address instances in which critical infrastructure systems are vulnerable to a cyber attack. To address this gap, Congress should grant CISA subpoena authority in support of their threat and asset response activities, while ensuring appropriate liability protections for cooperating private-sector network owners.

Third, elements of the U.S. Government and the private sector often lack the tools necessary for successful collaboration to counter and mitigate a malicious nation-state cyber campaign. To address this shortcoming, the Executive branch should establish a Joint Cyber Planning Office under CISA to coordinate cybersecurity planning and readiness across the Federal Government and between the public and private sectors for significant cyber incidents and malicious cyber campaigns. Within a similar vein, Congress should also direct the U.S. Government to plan and execute a National-level cyber table-top exercise on a biennial basis that involves senior leaders from the Executive branch, Congress, State governments, and the private sector, as well as international partners, to build muscle memory for key decision makers and develop new solutions and strengthen our collective defense.

Fourth, the United States must take immediate steps to ensure our critical infrastructure sectors can withstand and quickly respond to and recover from a significant cyber incident. Resilience against such attacks is critical in reducing benefits that our adversaries can expect from their operations—whether disruption, intellectual property theft, or espionage. Congress should direct the Executive branch to develop a Continuity of the Economy Plan. This plan should include the Federal Government, SLTT entities and private stakeholders who can collectively identify the resources and authorities needed to rapidly restart our economy after a major disruption. In addition, the commission recommends establishing a Cyber State of Distress tied to a Cyber Response and Recovery Fund, giving the Government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical National functions can continue to operate amidst disruption or crisis.

Fifth, the commission recommends 2 relevant initiatives to reshape the cyber ecosystem toward greater security for all Americans. The first, the creation of a National Cybersecurity Certification and Labeling Authority, would help create standards and transparency that will allow consumers of technology products and services to use the power of their purses over time to demand more security and less vulnerability in the technologies they buy. Furthermore, Congress should appropriate funds to the Department of Homeland Security (DHS), in partnership with the Department of Energy, Office of the Director of National Intelligence (ODNI), and the Department of Defense (DoD), to competitively select, designate, and fund up to 3 Critical Technology Security Centers in order to centralize efforts directed

toward evaluating and testing security of devices and technologies that underpin our networks and critical infrastructure.

Sixth, the U.S. intelligence community is not currently resourced or aligned to adequately support the private sector in cyber defense and security. While the intelligence community is formidable in informing security operations in instances when the U.S. Government is the defender, its policies and procedures are not aligned to intelligence collection on behalf of private entities, which constitutes around 85 percent of our critical infrastructure. To that end, Congress should direct the Executive branch to conduct a 6-month comprehensive review of intelligence policies, procedures, and resources to identify and address key limitations in order to improve the intelligence community's ability to provide intelligence support to the private sector.

Throughout the process of developing its recommendations, the commission always considered Congress as its "customer." Through the NDAA, Congress tasked the commission to investigate cyber threats that undermine American power and prosperity, to determine an appropriate strategic approach to protect the Nation in cyber space, and to identify policy and legislative solutions. As commissioners, we are here today to share what we learned, advocate for our recommendations, and work to assist you in any way we can to solve this serious and complex challenge.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID–19 pandemic has been a big wakeup call for us all because it illustrates the challenge of ensuring resilience and continuity in a connected world. It is an example of a type of non-traditional National security crisis that spreads rapidly through the system, stressing everything from emergency services and supply chains to basic human needs. The pandemic has produced cascading effects and high levels of uncertainty. This situation undermines normal policy-making processes and forces decision makers to craft hasty and ad hoc emergency responses. Complex emergencies that rely on coordinated action beyond traditional agency responses and processes illustrate what the commission saw as an acute threat to the security of the United States.

The lessons the country is still learning from the on-going pandemic are not perfectly analogous to a significant cyber attack, but are highly illustrative of the possible consequences due to several similarities between the 2 types of events. First, both the pandemic and a significant cyber attack are global in nature. Second, both the COVID–19 pandemic and a significant cyber attack require a whole-of-Nation response and are likely to challenge existing incident management doctrine and coordination mechanisms. Finally, and perhaps most importantly, prevention is far cheaper and more effective than response.

The global health crisis has reinforced the urgency of many of the core recommendations in the commission's March 2020 report. Responding to complex emergencies will require a balance between response agility and institutional resilience in the economy and critical infrastructure sectors. It relies on strategic leadership and coordination from the highest offices in Government, underscoring the importance of a National Cyber Director. It relies on a strong understanding of the risks posed by a crisis and a data-driven approach to mitigating those risks before, during, and after a crisis, validating the commission's recommendations. Specifically, successfully responding to a crisis relies on clear roles and responsibilities for critical actors in the public and private sector as well as established, exercised relationships and plans, highlighting the importance of Continuity of the Economy planning.

THE CHALLENGE

For the last 20 years, adversaries have used cyber space to attack American power and interests. Our adversaries have not internalized the message that, if they attack us in cyber space, they will pay a price. The more connected and prosperous our society has become, the more vulnerable we are to rival great powers, rogue states, extremists, and criminals. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the private sector and the public at large.

The American public relies on critical infrastructure, roughly 85 percent of which—according to the Government Accountability Office—is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment facilities to hospitals—are connected and vulnerable. There are also new industries and services, like cloud computing, which our society relies on for economic growth. As we saw last year, hackers don't just target the U.S. Government and military personnel—they increasingly target our cities and counties with malware and ransomware attacks.

Creating a secure Nation in the 21st Century requires an interconnected system of both public and private networks secure from state and non-state threats. China commits rampant intellectual property theft to help their businesses close the technological gap, costing non-Chinese firms over $300 billion per year. Massive data breaches, including those suffered by Equifax, Marriott, and the Office of Personnel Management (OPM), enable Chinese spies to collect data on over a hundred million Americans.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In spring 2014, Russian-linked groups launched a campaign to disrupt Ukrainian elections that included attempts at altering vote tallies, disrupting election results through distributed-denial-of-service attacks, and smearing candidates by releasing hacked emails. They continue to spread hate and disinformation on social media to polarize free societies. But they have not stopped there. The 2017 NotPetya malware attack spread globally, Iran and North Korea attack U.S. and allied interests through cyber space. Iranian cyber operations have targeted the energy industry, entertainment sector, and financial institutions. There are also documented cases of Iranian APTs targeting dams in the United States with distributed-denial-of-service attacks. North Korea exploits global connectivity to skirt sanctions and sustain an isolated, corrupt regime. The 2017 WannaCry ransomware attacks hit over 300,000 computers in 150 countries, including temporarily disrupting U.K. hospitals. According to United Nations estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year.

A new class of criminal thrives in this environment. Taking advantage of widespread cyber capabilities revealed by major state intrusions, criminal groups are migrating toward a "crime-as-a-service" model in which threat groups purchase and exchange malicious code on the dark web. In 2019, ransomware incidents grew over 300 percent compared to 2018 and hit over 40 U.S. municipalities. More recently, opportunistic hackers have hijacked hospitals and health care systems during the COVID–19 pandemic, taking advantage of poorly protected systems at their most vulnerable state. Remote access and the expansion of the work-from-home economy continues to increase the threat vectors for criminal actors as the world changes to meet the needs of a global pandemic.

STRATEGIC APPROACH

The strategy put forth by the Cyberspace Solarium Commission combines a number of traditional deterrence mechanisms and extends their use beyond the Government to develop a whole-of-Nation approach. It also updates and strengthens our declaratory policy for cyber attacks both above and below the level of armed attack. The United States must demonstrate its ability to impose costs while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking America in cyber space.

Since America relies on critical infrastructure that is primarily owned and operated by the private sector, the Government cannot defend the Nation alone. The public and private sectors, along with key international partners, must collaborate to build resilience and reshape the cyber ecosystem in a manner that increases its security, while imposing costs against malicious actors and preventing attacks of significant consequence.

Cyber deterrence is not nuclear deterrence. The fact is, no action will stop every hack. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly to benefit from targeting American interests through cyber space. Layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries (e.g., denial and cost imposition) with forms of influence optimized for a connected era, such as promoting norms that encourage restraint and incentivize responsible behavior in cyber space. Strategic discussions all too often prioritize narrow definitions of deterrence that fail to consider how technology is changing society. In a connected world, those states that harness the power of cooperative, networked relationships gain a position of advantage and inherent leverage. The more connected a state is to others and the more resilient its infrastructure, the more powerful it becomes. This power requires secure connections and stable expectations between leading states about what is and is not acceptable behavior in cyber space. It requires shaping adversary behavior not only by imposing costs but also by changing the ecosystem in which competition occurs. It requires international engagement and collaboration with the private sector.

Layered cyber deterrence emphasizes working with the private sector to efficiently coordinate how the Nation responds with speed and agility to emerging threats. The Federal Government alone cannot fund or solve the challenge of adversaries attack-

ing the networks on which America and its allies and partners rely. It requires collaboration with State and local authorities, leading business sectors, and international partners, all within the rule of law. This strategy also contemplates the planning needed to ensure the continuity of the economy and the ability of the United States to rebound in the aftermath of a major, Nation-wide cyber attack of significant consequence. Such planning adds depth to deterrence by assuring the American people, allies, and even our adversaries that the United States will have both the will and capability to respond to any attack on our interests. These 3 deterrent layers are supported by 6 policy pillars that organize the 82 recommendations that collectively represent the means to implement our strategy.

THE NEED TO REORGANIZE THE U.S. GOVERNMENT (PILLAR 1)

The Legislative and Executive branches must align their authorities and capabilities to produce the speed and agility required to defend America in cyber space. Greater collaboration and integration in the planning, resourcing, and employment of Government cyber resources between the public and private sectors is a foundational requirement. The U.S. Government needs strategic continuity and unity of effort to achieve the goal of layered cyber deterrence called for by the Cyberspace Solarium Commission. These actions require adjusting the authorities and alignment of fundamental processes the U.S. Government applies to defend its interests in cyber space.

First, Congress must reestablish clear oversight responsibility and authority over cyber space within the Legislative branch. The large number of committees and subcommittees claiming some form of jurisdiction over cyber issues is actively impeding action and clarity of oversight. By centralizing responsibility in the new House Permanent Select and Senate Select Committees on Cybersecurity, Congress will be empowered to provide coherent oversight to Government strategy and activity in cyber space.

Next, select entities in the Executive branch that deal with cybersecurity must be restructured and streamlined. Multiple departments and agencies have a wide range of responsibilities for securing cyber space. These responsibilities tend to overlap and at times conflict. The departments and agencies tend to compete for resources and authorities resulting in conflicting efforts that produce diminishing marginal returns. Establishing a National cyber director within the Executive Office of the President would consolidate accountability for harmonizing the Executive branch's policies, budgets, and responsibilities in cyber space while implementing strategic guidance from the President and Congress.

In addition to this National cyber director, a properly-resourced and empowered CISA will be critical to achieving coherence in the planning and deployment of Government cyber resources. Multiple administrations and Congressional sessions have worked to establish CISA as a keystone of National cybersecurity efforts, but work still needs to be done to realize our ambitious vision for this critical organization. That includes strengthening its director with a 5-year term and elevated Executive status, adequately resourcing its programs to engage with the private sector while managing National risk, and securing sufficient facilities and required authorities for its vital and growing mission. These changes will remove key limitations in CISA's ability to forge a greater public-private partnership and its mission to secure critical infrastructure.

Finally, the U.S. Government must more effectively recruit, develop, and retain a cyber workforce capable of building a defensible digital ecosystem and deploying all instruments of National power in cyber space. That will require designing innovative programs and partnerships to develop the workforce, supporting and expanding good programs where they are already in place, and connecting with a diverse pool of promising talent. In some cases, success in building a robust Federal workforce depends on stakeholders outside the Federal Government, like educators, nonprofits, and businesses. Policy makers should support these important partners by providing the tools they need to be effective, like classroom-ready resources, incentives for research on workforce dynamics, and clear routes for collaborating with the Government.

DETERRENCE BY DENIAL (PILLARS 3/4/5)

Denying adversaries' benefits of their cyber campaigns is a critical aspect of "Layered Cyber Deterrence." By ensuring the resilience of critical pillars of National power, reducing our National vulnerability, and disrupting threats through operationalizing collaboration between the Government and private sector we can effectively force adversaries to make difficult decisions regarding resourcing, access, and capabilities. The U.S. Government support must be better informed through a

Joint Collaborative Environment that would pool public-private sources of threat information to be coordinated through a Joint Cyber Planning Office and an Integrated Cyber Center at DHS. Paired with our recommendation to conduct a Biennial National Cyber Tabletop Exercise, that involves senior leaders from the Executive branch, Congress, State governments, and the private sector as well as international partners—the United States and her allies will be in a forward-leaning position and ready to lead.

Today, under the direction of Presidential Policy Directive 21, sector-specific agencies are the lead Federal agencies tasked with day-to-day engagement with the private sector on security and resilience. However, there are significant imbalances and inconsistencies in both the capacity and the willingness of these agencies to manage sector-specific risks and participate in Government-wide efforts. In addition, the lack of clarity and consistency concerning the responsibilities and requirements for these agencies continues to cause confusion, redundancy, and gaps in resilience efforts. For this reason, the commission recommends that Congress codify sector-specific agencies in law as "sector risk management agencies" to ensure consistency of effort across critical infrastructure sectors and ensure that these agencies are resourced to meet growing needs.

Denying adversaries' benefits starts with ensuring that our most critical targets are able to withstand and quickly recover from cyber attacks. In other words, we must build resilience. Effective National resilience efforts fundamentally depend on the ability of the United States to accurately understand, assess, and manage National cyber risk. Current efforts to assess and manage risk at the National level are relatively new and are significantly hindered by resource limitations, immaturity of process, and inconsistent capacity across departments and agencies that participate in National resilience efforts. Today, while the U.S. Government plans for continuity of operations and continuity of Government, no similar planning exists to ensure continuity of the economy. This must change, and the planning process should analyze National critical functions, outlining priorities for response and recovery, and identifying areas for resilience investments. In doing so, the continuity of the economy plan should identify areas for preservation of data and mechanisms for extending short-term credit to ensure recovery efforts. Additionally, Congress should also provide CISA with the necessary support to expand its current capability to issue Cyber State of Distress declarations in conjunction with Cyber Response and Recovery Funding. Furthermore, providing CISA with Administrative Subpoena Authority will dramatically improve the Federal Government's ability to actively notify critical infrastructure owners and operators that are on the front lines and being attacked by our adversaries who are largely acting with impunity.

Denying adversaries' benefits also must lie in driving down our National cyber vulnerability at scale. Today, vulnerability in our cyber ecosystem is derived not only from technology, but also human behavior and processes. The commission sought means to improve the security of both the technological and human aspects at scale. Moving the technology markets to emphasize security requires creating greater transparency about the security characteristics of technologies consumers buy. This is why the commission recommends the creation of a National Cybersecurity Certification and Labeling Authority and Critical Technology Security Centers to collectively to develop and facilitate authoritative, easy-to-understand security certifications and labels for technology products. By helping consumers make more informed technology purchases, the market will become a difficult place for vendors who do not prioritize security to do business.

Layered cyber deterrence includes shaping cyber actors' behavior through strengthened norms of responsible state behavior and non-military instruments of power, such as law enforcement, sanctions, diplomatic engagement and capacity building. A system of norms, based on international engagement and enforced through these instruments of power, helps secure American interests in cyber space.

To strengthen cyber norms and build a like-minded international coalition to enforce them, the commission recommends Congress create and adequately resource the Bureau of Cyberspace Security and Emerging Technologies led by an assistant secretary of state. The Bureau would bring dedicated cyber leadership and coordination to the Department of State.

Leading internationally also means having strong and coordinated representation in bodies that set global technical standards, therefore, Congress should sufficiently resource the National Institute of Standards and Technology to bolster participation in these bodies. American values, interests, and security are strengthened when international technical standards are developed and set with active U.S. participation. Engaging fully means we must also facilitate robust and integrated participation from across the Federal Government, academia, civil society, and industry; the United States is at its best when we draw input from all our experts.

In parallel to robust participation in multilateral bodies, law enforcement activities also provide fruitful ground on which to work with international partners and allies to hold adversaries accountable. We recommend providing the Department of Justice Office of International Affairs with administrative subpoena authority streamlines the Mutual Legal Assistance Treaties process, enabling U.S. law enforcement to help allies and partners prosecute cyber criminals. Additionally, the commission recommends Congress create and fund 12 additional Federal Bureau of Investigation cyber assistant legal attachés to facilitate intelligence sharing and help coordinate joint enforcement actions. Investing in these types of international law enforcement activities improve the credibility of enforcement and signal America's commitment to bring malicious actors to justice.

DETERRENCE BY COST IMPOSITION (PILLAR 6)

A key layer of the commission's strategy outlines how to impose costs to deter malicious adversary behavior and reduce on-going adversary activities short of armed conflict. As part of this effort, the commission puts forth 2 key recommendations: To conduct a force structure assessment of the Cyber Mission Force (CMF); and to conduct a cybersecurity and vulnerability assessments of conventional weapons systems and of the nuclear command, control, and communications enterprise.

Today, the United States has not created credible and sufficient costs against malicious adversary behavior below the level of armed attack—even as the United States has prevented cyber attacks of significant consequences. Our Nation must shift from responding to malicious behavior after it has already occurred to proactively observing, pursuing, and countering adversary operations. This should include imposing costs to change adversary behavior using all instruments of National power in accordance with international law.

To achieve these ends, the United States must ensure that it has sufficient cyber forces to accomplish strategic objectives in and through cyber space. The CMF is currently considered at full operational capability (FOC) with 133 teams comprising a total of approximately 6,200 individuals. However, these requirements were defined in 2013, well before our Nation experienced or observed some of the key events that have shaped our Government's understanding of the cyber threat. The FOC determination for the CMF was also well before the development of the Department of Defense's (DoD) defend forward strategy. Therefore, we recommend Congress direct the DoD to conduct a force structure assessment of the CMF to ensure the United States has the appropriate force structure and capabilities in light of growing mission requirements. This should include an assessment of the resource implications for intelligence agencies in their combat support agency roles.

If deterrence fails, the United States must also be confident that its military capabilities will work as intended. However, deterrence across all of the domains of warfare is undermined, and the ability of the United States to prevail in crisis and conflict is threatened, if adversaries can hold key military systems and functions, including nuclear systems, at risk through cyber means. Therefore, the commission recommends Congress direct the DoD to conduct a cybersecurity vulnerability assessment of all segments of nuclear command, control, and communications systems and continually assess weapon systems' cyber vulnerabilities.

Our hope is that, by implementing these recommendations, we can ensure our Nation is willing and able to counter and reduce malicious adversary behavior below the level of armed conflict, impose costs to deter significant cyber attacks, and, if necessary, fight and win in crisis and conflict.

CONCLUSION

The recommendations put forward by the commission are an important first step to denying adversaries the ability to hold America hostage in cyber space and will be critical to our efforts to re-establish deterrence in cyber space. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. Cyber operations have become a weapon of choice for adversaries seeking to hold the U.S. economy and National security at risk. Near peer adversaries such as China and Russia are attempting to reassert their influence regionally and globally, using cyber and influence operations to undermine American security interests. The concept of deterrence must evolve to address this new strategic landscape. Reducing the scope and severity of these adversary cyber operations and campaigns requires adopting the commission's strategy of layered cyber deterrence—improving our ability to defend our critical infrastructure and investing in an effective public-private collaboration.

To this end, we believe this committee must prioritize a selection of the commission's recommendations that include: Strengthening the Government with a National cyber director, an empowered CISA, a new Joint Cyber Planning Office, and improved intelligence support to the private sector; building resilience with Continuity of the Economy Planning, and a codified "Cyber State of Distress" tied to a "Cyber Response and Recovery Fund"; and, an improved cyber ecosystem with a National Cybersecurity Certification and Labeling Authority, and the designation of Critical Technology Security Centers.

The 2019 NDAA charted the U.S. Cyberspace Solarium Commission to address 2 fundamental questions: What strategic approach will defend the United States against cyber attacks of significant consequence? And what policies and legislation are required to implement that strategy? The commission has delivered on its mission in the promulgation of "layered cyber deterrence" strategy and the corresponding legislative proposals. We now need your help to enact these key legislative proposals as they will empower the Government and the private sector to act with speed and agility in securing our cyber future.

Mr. LANGEVIN. Thank you, Senator King. Again, thank you for your leadership on the Cyberspace Solarium Commission. As one of the co-chairs, you did an outstanding job, and I was proud to serve on that commission. Thank you for your testimony.

Now I recognize Congressman Gallagher to summarize the commission statement for 5 minutes.

Mr. Gallagher, you are recognized.

STATEMENT OF HON. MICHAEL GALLAGHER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN, AND CO-CHAIR, CYBERSPACE SOLARIUM COMMISSION

Mr. GALLAGHER. Thank you, Chairman Langevin, not only for chairing this hearing today, but for your immense contributions to the commission. Our final report would not have been possible, were it not for your leadership. In many areas we were building upon work that you have been doing for the last decade. So it was really great to get to work with you.

Thank you to Ranking Member Katko for your engagement from the start of this effort, for meeting with us and our staff multiple times, and for your leadership on these issues.

Thank you, Chairman Thompson, for giving us this forum today.

Let me just echo what my co-chair, Senator King—who is married to a Packers fan, I should note—said at the outset, which is, you know, we were—we come from different parties, we were appointed by partisans on different sides, and certainly the outside experts, Commissioner Spaulding and Ravich were, as well. But it would have been impossible to determine the party affiliations if you were just to listen to one of the many debates we had as we met as a commission.

I think what came out of this process was a truly nonpartisan report that attempts to put the interests of the country ahead of any parochial or political interests. So this really has been an issue that every Presidential administration for the past 25 years, Democrats and Republicans, has tried to figure out: How do we defend U.S. interests and promote U.S. values in cyber space?

Despite these well-intentioned efforts, our networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state-sponsored intellectual property theft via cyber means. A major cyber attack on our Nation's critical infrastructure and our economic system would create chaos and lasting damage.

So, in an effort to forestall such a future, the Cyberspace Solarium Commission examined a broad range of structures and policies that could more effectively defend our Nation in cyber space.

I should admit our public relations plan, when we released the report publicly on March 11, 2020, did not factor in a global pandemic taking over the conversation. But that is all the more reason why it is important to have hearings like this today. We hope that, not only will you digest our full report, but also read our pandemic annex.

But I just would highlight a few of the commission's key recommendations up front here.

One, reform the U.S. Government structure and organizations for cybersecurity. This starts with establishing a National cyber director situated within the Executive office of the President, who is Senate-confirmed and supported by the Office of the National Cyber Director, as Senator King outlined.

It also continues with strengthening CISA, as Representative Katko outlined, so that CISA can better serve as that central core element to support and integrate the Federal, State, and local, and private-sector cybersecurity efforts.

I think it is important to note that the overall approach we are taking here is not to create a bunch of new organizations within the Federal Government, but rather an attempt to elevate and empower existing organizations like CISA, who have made important progress in recent years, but need more support from Congress.

Second, I just would say we have a variety of recommendations on promoting National resilience, specifically that Congress should codify the roles of sector-specific agencies, focusing National risk management efforts, and also developing and maintaining a continuity-of-the-economy planning process so that we think through the unthinkable now, so we are not having to make things up on the fly in the wake of a cyber 9/11.

Then third and finally, I just would highlight the need to reshape the cyber ecosystem toward greater security. We are recommending, for example, that Congress establish and fund a National cybersecurity certification and labeling process to establish and manage a program on security certification and labeling of ICT products, as well as establish a Bureau of Cyber Statistics charged with collecting and providing data on cybersecurity.

These recommendations, and many more like them in the report, are all designed to implement the commission's recommended strategy of layered cyber deterrence, which is our theory for how we evolve into a harder target, a better ally, and a worse enemy in how we better defend our Nation, our economy, and our way of life in cyber space.

So thank you for giving us the opportunity to present our findings here today. We look forward to the debate. Again, I just want to highlight not only the contributions of the commissioners that you will hear from, but also our wonderful staff who has dedicated a year of their life to this important effort.

I yield back.

Mr. LANGEVIN. Thank you, Chairman Gallagher. Again, I commend you for your leadership on the Solarium Commission. Both you and Senator King made a great team in co-chairing the Cyber-

space Solarium Commission. We are greatly indebted to you for your work and service.

With that, I thank you for your testimony, and I now recognize Ms. Spaulding to summarize the commission's statement for 5 minutes.

[Pause.]

Mr. LANGEVIN. Commissioner Spaulding, you are muted. We need to unmute you.

There you go, you are unmuted.

STATEMENT OF SUZANNE SPAULDING, COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Ms. SPAULDING. Thank you, Chairman Langevin. Thank you, Chairman Thompson, Ranking Member Katko, and Members of the committee. Thank you for this opportunity to be here today to testify. It is an honor to be here with my fellow witnesses.

Particularly, Chairman Langevin, an honor it was to work with you again, having worked with you in 2007 on the Commission for Cybersecurity for the 44th President, which you co-chaired. I want to thank you for your long, outstanding leadership on cybersecurity issues.

The bipartisanship, nonpartisanship which you have heard today, really, that tone was set at the top by our 2 co-chairs, Senator King and Congressman Gallagher. So thank you for that.

Of course, a pleasure to work with Commissioner Ravich.

I want touch briefly today on 3 key areas that I think should and must be acted on very quickly, given the vulnerabilities particularly, as we have noted, with the pandemic.

The first is strengthening DHS's Cybersecurity and Infrastructure Security Agency, or CISA, as the organization that I once led at DHS is now called, thanks in no small measure to the work of this committee and Chairman Thompson, and I thank you for that.

With malicious cyber actors targeting hospitals, vaccine development, and governments at every level, and a stay-at-home work force presenting a massive attack surface, CISA's work has never been more important. This is why the commission urges Congress to provide CISA promptly with the resources and authorities, including administrative subpoena authority, that it needs to be the National risk manager; to serve as the central civilian cybersecurity authority to support Federal, State, local, territorial, and Tribal governments, and the private sector; to conduct continuity of the economy planning, a concept that Commissioner Ravich brought to the commission, so important; identify systemically important critical infrastructure; and coordinate planning and readiness across Government and the private sector.

Second, with regard to improving the cyber ecosystem and reducing vulnerabilities, the commission turned first to improving the efficiency of the market. We looked at why isn't the market performing its function of driving better cybersecurity?

A key reason, we determined, was that markets need information to operate effectively. So we ask that Congress establish that National cybersecurity certification and labeling authority, the kind of underwriter laboratories effort that Congressman Gallagher, mentioned; publish guidelines for secure cloud services; create that Bu-

reau of Cyber Statistics; promote a more effective and robust cyber insurance market; and pass a National data breach notification law.

Finally, I believe one of the most important pillars in the report is resilience. We need to reduce the benefit side in the adversary's cost-benefit analysis. Often that means reducing our dependence upon those network systems, developing redundancies, maybe even analog systems. Paper ballots, for example, are a way of building resilience into our election infrastructure.

We have a number of urgent election-related recommendations, including reforming regulation of on-line political advertisements, providing grant funding for States to improve election systems, replace outdated equipment, ensure voter verifiable paper-based systems, and conduct post-election audits. These are perhaps the most urgent of our recommendations.

I would like to close with our recommendation to build public resilience against information operations that target elections, but also democracy as a whole. Media literacy is important, but we also need to focus on deterring the key objective of our adversaries, which is to weaken democracy by pouring gasoline on the flames of division that already engulf on-line discourse, pushing Americans to give up on institutions, not just elections, but the justice system, the rule of law, and democracy itself. They portray our institutions as not just flawed, but irrevocably broken. Where protesters and judicial reform advocates seek changes to make our institutions and our Nation stronger, our adversaries seek only to make us weaker. They want Americans to despair at the prospect of bringing about change, to despair at the prospect of being able to discern fact from fiction. They want to destroy the informed and engaged citizenry upon which a healthy democracy depends.

To defeat our adversaries objective, the commission calls for reinvigorating civics education to help Americans rediscover our shared values, understand why democracy is so valuable, that it is under attack, and that every American must stay engaged to hold our institutions accountable and continue to move us toward that more perfect union.

Thank you for this opportunity, and I look forward to your questions.

Mr. LANGEVIN. Thank you, Commissioner Spaulding, again, both for your participation and valuable contributions to the Solarium Commission, but your dedication and work on cyber in general. With that, thank you for your testimony.

Finally, I now recognize Ms. Samantha Ravich to summarize the commission's statement for 5 minutes.

Dr. Ravich, you are now recognized.

STATEMENT OF SAMANTHA RAVICH, PH.D., COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Ms. RAVICH. Thank you. Thank you. Chairman Langevin, Chairman Thompson, Ranking Member Katko, distinguished Members of the committee, and my fellow witnesses, whom I have grown to know and greatly admire over this past year. I thank you for inviting me to participate in this important hearing about one of the most pressing questions that our Government is currently tasked

with answering: What steps can the Federal Government and the private sector do to defend our businesses, our military, our citizens, our country against future cyber attacks?

Our recommendations in the Cyber Solarium Commission focused on shaping the international cyber battle space, hardening our resilience, and maintaining our capability, capacity, and credibility to impose costs on the adversary, all in the service of deterring the type of catastrophic attack that our 2 esteemed commission chairmen laid out in plainspeak in the opening pages of the report.

But we would not have lived up to the great responsibility given to us if we had not thought about what our country would do in the aftermath of a significant cyber attack. So I want to spend the next few minutes underscoring one of the commission's recommendations: The need for the United States to develop and maintain a continuity of the economy, or COTE plan, which was introduced last month as a bill in the Senate Banking, Housing, and Urban Affairs Committee by Senator Peters.

During the Cold War the United States developed continuity of operations, COO, and continuity of Government, COG, plans to ensure that the Government could reconstitute and perform a minimum set of essential public functions in the event of a nuclear——

[Audio malfunction.]

Ms. RAVICH. While COO, COG—Government contingency planning for the last 60 years, no equivalent effort exists to ensure the rapid restart and recovery of the U.S. economy after a major disruption, despite the 2017 U.S. National Security Strategy identifying economic security as National security, and the recognition that the private sector, as much as the U.S. Government itself, is a critical component of the security of our populace.

So think about it for a moment, what it would mean for the U.S. military and the security forces of our allies if there was a major attack on bulk power transmission, not only knocking out the lights in major metropolitan areas, but taking transportation systems offline; or if the major stock exchanges were compromised; if wholesale payments, medicine, telecommunications, and trade or logistics were brought down.

Now think about the difficulties that would create for mobilizing and deploying forces if this all occurred during a time of international crisis, not knowing which plane, train, or bus to hop on to get to the rally point; leaving loved ones at home, scared in the dark and not knowing if their medicine or baby formula will still be stocked at the local Walmart; much of the economic base of the United States potentially losing complete access to their data for good.

Creating and exercising a continuity-of-the-economy plan will serve as a visible deterrent to adversaries by demonstrating that the United States has the wherewithal to respond to a significant cyber attack. It will show that we will not be cowed, and that, if the economy upon which our livelihoods depend is brought down by an adversarial cyber attack, they, the adversary, will feel our wrath.

Our commission's recommendation on COTE revolve around, in part, determining any additional authorities or resources that will

be required to implement plans in the case of a disaster, and establishing a framework for rapidly restarting and recovering core functions in a crisis, giving precedent to functions whose disruption would cause catastrophic economic loss, lead to a runaway loss of public confidence, imperil human life on a National scale, or undermine response, recovery, or mobilization efforts in a crisis.

Continuity-of-the-economy planning might also further review the feasibility of disconnecting critical services or specific industrial control networks if National security concerns overwhelm the need for internet connectivity continuity.

Continuity-of-the-economy planning should also further explore options to store backup, protected data across borders with allies or partners, particularly in areas where economic disruption in either country could have cascading effects on the global economy. This could include technology that considers what seed data would need to be preserved and protected in a verified format, with a process to assure no compromise or manipulation.

Finally, COTE must take into consideration the lack of readiness by the general public. By its very nature, continuity-of-the-economy planning will not prioritize. It will only prioritize the most essential functions of the country and the locales, both to enable a rapid recovery from a devastating cyber attack, and to preserve the strength and will to quickly punish the attacker.

Many industries will not be included in this planning, and most citizens will not be able to rely on Government assistance in the period following an attack. But as is also true of natural disaster preparedness, the American people do not need to be helpless. DHS and other relevant agencies should expand citizen preparedness efforts and public awareness mechanisms to be prepared for such an event.

COTE, along with many other recommendations in the report, seeks to build upon the work of the Cybersecurity and Information Security Agency, CISA, at DHS, what they have been working on for the past couple of years, and seeks to ensure that the United States is prepared to respond and recover to the full range of disruptive cyber attacks below and up to the threshold of COTE.

While it is true that there is no magic solution that will protect the United States from cyber attacks in perpetuity, there are steps that the Federal Government can undertake that will significantly improve the Government's ability to protect and defend itself from hostile cyber operations.

So as we sit here in our virtual COVID world, trying to think the unthinkable and plan for the unplannable, we must ask ourselves the hardest question of all: What would a cyber day after look like if we didn't undertake continuity-of-the-economy planning?

So I thank you for this opportunity to testify—questions and discussions. Thank you.

Mr. LANGEVIN. Very good. Thank you, Commissioner Ravich, for your testimony and, again, for your leadership on cybersecurity. You made a valuable contribution, likewise, to the Solarium Commission process and its recommendations.

With that, again, I thank all the witnesses for their testimony.

I remind subcommittee Members that we each have 5 minutes to question the panel, and I now recognize myself for 5 minutes to begin.

I will start with you, Senator King. Yesterday we saw a multinational coalition announce that Russian agents were targeting vaccine research through cyber space. In this pandemic, health care networks are incredibly important to our security. And while it is not clear whether the Russians were seeking to destroy data, the attempts are clearly troubling.

So how would a National cyber director play a role in preventing incidents like this?

Why did the commission find this construct most efficient?

Senator KING. Well, I think the key is to have someone in overall charge.

As I mentioned before, we have got responsibility for cyber scattered throughout the Federal Government, a variety of different agencies, a variety of different authorities, funding levels. But there is no central coordinating function. There is no person with the authority of the White House to settle turf wars, to oversee budgets, and to basically forge cooperation through the various agencies that are involved.

It was—I think it was one of the most obvious suggestions of the commission that we talked about. Now, we had quite a bit of discussion about where it should go, and how it should be structured. The—but the conclusion—one thought was elevate CISA, or create a new—essentially, a new Cabinet office. We rejected that because, No. 1, it would take a long time. No. 2, it would be duplicative of other functions that are already there. It wouldn't have the power and authority of the White House.

So the model we ended up approaching it as is the U.S. trade representative, who has responsibility for trade that cuts across a lot of Federal agencies, is Presidentially-appointed, Senate-confirmed, and has that authority within the Executive Office of the President.

But the fundamental idea—and I used—I was in business before I got into politics. When I was doing contracting, I wanted one throat to choke. That is what we are really talking about here, one person that is responsible, can be held accountable. I feel this is, actually, a favor to the President, to have somebody in that office that he or she can hold responsible for, and will be accountable for all the various complex operations of the Federal Government with regard to cyber.

Mr. LANGEVIN. Thank you, Senator King. I completely agree with, I concur with you.

Congressman Gallagher, on Wednesday we both testified before Chairwoman Maloney and the Oversight and Government Reform Committee. You said something very interesting about ensuring we appropriately balance offensive and defensive cyber.

Why is strengthening CISA so fundamental to the commission's report?

Mr. GALLAGHER. Thank you. Well, I think, first, let me just connect it to what Senator King just said. I mean, not only is it important to have a National cyber director to do preplanning, coordinate all the efforts of the Federal Government, but, as I alluded to in

my opening testimony, we have organizations right now that are doing good work. We really felt the best path forward was to elevate, empower them, and give them the tools they need to get the job done.

Strengthening CISA in that regard is perhaps one of the most important recommendations in our final report. As Senator King and I point out in the Chairman's letter opening the report, it is not just a matter of better enabling CISA to be able to do that defensive mission, it is not just a matter of giving CISA, for example, the authority to do persistent threat hunting on .gov networks in the way that CYBERCOM and NSA can do that on .mil networks. It is also a matter of making the mission of CISA so appealing that CISA can compete for talent with the likes of Google, Apple, Facebook, and win.

We know we can't compete when it comes to what we can pay some of the most talented cyber warriors out there, but we can compete on mission. Indeed, that is one of the things that General Nakasone told us about the NSA. While he worries about retention, he can always compete on mission.

So, by giving CISA that elevated position, that really appealing mission, we believe that we can sort-of solve the human element that is endemic to every cyber issue. Because, at the end of the day, while discussions about cyber can get very technical, they can devolve into jargon about, you know, this tech—that—these are fundamentally human problems.

I mean, my understanding, at least, of the Twitter hack this week was that it was—they fooled a human being into providing administrative credentials that resulted in the attack. So our greatest failures have been human failures. Our greatest successes will also be human successes.

So, empowering CISA, giving the director a higher level of authority and a longer term is one step toward that sort of human solution to human problems in cyber.

Mr. LANGEVIN. Thank you for that answer, and very insightful and helpful for everyone to understand. I deeply appreciate the work that Director Chris Krebs at CISA, the team there, but they also actually added resources to be able to grow their entire cyber work force, inherent capability there. I look forward to supporting that effort.

So my time has expired. I now recognize the Ranking Member of the subcommittee, Mr. Katko, for 5 minutes.

Mr. KATKO. Thank you very much, Mr. Chairman, and thank you all for, really, a great conversation. It is wonderful to hear people not sniping from side-to-side, which is all being on the same page about what we need to do in a bipartisan manner. It is truly inspiring.

I do want to talk a little bit more about the leadership issue, because I think it is critically important. It is a central focus upon which all this sort of stuff can happen. For 20 years I was a Federal organized crime prosecutor, and part of that was doing the organized crime drug task force cases. We had our quarterback, and that was the Office of National Drug Control Policy. He was over it, and be able to look over all the different disparate agencies that

had a hand in drug enforcement, and kind-of be that person that the President needs to advise him all drug-related matters.

So I know I—Senator King, I heard you talk a little bit about the leadership position, why it is important. But, you know, I want to drill down a little bit farther, just so people understand why we need it, similar to the ONDCP position.

So, Ms. Spaulding, perhaps you could talk about why a National cyber director is important. What are the different agencies that are involved in the cybersecurity? Because I know I have Homeland Security, Department of Defense. There is a lot more. So I would like to kind-of get an understanding of why we need this coordinated position.

Ms. SPAULDING. Ranking Member Katko, thank you. You are absolutely right. There is really no major agency in the Federal Government that isn't in some way involved in cybersecurity. Certainly every agency is involved in ensuring that it is able to perform its mission-essential functions on behalf of the American public in the wake of cyber threats and cyber risks.

So the National cyber director is absolutely essential. We cannot help but have this cyber activity distributed across the Government. The, you know, Department of Energy is the—they are the experts in the electric sector.

[Audio malfunction.]

Ms. SPAULDING [continuing]. In the financial services sector. Having those agencies bring that sector expertise together with cyber expertise is really important.

So if you are going to have it distributed at NSA and FBI and DHS and DOE, et cetera, then you need that central coordination function. That is why that National cyber director is so important.

Again, having been the under secretary, that is the—was the equivalent of the director of CISA, I think that White House support is critically important. It really should not in any way undermine CISA's coordination role across civilian government and with the private sector, but stand behind and give the imprimatur of the White House as CISA endeavors to undertake those activities.

Mr. KATKO. OK, thank you very much. I—in the interest of time I will forgo asking Senator King, because, really, I understand fully what the issue is.

But I will note that, from the leadership position, and having that consistent leadership at the top of CISA, and de-politicizing the assistant director positions are very important adjuncts to that, and attracting and maintaining the talent.

But I do want to talk for a second, because we have 4 nuclear power plants in my district. We have a major grid issues in upstate New York. So, Ms. Ravich, I want to ask you real quick about my concerns in that area.

Some of the most vulnerable areas of our Nation's infrastructure and our local municipal utility services often have limited budgets to support their cyber capabilities. Was there a discussion at all during the commission's work as to how to potentially assist State and municipal power and water utilities with their cyber-related mitigation and controls and coordination?

Ms. RAVICH. Yes, thank you. Thank you very much. We actually did look particularly at water utilities. There are 70,000 water util-

ities across the United States. There are 3,000 water utilities alone in the State of California. That is equal to all electric utilities across the country. Many of them are very small. Many of them, to cut costs and deal with personnel issues for the last number of years, have put on—incorporated some technology that, frankly, isn't safe. Some of the technology has been made in adversarial countries, and now it is in our water systems. So, while you may be able to live in the dark for a day or 2 without energy, try living without water.

So we recognize this, and we had long conversations about what could be done to help State, local, Tribal, territorial, especially, and create—ask for, as a recommendation, the creation of a cybersecurity assistance fund, knowing that, again, State and local, you know, needs best practices, needs assistance. They are not going to be the repository of all cybersecurity best practices. To make us all safe, we absolutely have to, from the Federal Government on down, help the smallest among us.

Mr. KATKO. Thank you very much. It is an important issue. I have got plenty more questions, but I know I am out of time. So I yield back, Mr. Chairman.

Mr. LANGEVIN. Very good, Mr. Katko. Thank you for your line of questions.

I just wanted to yield to—if the Chairman is on still, I will yield to Chairman Thompson. If not, we will go to Congresswoman Sheila Jackson Lee.

OK, I believe Mr. Thompson has stepped away, so Congresswoman Sheila Jackson Lee is recognized for 5 minutes.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. I appreciate this very important hearing, and I am delighted to be here with the—some very important witnesses that include Commissioner Ravich, as well as Commissioner Spaulding and my colleagues, Representative Gallagher and Senator King. I thank them both for their service on this committee.

Particularly, I will join with my voice, Congressman Gallagher, to congratulate you on the birth of a beautiful baby and, I might imagine, where opportunities are not limited. So I am delighted, and wish your family the best.

This is a very important hearing that deals with addressing the question of the recommendations by the Cyberspace Solarium Commission related to how the Federal Government can be more secure. I am wearing a mask because I am in the epicenter here in Houston, Texas. I just came to my office to be a part of this very important hearing. But we are fighting against very large numbers of COVID–19. In fact, of course, we are about 75,000 cases here in Houston, my home town, and 717 deaths.

Interestingly, cyber is part of how we will survive, because many people have turned toward cyber and connecting through the system.

I wholeheartedly agree with the need for a cyber National director, and I support that. I am also introducing an amendment to protect—to NDAA to protect the security of emails. I want to thank Congressman Langevin for his leadership and support of the amendment, cosponsoring it, as well as Congressman Gallagher.

I want to raise 2 questions as quickly as I can. Yesterday we were alerted to a coordinated hack of major U.S. Twitter accounts, including those of President Obama, Elon Musk, Bill Gates, Mike Bloomberg, and former U.S. President Joe Biden, and many others. At that time, where misinformation—at this time, where misinformation poses one of the greatest threats to National security, we need cybersecurity policy that will uphold the truth.

The commission made a number of recommendations designed to improve collaboration between CISA and the private sector. So I would appreciate it if—I first go to Commissioner Ravich—to elaborate on any recommendations that you believe would have the potential to prevent a similar breach—that we have asked for our private sector to ramp up their system. I think the Government needs to not deny the First Amendment rights, but has to have a forceful place in this. I would welcome the comments of our two co-chairs, Congressmen Gallagher and King, but I will start with Commissioner Ravich on that question.

Let me ask my second question, just so it is on the record for answering, and that is we are very much dependent, potentially, on the ending of COVID–19, on vaccines. We have just determined over the last couple of days that Russia has been interfering with the cyber, or the research on vaccines by a number of our companies, which really mean life or death for many Americans.

So, Commissioner Ravich, would you answer the first question about the violations of Twitter accounts? Thank you.

Ms. RAVICH. Yes. Thank you. Thank you very much. You know, we absolutely looked at—and this was, again, before COVID started and we were all working from home and relying on these devices on these networks to be able to interact with our Government, to be able to register to vote, to be able to go to the DMV virtually, our Social Security payments. Now we are realizing that many of these networks could be untrustworthy.

So a few things that we certainly highlighted in our original report, and then in our pandemic annex, things like the internet of things security, that individuals, our populace, should not have to be cybersecurity experts. It is absurd in this day and age to say that, when my mom or my neighbor goes to the store and buys a router, that they have to be cybersecurity experts to know which one is going to protect them better.

The same way, when you see the locked icon on your email, the idea that I should automatically know that this is a trusted certificate. No, there have to be better safeguards in place from the Government itself.

So the commission really took kind-of 2 tacks at this. One is what are—what is the responsibility inside the Government? How can we push ahead with better cybersecurity recognition of what is secure for individuals that they know what to buy and what not?

But also, what are the responsibilities from the private sector, right? The Government can only do its job if it understands attribution better. What is being attacked? What type of industrial control systems are most in the crosshairs of a Russia or Iran or a China or North Korea? Right? So the U.S. Government needs better information and data to be able to do intel sharing back to the private sector.

So these are some of the things that the commission really focused on. But it has to be a different type of relationship between the U.S. Government and the private sector than really existed before, if we are all going to be safer.

Ms. JACKSON LEE. Thank you. If Senator Gallagher and Representative—Senator King and Representative Gallagher could take a moment to comment on Russia's——

Mr. LANGEVIN. Congresswoman, you are not coming through.

Ms. JACKSON LEE [continuing]. Research.

Mr. LANGEVIN. Congresswoman Jackson Lee, you are coming through gargled.

Ms. JACKSON LEE. Senator? Senator King.

Mr. LANGEVIN. Senator King is muted.

Senator KING. Could you restate the question, Congresswoman? I couldn't hear it.

Ms. JACKSON LEE. I would be happy to.

Senator KING. Yes.

Ms. JACKSON LEE. I thank the Chairman for indulging.

I just want you to focus on the interference that has been reported by recent reports about Russia's interference in our vaccine research—COVID–19 is a pandemic in our Nation surging in many States—as it relates to the work that we are doing here to shore up our cyber systems.

Maybe Representative Gallagher would comment, as well. But the Russian's interference with vaccine research, how important the report of the Solarium Commission's report is in the work going forward.

Can you hear me? Did you hear me?

Senator KING. Yes, I can. I did. Thank you very much.

First I want to send my warmest thoughts to the people of Houston. I know what you are going through. I have seen it, and I am following it, and it is a very tough time. I know it means a lot to them that you are there with them on this—in this terrible time.

What the Russians appear to be doing, I think there are a couple of lessons to be learned from this.

No. 1, there are no boundaries for what our adversaries will do.

No. 2, the Russians are doing something that the Chinese, in fact, have been doing for many years, which is, essentially, theft of intellectual property. The estimates are that Chinese theft of intellectual property has cost our economy billions of dollars. So clearly, this is one of the most important areas that we need to shore up our defenses.

We attended to this in a number of different ways in the report. But the fundamental—I think one of the fundamental issues is, as I mentioned in my opening statement, they have to understand that there is a price to be paid for this. If the Russians or the Chinese or the Iranians or whoever it is comes after us and does something like this, and we can attribute it to a particular country, there needs to be—there need to be consequences. There need to be results. Otherwise, they will keep doing it. Why wouldn't they?

So that is the kind of strategic area that we are talking about. But then also, we need to be more defense-oriented. It is very interesting that—I can't remember—85 percent of cyber risk rests upon individuals doing things like clicking on phishing emails. In other

words, the most basic kind of cyber hygiene would be tremendously important in protecting our companies and our country from these kinds of attacks.

I don't know how they got into those vaccine companies, but it wouldn't be surprising at all if it was some kind of phishing expedition that got the credentials, that got the password.

So the Government has a lot of things that we can do, and they are all in our report, or many of them are in our report. But we also need to support and encourage the citizens to understand the magnitude of this risk, because it may not be that they hit the Pentagon, but they are going to try to hit smaller companies and get into the system in that way.

So you raise a very important question that I think we really have focused upon, and must continue to do so.

Mr. LANGEVIN. Thank you, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you. Thank you so very much. Thank you.

Mr. LANGEVIN. Mr. Joyce is now recognized for 5 minutes.

Ms. JACKSON LEE. Thank you very much.

Mr. JOYCE. Thank you. Thank you, Senator King, Representative Gallagher, Dr. Ravich, and Commissioner Spaulding.

I will join in congratulating you, Mike, on the birth of your wonderful daughter. This is an important time in life, and yet you are stopping that new family moment and joining with us.

Each of us, each of us is aware of the hostile cyber—and you mentioned that, Dr. Ravich.

I think that the discussion, Senator King, that you just talked about is important, as well. But Mike Gallagher said something that is important to this conversation. Our greatest failure will be in human failure. Senator King, you mentioned that, how easy it is for someone to open an email and allow that integration into someone's personal cyber world to be shared and, ultimately, potentially destroyed.

Five years the DMARC protocol has been established. It is deployed very, very sporadically, but it has increased. What I am going to ask both you, Commissioner Ravich, and Commissioner Spaulding to address is what barriers exist to that old deployment of DMARC, so that potential integration can occur, and potential protection occur, as well.

Ms. RAVICH. OK, I don't know if I should go first.

Well, first of all, I think it is a great point, because we, obviously, would all be more secure if the uptake on protocols like that were more expansive. It goes back to some of the other things that we were looking at on the commission directly, which will get to your point.

We had looked at things such as final goods assembly liability, rights? I mean, you know, kind-of as I was saying before, why should my mom be a cybersecurity expert, right? Why should my doctor be a cybersecurity expert? They should be able to go—and the devices that they are buying, they should know that they are secure.

The same thing when I—if you sent me an email, I should know it is from you. Right now, frankly, in not all places are things like trusted certificates actually to be trusted.

So we didn't want to be too prescriptive in terms of how the private sector needs to start to layer on much greater security in IoT, for instance, and devices, hardware, and software. So we recommended a number of different ways to kind-of skin that cat.

But it is true, we are living in a time where, if we don't make these types of devices, hardware, software more secure, we will all be more at risk.

Ms. SPAULDING. Congressman, I couldn't agree more, and thank you for your leadership on this important issue.

You are absolutely right that email is one of the most troubling vectors, and most frequent and common vectors for malicious cyber activity to get into networks and systems. DMARC, domain-based message authentication reporting and conformance, is one of the protocols that has proven to be most effective, really, at stopping this kind of activity, so critically important.

You ask why isn't it then just uniformly adopted across the board? You are correct that it is gaining ground, and its adoption is moving forward. But I think it is leaders, CEOs, boards of advisers, secretaries of departments and agencies, leaders across the board need to support their chief information security officers when they make these kinds of recommendations. It is those leaders that decide about resource allocation, and that becomes very important.

To do that, it is helpful to be able to show a return on investment. That, again, requires information. It is one of the reasons that the commission has a recommendation that would require key companies to report more information about malicious cyber activity, so that we can begin to build the kind of repository of data that allows us to be able to tell those decision makers who are allocating resources the costs of not implementing something as basic as DMARC.

Mr. JOYCE. I think that cost issue is important. I just have seconds left, but I am perplexed by only 80 percent of Federal agencies are reported to be implementing DMARC. Are there specific obstacles that we in Congress should address to see that all Federal agencies——

Ms. SPAULDING. So I think the number—I suspect that that 80 percent covers most, if not all, of the major departments and agencies of the Government. There are lots of very tiny—the Millennium Challenge Corporation, the Denali Commission, et cetera—that really just need a lot of hand-holding to make these technical changes.

But I applaud you. Keep, you know, keeping their feet to the fire, and keep pushing this. It is really important. But thank you.

Mr. JOYCE. Thank you, Commissioner. Thank you, and I yield my time.

Mr. LANGEVIN. I thank the gentleman.

Before I turn to Miss Rice, I need to step away from the Chair for a few minutes. There is a press conference and a meeting with our Governor that I need to—a virtual one that I need to jump on to. It is COVID-related, and related to our small business community. So I will be stepping away as briefly as possible, and Ms. Underwood will be taking the gavel to chair the hearing, going forward. I hope to make it back before the conclusion.

In the event—in the unlikely event that I am not able to get back before this is concluded, I do want to thank our panelists today for their testimony, their leadership on the Solarium Commission, and their leadership on cyber, which I am grateful for.

With that, Miss Rice is recognized now for 5 minutes.

Miss RICE. Thank you so much, and I want to thank all of the—my 2 colleagues and our private-sector witnesses here today, members of this commission.

As I—if we do not implement every single recommendation in this report, shame on us, as a Government. I mean, it is just such common-sense stuff. With everything that is going on right now in the world, we see in this report why it is so important to implement every single recommendation.

Congressman Gallagher, I just want to go to you first, because it seems to me that this is a constant, constant issue that comes up between public and private partnership. Why is it, you know, that it is hard for us to get that right?

I mean, do you think it is possible to continue incentive-based public-private cybersecurity partnerships as part of an effective cyber defense program, or do you think it is going to come to Congress having to more strongly consider imposing mandates?

Mr. GALLAGHER. Well, I think the other commissioners would agree that the approach we have largely taken in this report was to try and incentivize the private sector to work more closely with the Federal Government or, as we say in the Chairman's letter, try and incentivize the C-suite types in the private sector to take cybersecurity seriously.

There are areas, however, where we are, you know, imposing further requirements that some in the private sector will no doubt view as onerous, such as the need for large, publicly-traded companies to do mandatory penetration testing.

But I do think—and connected to the earlier series of questions on the Russian hack and things like that—I think, culturally, what we are trying to do here is shift the culture in the intelligence community and at CISA—and this is my verbiage, not contained in the final report—from a culture of need-to-know to more toward need-to-share.

So it is not just that we need the private sector to step up and do more for their own security, but we also want our cybersecurity professionals in the Federal Government to be in a posture where they are constantly sharing information with the private sector, so that they are seen as a valued partner with the private sector, and the private sector doesn't view them suspiciously.

So, toward that end, we recommend creating a joint collaborative environment, a common and interoperable environment for sharing and fusing threat information inside, and other relevant data across the Federal Government, and then between the public and private sectors. Our recommendation to strengthen a public-private, integrated cyber center within CISA is intended to allow for that closer collaboration between the public and private sector.

Then finally, we have a recommendation about establishing a joint cyber planning office under CISA to coordinate cybersecurity, planning, and readiness across the Federal Government and between the public and private sector.

So I guess, in sum, I still maintain hope that we can pursue an incentive-based approach. But you are right to suggest that I think everything hinges on that—the level of trust between the private sector and the public sector. Because the reality is, as Senator King and I say in the opening letter, you know, we are not the Chinese Communist Party. We can't just dictate outcomes for the private sector, nor should we want to, right? We want to maintain the free and open and innovative environment we have in America.

So it is a delicate balance, but it is one we hope we have struck well in the commission's final report.

Miss RICE. Yes. So it sounds like a little bit of territorialism, too, which is one of the things that we learned about in a post-9/11 world. To see that possibly still kind-of rearing its head is not a good thing.

You know, I just want to be very mindful of my time, and all of our witnesses' time. I have to give a shout out to Chris Krebs, because I think he is doing such a great job at CISA, especially in the area of election security, really reaching out to individual States to help them secure their election infrastructure.

But I would like to ask both Ms. Ravich and Spaulding, in light of the threats and challenges associated with the upcoming 2020 election, do you think the Federal Government is doing enough to defend elections from foreign interference?

Ms. SPAULDING. So I am happy to start on that. I think not yet, no.

I agree with you. I think Chris Krebs and the men and women at CISA are doing a terrific job, and working very hard with State and local election officials, who I think are also taking this very seriously. But our—in the commission report we have a number of recommendations that we really hope Congress will act on, and will act very quickly.

One of those, obviously, is the reforming of on-line political advertising to prevent foreign interference in that regard.

But the other is providing the wherewithal, the support to our State and local officials so that—in the form of grants, so that they can do the things that need to be done to put secure systems in place, but also to put paper-based audit capabilities in place so that we can reassure the public about the legitimacy of the process when it is challenged.

Ms. RAVICH. Yes, so let me jump in. That is very thoughtful, as always, what Suzanne had said.

You know, our commission report, as the 2 co-chairmen said, is—has 3 parts of layered defense. When you look at elections, each part of that layered defense has to be deployed, right?

So shaping international behavior, it is not only us that is being attacked in our election, it is all free and democratic nations. So the——

[Audio malfunction.]

Ms. RAVICH [continuing]. With partner nations, our friends and allies, those who believe in democracy and free enterprise, so that together we can share lessons learned and bolster our systems.

The second, resilience. Suzanne spoke about it, as always, you know, brilliantly. The Election Assistance Commission needs a stable budget, needs senior cyber expertise because this is not one and

done. It is not like we are going to protect our systems, and then that is it, we don't ever have to protect them again. It is going to be consistent and constant.

The third part of layered defense is imposed costs, right? So the adversaries that try to undermine what makes us a great Nation, you know, have to actually really understand there will be costs imposed upon them for this.

So the 3 parts of layered defense you can see when you look at the question of elections, how they all must relate to one another to make us more secure.

Miss RICE. Thank you so much. If we can't protect our elections, I mean, that will doom our democracy, I think, quicker than anything else.

So I want to thank you all so much for being here today, and I yield back.

Ms. UNDERWOOD [presiding]. Thank you. I now recognize myself for 5 minutes.

I would like to start by thanking Chairman Thompson for calling today's hearing, and Chairman Langevin for his dedicated work to strengthen America's cybersecurity, both as a commissioner and as a valuable Member of this committee. Cybersecurity advocates like Mr. Langevin have been sounding the alarm for years about America's vulnerability to cyber attacks.

As a representative from Illinois, a State that experienced a major cyber attack in our election system in 2016, I am well aware that such attacks pose a threat at all levels of government, and so a whole-of-Government response is required.

In the last few months the COVID–19 pandemic has exposed this vulnerability like never before. As Americans have struggled to telework securely, overworked hospitals have suffered ransomware attacks. Cyber attacks have targeted vaccine developers, and more.

I am pleased that the commission built on the recommendations in the March report by publishing a white paper in May on cybersecurity lessons from the pandemic. In this white paper, the commission found that maligned foreign disinformation operations are undermining public health: "The resulting confusion is threatening to become a literal matter of life and death."

Ms. Spaulding, can you elaborate on how disinformation impacts our cybersecurity, public health, or other areas of National security, even to the point of life and death?

Ms. SPAULDING. Absolutely, Congresswoman, thank you for that really important question that—we have seen our adversaries take advantage of this situation, and putting out disinformation around COVID that confuses the public. It may not be that they are able to convince the public necessarily of the narrative that they are pushing, but they create confusion, which is deadly enough. If the public gives up, as I say, on their ability to figure out what is fact when—at a time when giving the American public facts about what they should be doing to protect themselves, their families, their communities, and our Nation, that is extremely destructive.

When we see the COVID coming together with our elections as election officials are making decisions about how to adjust, whether to adjust elections in light of the pandemic, and then those are winding up in courts—and we have seen disinformation around all

3 of those: COVID, elections, and the courts—and that is a really dangerous combination that threatens the peaceful transition of power.

Ms. UNDERWOOD. Thank you. I agree with the commission's assessment of the severe and even deadly security threat posed by disinformation, which is why, in the last month, I introduced the Protecting Against Public Safety Disinformation Act. This bill would direct the Department of Homeland Security to assess maligned foreign disinformation operations that threaten public safety and share their findings with State and local authorities like public health departments, emergency managers, and first responders.

The commission's recommendations repeatedly highlight the role of State and local officials in hardening our cybersecurity posture. Ms. Spaulding, why is it so important for State and local officials to be involved in our National response to disinformation and other cybersecurity threats?

Ms. SPAULDING. So we have gotten used to the idea that State and local officials are on the front lines of responding to disasters in the real world. We have to understand, as you say, that they are also often on the front lines of responding to disinformation that causes confusion in their communities.

We know that local sources of information are often more trusted than National sources. We also know that they are being targeted, both with ransomware, with traditional cyber activity, but that traditional cyber activity can also be designed to undermine public confidence, so part of an information operation. They need to be supported in combating that.

Ms. UNDERWOOD. Thank you. As you may know, the personal information of 76,000 Illinois voters was accessed by Russian operatives in 2016. Since then, our State and local election officials have been working hard to improve election systems and infrastructure. But due to limited resources, some have faced challenges in upgrading legacy machines and hiring additional cybersecurity personnel. Now, when State budgets across the country have been devastated by this pandemic, Federal support is more urgently needed than ever.

So over 2 months ago, the House passed a bill, the Heroes Act, which would provide $3.6 billion for election security grants in the State. Unfortunately, the Senate has yet to act on this bill. We know that election security grants like those in the Heroes Act would equip these State and local officials with the resources that they desperately need in order to secure our elections and our National security ahead of the election in November.

With that, I yield back. I have to step away, and so Miss Rice will now Chair the hearing. Thank you.

Miss RICE [presiding]. Thank you so much. I—it looks like we have come to the end of the questioning, so I would love to thank the—all our witnesses for your valuable testimony today, and the Members for their questions.

This is a report that every single Member of Congress needs to digest, and immediately get on board doing something about, and implementing as many of these recommendations as we can.

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

Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, other than to congratulate Mike Gallagher once again on lovely baby Grace, the subcommittee stands adjourned. Thank you all.

[Whereupon, at 2 p.m., the subcommittee was adjourned.]