# U.S. CYBERSECURITY PREPAREDNESS AND H.R. 7331, THE NATIONAL CYBER DIRECTOR ACT

## HEARING

BEFORE THE

## COMMITTEE ON OVERSIGHT AND REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

JULY 15, 2020

## Serial No. 116–102

Printed for the use of the Committee on Oversight and Reform

Available on: *govinfo.gov, oversight.house.gov* or *docs.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE
40–844 PDF WASHINGTON : 2020

## COMMITTEE ON OVERSIGHT AND REFORM

CAROLYN B. MALONEY, New York, *Chairwoman*

ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
RAJA KRISHNAMOORTHI, Illinois
JAMIE RASKIN, Maryland
HARLEY ROUDA, California
RO KHANNA, California
KWEISI MFUME, Maryland
DEBBIE WASSERMAN SCHULTZ, Florida
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont
JACKIE SPEIER, California
ROBIN L. KELLY, Illinois
MARK DESAULNIER, California
BRENDA L. LAWRENCE, Michigan
STACEY E. PLASKETT, Virgin Islands
JIMMY GOMEZ, California
ALEXANDRIA OCASIO-CORTEZ, New York
AYANNA PRESSLEY, Massachusetts
RASHIDA TLAIB, Michigan
KATIE PORTER, California

JAMES COMER, Kentucky, *Ranking Minority Member*
PAUL A. GOSAR, Arizona
VIRGINIA FOXX, North Carolina
THOMAS MASSIE, Kentucky
JODY B. HICE, Georgia
GLENN GROTHMAN, Wisconsin
GARY PALMER, Alabama
JAMES COMER, Kentucky
MICHAEL CLOUD, Texas
BOB GIBBS, Ohio
CLAY HIGGINS, Louisiana
RALPH NORMAN, South Carolina
CHIP ROY, Texas
CAROL D. MILLER, West Virginia
MARK E. GREEN, Tennessee
KELLY ARMSTRONG, North Dakota
W. GREGORY STEUBE, Florida
FRED KELLER, Pennsylvania

DAVID RAPALLO, *Staff Director*
EMILY BURNS, *Chief Counsel*
MARK STEPHENSON, *Chief Counsel*
AMY STRATTON, *Clerk*
CONTACT NUMBER: 202-225-5051
CHRISTOPHER HIXON, *Minority Staff Director*

---

# C O N T E N T S



*Written opening statements and witnesses' written statements are available at the U.S. House of Representatives Repository: docs.house.gov.*

INDEX OF DOCUMENTS

---

*The documents entered into the record are available at: docs.house.gov.*

# U.S. CYBERSECURITY PREPAREDNESS AND H.R. 7331, THE NATIONAL CYBER DIRECTOR ACT

**Wednesday, July 15, 2020**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON OVERSIGHT AND REFORM,
*Washington, DC.*

The committee met, pursuant to notice, at 12:16 p.m., via WebEx, Hon. Carolyn B. Maloney [chairwoman of the committee] presiding.

Present: Representatives Maloney, Norton, Lynch, Connolly, Raskin, Rouda, Khanna, Mfume, Sarbanes, Welch, Speier, DeSaulnier, Tlaib, Porter, Comer, Jordan, Gosar, Massie, Grothman, Cloud, and Keller.

CHAIRWOMAN MALONEY. Good afternoon. The committee will come to order. Without objection, the chair is authorized to declare a recess of the committee at any time.

I recognize myself for an opening statement.

Ladies and gentlemen, thank you all for being here today. As our Nation reckons with the monumental human and economic toll of the coronavirus crisis, we must look critically at the warnings we had and the decisions made about them.

The most recent Worldwide Threat Assessment of the U.S. Intelligence Community, released in January 2019, warned, and I quote, "The United States and the world will remain vulnerable to the next flu pandemic or large-scale outbreak of a contagious disease that could lead to massive rates of death and disability, severely affect the world economy, strain international resources, and increase calls on the United States for support."

We must ask ourselves what other warnings are going unheeded, and what can we do right now to protect the American people from other catastrophic threats? Before the unthinkable happens in the future, how can we exercise strategic, decisive foresight to the best of our ability today to ensure we are a nation prepared tomorrow?

That same Worldwide Threat Assessment lists cyber attacks as a top global threat, with China, Russia, Iran, and North Korea waging a silent war capable of shutting down critical infrastructure, breaching sensitive information systems, and jeopardizing critical sectors in America and globally.

The report states, and I quote, "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic,

and military advantage over the United States and its allies and partners."

Cyber-attacks are a critical, complex, prevalent, and growing threat to the Nation's safety and economic security, touching nearly every aspect of our lives. This assessment was upheld by recent findings from the U.S. Cyberspace Solarium Commission, which was established by the 2019 National Defense Authorization Act to review the state of our cybersecurity posture and develop bipartisan solutions for defending America against cyber-attacks.

This commission of congressional, executive branch, and private sector cybersecurity leaders sounded the alarm that, in addition to millions of intrusions that disrupt operations in America on a daily basis, we remain vulnerable to catastrophic attacks on critical infrastructure and economic systems that could cause widespread damage and death.

A number of the commission's recommendations fall within the legislative jurisdiction of this committee. This includes one that has sparked a high level of interest on both sides of the aisle, the recommendation for a centralized cybersecurity position at the White House to develop and streamline the Federal Government's strategy, coordination, and response to cyber-attacks.

This role was first formalized during the George W. Bush Administration and then elevated and expanded during the Obama Administration. But in 2018, then-National Security Adviser John Bolton eliminated the role, reportedly to cut "another layer of bureaucracy."

The move generated widespread bipartisan concern. In 2019, the United States was rated as the fifth most cyber-secure nation in the world. In 2020, it dropped to the seventeenth.

Today, we will review H.R. 7331, which would implement the commission's recommendation to establish a National Cyber Director in the Executive Office of the President. This new position would restore that cyber coordination and planning function to the White House. In addition, for the first time, it would be backed with resources and statutory authority to lead strategic planning efforts, review cybersecurity budgets, and coordinate national incident response.

A challenge as complex and pervasive as cybersecurity requires that our Government be strategic, organized, and ready. Democrats and Republicans agree we need a National Cybersecurity Director to ensure we are fully prepared for, and coordinated in, our response to cyber-attacks as our Nation fights this silent war. Our mission today is to gain a detailed understanding of the threats we face and to thoroughly examine H.R. 7331 as the vehicle for preparing our country against those threats.

I now recognize the distinguished ranking member for his opening statement. Representative Comer?

Mr. COMER. Thank you, Chairwoman Maloney, for holding this hearing to address our Nation's cybersecurity posture and to explore the merits of U.S. Cyberspace Solarium Commission's recommendations to establish a National Cyber Director office within the Executive Office of the President.

The Federal cyber domain, we can all agree, is dynamic and dispersed, with varying jurisdictions and expertise across the Federal

Government. These agencies are organized to combat cyber-crime, defend against national security intrusions, and support the security needs of the private sector's critical industries and commercial interests.

Our Nation has continuously become more and more reliant on technology over the last three decades. Our reliance on technology and interconnected information systems is more important than ever, with the pandemic forcing organizations to quickly build out remote operations and our Nation's work force pivoting to a work from home posture. Increasingly, foreign state actors, extremist groups, domestic agitators, and criminal enterprises all have a vested interest in exploiting U.S. networks.

The remote operations of the pandemic have created new cyber vulnerabilities for these malicious actors to take advantage of. These are the same actors who also target our private sector partners and state and local institutions. Breaches in Federal and commercial networks by foreign governments have exposed sensitive intelligence data, proprietary military designs, and Government personnel data.

Because of cybersecurity risks, we must all do our part to maintain a safe and secure national cyber infrastructure, and by continuing to foster relationships across the private sector and our state and local partners, we can share vital cyber threat information that helps secure our critical infrastructure.

We will hear today from notable subject matter experts who have deep experience navigating the Nation's cybersecurity environment. They also have experience with efforts to combat damaging cyberattacks from foreign adversaries like China. Historically, China has hacked into the FDIC, stolen valuable U.S. R&D, and paid our university professors to improperly share valuable intellectual property. I would welcome the opportunity to work with the majority to hold China accountable for these bad acts, as well as their deceptive tactics over the course of this pandemic. That would be a great hearing, Madam Chairman.

Today, however, we look forward to evaluating the proposal to establish a National Cyber Director to oversee the cybersecurity policy, planning, and operations of the Federal Government. In evaluating this legislative proposal, we have a duty to the American people to be a good steward of taxpayer dollars and not create more bureaucracy. Establishing a clear and convincing rationale for establishing such a critical position requires the kind of due diligence and thoughtful assessment that our committee's hearing processes afford. The current and projected cybersecurity landscape is complicated with many actors and operations that must work in harmony.

While there have been more than several high-profile cybersecurity incidents over the past decade, I must note that recent attempts at targeting our Nation's coronavirus biomedical research activities and use of remote work platforms have been taken very seriously by Homeland Security and law enforcement officials within the Trump administration. The administration has done what is expected of cybersecurity professionals. It has prioritized defending against potentially harmful cyber incidents wherever and whenever threats are found.

I think we all want our Nation's cybersecurity to be effective, both defensively and offensively. To this end, it is imperative that Congress and this committee fully evaluate the reasons why the commission recommended the statutory creation of the National Cyber Director.

The main questions I have toward this goal are, "Is it necessary to create another Federal office to have someone truly in charge, and if so, will that official, in fact, have the authority to make the decisions that need to be made? Will everyone else fall in line and work in harmony?

We know that multiple Federal agencies have a piece of the cybersecurity pie. So, by authorizing a new oversight and coordinating official, are we legitimately creating a system that will be more prepared to face growing cyber threats? Will the National Cyber Director utilize the existing cyber leadership and expertise in our Government, or do we risk making that bureaucratic pie bigger and creating duplicating functions? Will a National Cyber Director add value to this Nation's cybersecurity infrastructure, or should we align and support systems already in place?

I look forward to hearing about tangible examples of how this National Cyber Director would actually respond to a cyber incident and how that might be better than the system already in place. In a fluid environment, when response time and expertise are paramount, we cannot afford to introduce inefficiencies or bureaucratic hurdles to the Government's ability to respond to a national cybersecurity incident in real time.

Madam Chairwoman, I think we agree our Nation's cybersecurity enterprise deserves a supported public policy that will not hinder dynamic, focused, and strategic planning and operation. I am pleased to be working with you on this issue, but again, I want to ensure that we are not fostering redundant efforts across the Federal cyber sector. In establishing a Senate-confirmed cybersecurity leader, we need to be comfortable in limiting Presidential prerogative to implement preferred policies on behalf of the American people.

Again, I appreciate this opportunity to review this recommendation and hear from these expert witnesses. I yield back.

Chairwoman MALONEY. Thank you, Mr. Comer.

I now recognize the distinguished chairman of the Subcommittee on National Security, Mr. Lynch, for an opening statement.

Mr. LYNCH. Now thank you, Madam Chair, and thank you for convening today's important hearing on H.R. 7331, which allows for the creation of a National Cyber Director, which is an idea that is not only reasonable, but necessary and long overdue given the world in which we live.

I am well aware of the lengthy review and study that Mr. Langevin has engaged in over the years on this issue. He has been nothing short of relentless in his mission, and I thank him and our friend and colleague Mr. Gallagher for their bipartisan commitment to defending our Nation's cybersecurity and for their testimony before our committee.

I also want to take a minute just to thank Mr. Katko, Mr. Ruppersberger, and Mr. Hurd, who are also original co-sponsors of H.R. 7331.

Now for years, foreign policy and national security experts have considered cyber to be the battlefield of the future. And for anyone paying attention, that future is already here. Back in 2014, hackers, likely affiliated with the Chinese government, breached the information system of the Office of Personnel Management, compromising the personal data of at least 22 million people, including, most notably, Federal employees who had either applied for or received security clearances for access to classified information.

We are also well aware of Russia's sweeping and systemic efforts in 2016 to interfere in the Presidential election by hacking the computer network of the Democratic National Committee and attempting to penetrate the election infrastructure in all 50 states.

To speak to some of Mr. Comer's concerns, most recently our National Security Subcommittee staff, which I chair, we held a briefing with the Federal Bureau of Investigation and the Cybersecurity Infrastructure Security Agency to discuss the latest uptick in cyber-attacks during the coronavirus pandemic against the Federal Government agencies, research and academic institutions, and even private citizens. During the briefing, our committee was told that every institution or agency conducting coronavirus vaccine research is a target for—is a current target for foreign cyber attackers.

As our intelligence agencies warned before 9/11, the system is blinking red. Yet only two years ago, then-National Security Adviser John Bolton dismantled the national cyber coordinator position at the National Security Council, leaving the U.S. cybersecurity policy rudderless and disjointed.

The need for greater leadership, strategic planning, and policy coordination to ensure the security of our Nation in the cyber domain could not be more urgent or important. So, I am pleased to support H.R. 7331, which will allow for the creation of a National Cyber Director, and I would encourage all of my colleagues to do the same.

Again, I want to thank the chairwoman for her willingness to hold this hearing today, and I want to thank all of our witnesses for testifying. I look forward to the discussion and for building even greater bipartisanship and consensus around the importance of H.R. 7331.

Last, I am also currently in a markup over in T&I—I am at the Capitol today—where I have an amendment pending. So, I am going to have to jump out and then jump back in. I apologize for that, but that is our schedule. I yield back. Thank you, Madam Chair.

Chairwoman MALONEY. Thank you, Mr. Lynch. I now recognize Mr. Grothman for an opening statement.

Mr. GROTHMAN. OK. Can you hear me?

Chairwoman MALONEY. Yes. We can hear you.

Mr. GROTHMAN. Good. I appreciate this opportunity in my role—first of all, it is good to see we got our witness on here from Wisconsin. So, I thank you for bringing him in. I appreciate this opportunity in my role as ranking member of the National Security Subcommittee on Oversight to address an issue with major national security ramifications.

As Ranking Member Comer addressed in the opening comments, our Nation's adversaries will stop at nothing to steal our secrets,

commercial expertise, and sensitive information held on a sprawling computer network connecting both public and private sector organizations. Chief among these cyber offenders is the Chinese government.

Unfortunately, despite a desire to play by the rules in international commerce, as President Trump says, we have been treated unfairly by the Chinese. Oftentimes, this well-intentioned global posture costs the United States our valuable intellectual property, which flows out of our Nation's research institutions into Chinese hands. The hearing today will help us determine whether our Federal Government needs support in defending against these high-stakes malicious cyber attacks and continual intrusions.

One of the proposals by the Cyberspace Solarium Commission was the formation of a new National Cyber Director office and a Senate-confirmed official inside the White House. While I appreciate the commission's desire to ensure that the Federal Government's cybersecurity infrastructure includes a one-stop shop for cyber guidelines, I wonder whether we might be too quick to create yet another new bureaucracy by not carefully considering potential downsides to this reform.

We must keep in mind the Trump administration's success in protecting our last mid-term elections from disruptive cyber incidents, and the administration's strong stance against those who wish to take advantage of international attempts to exploit the technology challenges presented by the pandemic. Would we be doing a disservice to various agencies which already effectively coordinate cybersecurity responses for our Nation?

I want to keep an open mind on the merits of any proposal to improve our national cybersecurity, and I appreciate today's witnesses and the time and attention they have each dedicated to protecting our Nation's information and critical infrastructures.

I look forward to the witnesses' testimony and their perspectives on whether the creation of a National Cyber Director will add value to the current multi-agency cyber framework to properly de-conflict and coordinate effective responses to cyber attacks against our Government and private sector.

Thank you, Chairwoman Maloney and my counterpart on the National Security Subcommittee, Chairman Lynch, and Ranking Member Comer, for all of your interest in these pressing issues. I look forward to working with each of you to ensure that we strengthen America's cybersecurity against all types of threats and any foes from abroad who wish to do Americans harm. I yield back.

Chairwoman MALONEY. Thank you, Mr. Grothman.

I will now introduce our first panel of witnesses consisting of our colleagues here in the House of Representatives who served on the U.S. Cyberspace Solarium Commission—Congressman Jim Langevin of Rhode Island, commissioner of the Cyberspace Solarium Commission and chairman of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee, who has been championing this effort for many, many years, and Congressman Mike Gallagher of Wisconsin, co-chair of the commission and a proud new father of Grace Ellen Gallagher. Congratulations on truly life's greatest experience of becoming a father, and it is the

best job in the world. So, we are very pleased to have you both here today.

With that, Mr. Langevin, you are now recognized to provide your testimony.

**STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF RHODE ISLAND AND COMMISSIONER, U.S. CYBERSPACE SOLARIUM COMMISSION**

Mr. LANGEVIN. Very good. Well, thank you, and good afternoon, Chairwoman Maloney, Ranking Member Comer, and distinguished members of the committee. It is always humbling to sit on this side of the table, the witness table, even when it is virtual. I want to begin my remarks by thanking all of you for the important work that you do. I particularly want to thank Chairwoman Maloney for convening this hearing and for her partnership in raising the issue of creating a National Cyber Director.

I join you today as a representative of the Cyberspace Solarium Commission. I am proud to be joined by my colleague, Congressman Mike Gallagher, one of the co-chairs of the Solarium Commission.

I also want to congratulate him on being the newest father in the House to his daughter Grace. Congratulations, Mike. I know you are coming off paternity leave to be here for this hearing, so thanks, and I commend you for your work.

In the 2019 National Defense Authorization Act, Congress charged the Solarium Commission with developing a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequence. In our first meeting, however, outside experts on congressional commissions told us that we were attempting the impossible. We were trying to have a 9/11 Commission-level of impact without the precipitating event of a September 11.

Well, Madam Chair, I reject that cynical view. I believe that if we come together in a nonpartisan fashion to implement the Solarium Commission recommendations, we can alter the trend that sees our cyber risk grow year after year. We can push back on our adversaries, who see the cyber domain as the ultimate realm for asymmetric operations in the gray zone short of war. We can seize the initiative and ensure that we are not left to wonder the day after an attack what more could we have done.

So, that is how I view the work of the Cyberspace Solarium Commission. That is the urgency I bring to the table. And more so than any of the other 82 recommendations the Solarium Commission proposes, the National Cyber Director is essential to seizing the initiative from our adversaries.

It is essential because cybersecurity permeates every aspect of our society and every aspect of our Government. Every department and agency, from the Department of Agriculture to the Department of Veterans Affairs, relies on secure information technology to conduct business, yet very few of them have cybersecurity as part of their mission, nor is it their primary focus.

Because cybersecurity is difficult to measure, we end up with misaligned incentives. People skimp on cybersecurity because they

would rather invest in operationally relevant programs in their department. We need a strong leader in the White House to defeat the inertia that pushes investments in cybersecurity down the road or until a devastating breach occurs. We also need as strong cyber leader in the White House to coordinate strategy.

Beyond Government systems, our national and economic security rely on critical infrastructure, most of which is owned and operated by the private sector. Where once we could rely on two oceans and friendly neighbors to insulate us, today our banks, hospitals, and power plants are on the front lines of shadow campaigns to undermine our way of life. Only within the White House can we break down agency silos to ensure that we have a "whole of nation" effort to protect our networks.

Finally, Madam Chair, we need a National Cyber Director in the White House to coordinate incident response. We are living through a public health crisis right now, the likes of which we have not seen in over a century. When our adversaries strike us in cyberspace, we must be prepared to defend early, to stamp out the infections from computer viruses, to quarantine affected networks, and to inoculate uninfected machines by patching them. This is only possible with a National Cyber Director.

This idea, of course, is not new. I worked on it with the CSIS Commission for the 44th Presidency in 2008. But as my friend Mr. Gallagher has taken great pains to describe at length, the Solarium process pioneered by President Eisenhower has a way of refining one's thinking. We debated the proposal for a National Cyber Director extensively, and we were very deliberate in our decisionmaking.

We chose an office in the White House because only the White House can truly reach across departments and agencies to manage a risk so pervasive as cyber. We chose a Senate-confirmed position because congressional oversight and buy-in is critical to the success of the office. We chose to preserve a coordinative rather than operational bend to the role because our cyber defenders need strategic guidance, not tactical advice.

Madam Chair, just to conclude, there are some who argue that the National Cyber Director is congressional overreach. There are those who say that the President is the ultimate arbiter of the Executive Office of the President and that Congress has no business interfering in these Article II affairs. Those people, respectfully, disregard history, as Congress has helped to guide White House structure in the past when the moment demanded it, such as when Congress created the Office of Science and Technology Policy or the U.S. Trade Representative. But more concerning to me, these people implicitly endorse the status quo, and that scares me.

It scares me because every day I wake up and see our adversaries making gains in cyberspace. I saw it under President Bush, I saw it under President Obama, and I see it today under President Trump. I see our adversaries stealing our intellectual property, shaping norms that suit their interest on the international stage, striking out at our partners and allies, and attempting to undermine our elections.

Madam Chair, it is time we seize the initiative. It is time we set the agenda, pushing back on our competitors and shaping their be-

havior by improving our resilience and in strengthening the cyber ecosystem. It is time we empower the National Cyber Director at the White House.

Madam Chair, with that, serving on the Cyber Solarium Commission with Mr. Gallagher has been one of the most rewarding experiences of my life. His leadership and that of Senator King, the contributions of our fellow commissioners, and the enormous dedication of our immensely talented staff are all reflected in the bill that we are discussing today. It is an honor to have the opportunity to present it before you, and I look forward to answering any questions that you may have.

Chairwoman MALONEY. Thank you so much, Congressman Langevin, and thank you for your leadership and passion for the security of our Nation. I now recognize Mr. Gallagher.

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

Mr. GALLAGHER. Thank you, Chairwoman Maloney and the rest of the committee, and thank you for the kind words about my newborn daughter. If I pass out during this hearing, it is not only because I am nervous to be on the wrong side of the hearing here as a Member, but because I haven't had much sleep in the last two weeks. But we are truly blessed, and I appreciate the kind words.

As Dwight Eisenhower said, "We do not keep security establishments merely to defend property or territory or rights abroad or at sea. We keep the security forces to defend a way of life."

And right now, emerging technology empowered by stronger and more capable digital networks is being infused into every part of our Government, economy, and our way of life. How we navigate the resulting opportunities and challenges will determine the effectiveness of our Nation to deal with future cyber-driven or cyber-enabled contingencies. For the past 20 years, commissions, initiative studies, and even four Presidential administrations have been challenged to define and establish an effective national-level model for coordinating cyber strategy, policy, and operations.

I believe it is imperative that the executive branch have a strong, stable, and expert-led cyber office and leader within the White House. Whether to create the position of a National Cyber Director, however, and what that position would entail was one of the most spirited and important debates we had over the course of the commission.

My colleague Jim Langevin was absolutely incredible in his thought leadership and his dedication to the integrity of the Cyberspace Solarium Commission process, and I learned a ton from him throughout. And due to Jim's leadership, we really considered, one, how to address the gap in national leadership and coordination and consistent prioritization; two, whether to recommend Senate confirmation; and three, the size, structure, and scope of authorities for the coordinator and leadership office.

Ultimately, we decided that the Federal Government would be better equipped by strengthening existing department and agency efforts in cybersecurity, including the Cybersecurity and Infrastructure Security Agency, rather than the creation of a new depart-

ment, as many advocated for. Therefore, without a new agency, the commission deemed the institutionalization of a cyber coordinator position in the White House within the Executive Office of the President to be essential to give the position a high enough level of prominence to effectively coordinate national strategy and provide much-needed leadership internationally, with state, local, tribal, and territorial governments, and with the private sector.

And in recognition of that need for better collaboration, the Chamber of Commerce recently endorsed the National Cyber Director Act, our bipartisan legislation that Representative Langevin has led.

The commission spent an enormous amount of time weighing the pros and cons of this position and in contemplating the stature of the position. We determined that requiring it to be Senate-confirmed, similar to the way in which the U.S. Trade Representative is Senate-confirmed, would not only signal that Congress is committed to cyber issues but also afford us, as legislators, a level of access to that conversation, but also the person that occupies that position a level of political support that bipartisan endorsement would bring while maintaining the discretion of the President in selecting that candidate.

Making the role Senate-confirmed, in other words, would provide greater permanence by institutionalizing the position's existence and ensuring the role would endure throughout Presidential transitions and not just be dependent on the whim of a particular President or a particular National Security Adviser.

I understand there are those, particularly my Republican colleagues, who may be skeptical that this is an added layer of bureaucracy. I just would say to you that I came into this discussion with that as my ideological prior. But unless you believe that the status quo is, indeed, getting the job done, unless you believe that we are, at present, well-structured to avoid a cyber 9/11, as my colleague referred to, then you have to consider how we can make a meaningful reform of the status quo.

Indeed, rather than creating an entirely new agency, which would take years to create, which would be much more complex and would further muddy the bureaucratic waters, I view the creation of a single focal point in the White House, a single person—or to quote my co-chair Angus King, a single throat to choke—someone who is responsible for this effort, to be the least bureaucratic, the least onerous, and the most efficient of all possible options. It also gives Congress a greater window into this discussion, as I alluded to.

I believe, in closing, that we in Congress must sufficiently enable the Federal Government to create a cohesive national strategy and defense in the cyber domain, as we do in all other domains of battle, and we must do so today. So, I urge you to support the commission's recommendation on the creation of a National Cyber Director so that, in Ike's words, "When we fight, we will fight in all elements as one single, concentrated effort."

With that, I will close my comments. I thank you for your time and consideration.

Chairwoman MALONEY. Thank you, Mr. Gallagher. This is truly a bipartisan goal to protect our country.

We will be limiting questions for the first panel. I now recognize myself for five minutes for questions, and Mr. Gallagher, I want to start with you.

The current coronavirus crisis has created a systemic shock that has exposed a number of critical ways in which our country failed to prepare for what many would call the "inevitable." In our increasingly connected and technology-driven world, many experts warn that a large-scale cyber-attack is also inevitable.

The Solarium Commission recently released a white paper examining cybersecurity in the context of the pandemic, and Mr. Gallagher, your white paper lays out some interesting parallels between lessons learned during the coronavirus pandemic and how these lessons can inform our preparation for significant cyber-attacks. Can you share some of these parallels and your recommendations with us?

Thank you.

Mr. GALLAGHER. Absolutely. You know, obviously, they are not perfectly analogous events, but I would highlight a few similarities. There are really three stand out in my mind that we analyzed in our white paper, our pandemic annex. First, both the pandemic and a significant cyber-attack can be global in nature, requiring that nations simultaneously look inward to manage a crisis as well as work across borders to contain its spread. Both are difficult to contain across borders as well.

Second, I would argue that both the coronavirus pandemic and a significant cyber-attack require a whole of nation response effort and are likely to challenge existing incident management doctrine and coordinating mechanisms, as we are discovering right now with every state, every county, every city government, and a bunch of nonprofits having to figure out how they can all work together in order to slow the spread of the disease.

And finally, and perhaps most importantly, I would argue the similarity is that prevention is far cheaper and pre-established relationships far more effective than a strategy based solely on detection and response. That is why if you read not only our pandemic annex but our broader Cyberspace Solarium report, which we had the unfortunate timing of releasing on March 12, 2020, the last week we were in session in the House before shutting down, you will see that a lot of what we are trying to do is to get left of boom, for lack of a better term, figuring out how we can force the Federal Government—in partnership with Congress, in partnership with state governments, tribal governments, territorial governments—to think through the unthinkable. Think through how we can rapidly restore our economy in the event of a cyber-attack, to be able to come back stronger and strike back against our enemies and, therefore, restore deterrence.

So, you know, I will be cautious about extending the similarities between the pandemic and a cyber-attack too far, but those three stand out in my mind.

Chairwoman MALONEY. Well, thank you. Thank you very much.

Mr. Langevin, the commission recommends establishing a National Cyber Director to coordinate the Federal Government's incident response activities. Can you share examples of how the

coronavirus pandemic and shifts to remote services have led to additional cybersecurity challenges?

Mr. LANGEVIN. Sure. Thank you for the question, Madam Chair.

Certainly, the pandemic influence has shown the challenges of needing a coordinated response, and when you have a diffused response and many people in charge—for example, just so you can get to the states as we have—it makes it more challenging to have a cohesive direction in which to go. So, we want to make sure that with respect to a cyber incident that we are both having someone that thinks about this in terms of pre-planning, so looking at the most vulnerable areas, say, of potential cyber-attacks on critical infrastructure, which is owned and operated in the private sector, and figuring out how we can make our cyber networks more resilient and how we would get them back up and running more quickly.

But in the actual incident, if it were to occur, that you have a single point of contact that is both the principal adviser to the President, he or she is the coordinator to bring the interagency together, or the National Security Council together, or the Economic Security Council together to lay out options for response and have a more coordinated, cohesive, and effective response.

Chairwoman MALONEY. Thank you. How would establishing this role have made a difference in our response to the COVID–19 pandemic?

Mr. LANGEVIN. Well, I think it is probably more analogous to how we would, say, respond to a cyber-attack or intrusions on our elections, but certainly, there are elements of cyber response to COVID. For example, what we know of the Chinese and other entities trying to steal intellectual property for the development of a coronavirus vaccine or therapeutics. We would have a much more focal point in which the Cyber Director would, again, be able to coordinate the relevant departments and agencies or private sector entities to effectively coordinate the response that needs to be taken to protect those networks and prevent intellectual property, hopefully, from occurring in the first place.

Chairwoman MALONEY. Thank you.

Now for both of you, is it your opinion that establishing a National Cyber Director is an essential step in ensuring the U.S. is in the best position to prevent and, if necessary, respond to a crisis induced by a significant cyber-attack?

Mr. LANGEVIN. I certainly feel that that is the most effective way to both prevent and also respond to a cyber incident of significant consequence. We thought this through very clearly, and as my colleague pointed out, of the various ways we could have gone having this at an existing department, existing agency, or having the authority in a new cybersecurity agency, or having it in the Senate-confirmed Executive Office of the President position, we felt this was the best way to go of the various options we would have recommended.

Again, it doesn't create an excessive new bureaucracy. I believe it is very streamlined, very focused. It gives strategic guidance and both advice to the President, but it is going to—the coordinating authority to make sure all the oars are pulling in the same direction in the event of a cyber incident.

Chairwoman MALONEY. Well, thank you.

Mr. GALLAGHER. I would second——

Chairwoman MALONEY. Mr. Gallagher, do you want to add to that?

Mr. GALLAGHER. Well, I just would second Jim's remarks and say I think of it as a necessary, but insufficient recommendation. It is part of a broader suite of recommendations. I think, if you read our final report, what you see is a genuine attempt from commissioners on both sides of the aisle to elevate and empower existing agencies rather than create a bunch of overlapping new bureaucratic structures.

And I do want to commend the work of a lot of great leaders we have at the NSA, at CISA, who have really learned a lot of lessons in the last four years and come a long way. We are not saying they haven't done good work. We view this as a way to better empower them and build upon the lessons of the last few years.

Chairwoman MALONEY. Well, I agree with the commission and my bipartisan colleagues in Congress that we need a centralized cybersecurity position at the White House to develop and streamline the Federal Government's strategy, coordination, and response to cyber threats and strengthen all activities that are taking place now. I thank you all for your hard work and your testimony today.

I now recognize the distinguished ranking member for five minutes for questions. Representative Comer?

Mr. COMER. Thank you, Chairwoman. I had a very good conversation with Jim yesterday about this legislation, and I am going to direct my questions to my good friend Mike Gallagher. Will the National Cyber Director legislation create budgetary hurdles in how it works with the Office of Management and Budget, OMB, that might artificially constrain a President's cyber policy decisions?

Mr. GALLAGHER. We examined that in depth. Ultimately, I don't think so. We are giving—in our construct, giving the National Cyber Director budget certification authority, which effectively means he has the ability to look at various executive branch agencies when it comes to cyber elements within their budget and flag effectively for the President something of concern, but the President still retains the ultimate authority to adjudicate that dispute.

If, for example, there was a disagreement between OMB and the National Cyber Director, just as there is often a disagreement within different executive branch agencies, the President, and working through his National Security Adviser, can adjudicate those disputes, and he can choose whether or not to follow the advice of the National Cyber Director. So, while the National Cyber Director would have that budget certification authority, he can't go in and mess the entire process up, for lack of a better way to describe it.

Mr. COMER. OK. I have heard different people describe what they view this might entail, but would the new office comprise a large new staff? I have heard between 75 and 100 new staffers. Obviously, that would create a new bureaucracy, and we are always careful about creating new bureaucracies.

So, what is the prediction of a budget? How much will this cost? How many staffers are we talking about here?

Mr. GALLAGHER. I would say, as we estimate, 75 is about right, and I understand your concern. That is not nothing. That would replace about the 15 that are there right now.

I just would say if you look right now at the, let us say, the comparison of people and resources we devote for its offensive operations with NSA and Cyber Command versus what CISA has to do defensive operations, you will see a dramatic imbalance in terms of the personnel that we have, thousands of personnel difference. So, even though we would be adding anywhere between 75 to 100, that would be a small step toward perhaps correcting that imbalance, giving the White House better purview into defensive operation.

What the budgetary impact of that would be, we think it would be in the low, you know, about $10 million to $15 million, but some of that depends on whether these people are detailees from other agencies. But I am not suggesting it is nothing. It is a growing of an office within the organization, but that is also consistent with precedent for other Senate-confirmed offices within the Executive Office of the President.

Mr. COMER. And I certainly understand the concern and appreciate the effort here to alleviate that, but if this is staffed by career officials or detailees from other agencies, why won't it become another bastion for employees who refuse to honor the policy prerogatives of an incumbent President, something that this President has been battling, as you know, for the last 3 1/2 years?

Mr. GALLAGHER. Well, I don't doubt that that is a problem within the executive branch, and having worked in the executive branch, I think there is always a tendency, you know, for—if you are a bureaucrat, you sort of believe in the status quo. The old saying goes, "Where you stand depends on where you sit."

But at the end of the day, that is a broader cultural issue where everybody that works in the executive branch, whether they are wearing a uniform or they are a civilian, needs to understand that they work for the President, regardless of that President's party. So, I don't think this would solve that problem necessarily, but I don't think it would make it dramatically worse.

Mr. COMER. Just out of curiosity, have you had any conversations with anyone in the White House to gauge their level of support or opposition for this proposal?

Mr. GALLAGHER. I have had conversations with the White House.

Mr. COMER. OK. Well, good deal. Well, my time is about to expire, and I have the utmost respect for you, Representative Gallagher. You and Will Hurd on our side certainly are the foremost experts on cybersecurity. I appreciate what you are doing here and look forward to further conversations. With that, Madam Chairman, I yield back.

Chairwoman MALONEY. I understand that—right now? Thank you, Mr. Comer.

I understand Representative Chairman Lynch is at another meeting. So, I now recognize the distinguished ranking member for the Subcommittee on National Security, Mr. Grothman, for his questions.

[Pause.]

Mr. GROTHMAN. Can you hear me? Can you hear me now? Can you hear me?

Mr. GALLAGHER. Yes, loud and clear.

Mr. GROTHMAN. OK. OK, did the Solarium Commission take a position on whether our Nation's cybersecurity posture has improved over the years? Are things getting better or worse, I guess?

Mr. GALLAGHER. I will offer my view. I think after a year of extensive conversations with General Nakasone, Chris Krebs, and a lot of talented people in DOD, many of whom participate in the commission, I think we have gotten a lot better. And a lot of that is due to legislation that we have passed in Congress. On the Armed Services Committee, we have effectively devolved greater authority down to lower levels so that people can operate in cyber with the speed and agility that is necessary to have an effect.

I think if you look at sort of lessons learned from 2016, there was a concerted effort in 2018 to protect our democracy. So, I have actually been very impressed with the work of General Nakasone and a lot of other dedicated cyber warriors in this space.

Mr. GROTHMAN. OK——

Mr. LANGEVIN. Now if I could add, and I would agree with my—again, as the chairman of the Intelligence, Emerging Threats, and Capabilities Subcommittee, I oversee both NSA and U.S. Cyber Command. I see the extraordinary work that General Nakasone and his team are doing at U.S. Cyber Command. Also sitting on the Homeland Security Committee and on the subcommittee that helps to oversee CISA, we are getting better and better and more effectively organized to combat this growing threat.

So, we have gotten better, and I support, for example, the administration's new guidance on cyber, NSPM–13, so we are more forward leaning. So, defending forward, if you will. I think we were probably too reserved in past years, and now under the current construct, we are more forward leaning. So, as Chris Engels liked to say, it is defending early, or you could say it is often said defending forward. But I think it is the right strategy.

But our enemies and adversaries are getting more and more effective and more successful and sophisticated in their ability to carry out cyber-attacks of significant consequence. So, we need to continue to evolve, and that is why this new added position is helping us to get even better. Going from the category of, say, good, better, best——

Mr. GROTHMAN. We are moving to get better even faster. Is that what you are saying?

Mr. LANGEVIN. Yes.

Mr. GROTHMAN. We are only going to get better faster. Do we have a data bank of breaches or incidents that we feel we are going to try to prevent in the future? I mean, can you like rattle off the top 5 problems we have had in the last three years, say?

Mr. LANGEVIN. Well, just by way of example, and this is an example that I use pretty frequently, we are trying to prevent the next OPM breach, for example. The breach that occurred at the Office of Personnel Management happened because there was a Department of——

Mr. GROTHMAN. That is one. Why don't you rattle off like the three or four worst breaches in the last, say, four years that you feel concerned about?

Mr. LANGEVIN. Well, there was the WannaCry incident that occurred, the Sony breach that occurred that North Korea carried out. Of course, the WannaCry was probably one of the most costly cyber incidents that occurred in world history, and it cost FedEx and Merck and Maersk billions of dollars in lost revenue when their computers were wiped out or damaged. So, the amount of intellectual property theft that has occurred over the years, it has cost U.S. jobs and economic competitiveness to the tune of hundreds of billions, if not trillions, of dollars.

So, the list goes on and on, not to mention, of course, the amount of personal private information that has been stolen. We are getting better at responding to and protecting against these things, but we are not——

Mr. GROTHMAN. Well, why don't you just forward to me, you know, six or seven ones that we are trying to prevent in the future.

I missed something. One of you guys talked about John Bolton dismantling some agency or commission or whatever. Could you go over that a little bit?

Mr. LANGEVIN. Yes, if I could jump in on that? I know Mike is going to want to comment. But under every administration, we were making forward progress on cybersecurity. John Bolton was the first person really in an administration to take us backward when he eliminated the cybersecurity coordinator position.

Now that wasn't Senate-confirmed, didn't have policy or budgetary authority, but at least it was there. In fact, one of the people on the second panel, Michael Daniel, was the cybersecurity coordinator under President Obama. Rob Joyce under the Trump administration——

Mr. GROTHMAN. It just hits me as odd. I wonder what his logic was. Why did he do that?

Mr. LANGEVIN. I think he sold the President a bill of goods by eliminating the position. I think he did a disservice to the President.

Mr. GALLAGHER. I think he might argue he is streamlining the overall NSC process, and indeed, his predecessor—or his successor has tried to continue that process. I think what we are arguing is that even that status quo ante with a cyber coordinator was not sufficient really to get the overall interagency, interdisciplinary oversight you need of cyber, as well as develop long-term expertise.

Again, to go back to the Senate-confirmed bit, you know, we want this person to not only have the ear of the President, but be, you know, a single bellybutton that we, as legislators, can push to get answers when it comes to Congress.

As for your earlier question, Glenn, I will send you on—throughout our report, we really go through all of the major infiltrations attributed to China, Russia, North Korea, and Iran, as well as nonstate actors, and lay it out. And just one that always comes to mind for me as a defense guy, basically, from 2006 to 2018 something called Advanced Persistent Threat 10, when China was conducting systematic cyber espionage campaigns, stealing IP and compro-

mising computer systems containing personal information from over 100,000 U.S. Navy personnel.

So, in addition to OPM—and I have the letter I received from OPM framed somewhere here in my basement, saying my records have been hacked—there has been a lot of these little attempts to exfiltrate data directly from our military and compromise the data of military personnel.

Mr. GROTHMAN. I don't even know, Mike, if someone tries to do that, do we find out right away? Or might all sorts of things be going on, and we have no idea it happened?

Mr. GALLAGHER. It just depends. I mean, certainly there has been lag time in detection for some of the major breaches we have had. Again, I would say that we have gotten better in detecting how this happens. We are going to have testimony from a variety of true experts in this space, like our former colleague Mike Rogers, who can speak to that.

So, I think we are getting better at rapid detection, rapid attribution, and a better process for response. But as Jim rightly pointed out, the threats are getting better as well and better at anonymizing the origin of the threat.

Mr. GROTHMAN. Thank you.

Chairwoman MALONEY. Thank you very much to my esteemed colleagues for their tireless work on the commission and for sharing their work with us today.

Would either Mr. Langevin or Mr. Gallagher like to stay for panel two? You have been generous with your time, but we would be very happy to waive you in. Would you like to stay?

Mr. LANGEVIN. Yes, I would like to stay for a bit, Madam Chair[SA1]. And if I could ask unanimous consent that a letter of endorsement of the National Cyber Director by the U.S. Chamber of Commerce be added into the record? Could I ask unanimous consent to do that?

Chairwoman MALONEY. Absolutely. Absolutely. So ruled.

Mr. GALLAGHER. I, too, have the T&I markup going on right now. So, I may have to go in and out, as well as many diapers that I have to change upstairs. So, if you will indulge me with that, I may not be able to attend the whole second session.

Chairwoman MALONEY. Thank you. So, without objection, the gentleman from Rhode Island will be permitted to join the committee for this hearing on the virtual dais and question the second panel.

Now I would like to introduce our second panel. The Honorable—what? And the gentleman from Wisconsin. OK.

I will now introduce our second panel. The Honorable Mike Rogers, former Member of Congress, chairman of the House Permanent Select Committee on Intelligence from 2011 to 2015.

Michael Daniel, president and CEO of the Cyber Threat Alliance and former cybersecurity coordinator for President Obama from 2012 to 2017.

Amit Yoran, chairman and CEO of Tenable; founding director, U.S. Computer Emergency Readiness Team.

Suzanne Spaulding, Senior Adviser for Homeland Security at the International Security Program at the Center for Strategic and

International Studies; commissioner, U.S. Cyberspace Solarium Commission.

Jamil Jaffer, founder and executive director of George Mason University's National Security Institute.

The witnesses will be unmuted so we can swear them in now.

So, please raise your right hand. Do you swear or affirm that the testimony you are about to give is the truth, the whole truth, and nothing but the truth, so help you God?

[Response.]

Chairwoman MALONEY. Let the record show that the witnesses answered in the affirmative. Thank you, and without objection, your written statements will be made part of the record.

With that, Chairman Rogers, it is nice to see you again. You are recognized to provide your testimony.

**STATEMENT OF HON. MICHAEL J. ROGERS, DAVID ABSHIRE CHAIR, CENTER FOR THE STUDY OF THE PRESIDENCY; FORMER REP. AND CHAIRMAN, HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE**

Mr. ROGERS. Thank you, Madam Chair. It's good to see so many colleagues I had the privilege to work with and some new ones as well and to be on a panel of very distinguished experts in the field of cybersecurity and actually how we approach it.

This has been a very long journey for me, Madam Chair, to get to where I would sit in front of the committee and say I support a Cyber Director, as Congressman Langevin and my good friend Congressman Ruppersberger both have reminded me over the years how I was just wrong about this. Matter of fact, they've invited me to dinner under the—under the understanding that they want to watch me eat crow, as I testify today in my support, my wholehearted support for the National Cyber Director bill that you propose today.

I'll tell you why. I looked at it certainly when I was chairman, prior to being chairman on the Intelligence Committee, and now subsequently, in my private sector life doing both policy work with the center and the study of the presidency looking at all the machinations of how we can combat this threat. And in the private sector, I am part of several small cybersecurity startup companies that have had the opportunity to view how the Government is doing some of these things and offer products out into the commercial market to help defend our private sector from aggressive cybersecurity threats.

All of those things have led me to really change my mind. I looked back and have a lot of the same arguments. If it was—and if Congressman Langevin and Dutch Ruppersberger and myself and Representative Comer sitting in a meeting probably in 2008, I think it would have been two people on one side of the table and two people on the other. I was worried about this expansion. So, there was a lot of talk at that time about an agency or a czar, and I just didn't think we should go there, and we've had lots and lots of discussions.

What I find this bill does that I think was different than previous discussions is that it doesn't expand government, which I'm really concerned about, it focuses government. And if we need any-

thing now in the cyberspace, we need focus on what our Government is doing, and does it have the right resources?

You know, we've taken some important steps in the past in Congress. The Federal Information Security Management Act of 2002 kind of got it started. There was a modernization in 2014. But here is the problem.

Imagine if you take the quarterback and not let that quarterback train with the football team all year until the first game you put him out on the field. We're going to have problems. This is exactly how we have set up our ability to monitor, to oversee the large enterprise which is the Federal Government.

If you think about it, I know there's been a lot of talk about incidents, and we certainly need to be prepared there. And certainly, the NSA has that ticket. But think of these agencies—I'm just going to read off three of them. I went online on the Inspector General reports, and there are hundreds and hundreds and hundreds of these agencies, by the way, who are getting paid auditors to come in and do their basically review of their cybersecurity programs, if they're meeting Federal guidelines.

We think of the big ones, but we don't think of the Farm Credit Administration, or we don't think of the Committee for Purchase from People Who Are Blind or Severely Disabled. And think of the information that those organizations have that are pretty sensitive information, the Pension Benefit Guaranty Corporation. So, when you look at this whole—and I have dozens of these. I could go through them for an hour.

On all of the agencies who are absolutely under siege today, think of it. Billions of times a day, somebody is getting up in the morning with a sole purpose and job to try to penetrate the U.S. Government at any level. That happens every single day. Every agency I mentioned plus the hundreds others are under siege from cyber either espionage or destruction of data.

That's happening, and it's happening in a pretty big and significant way. And we're going to need to do something, and so we're looking at it from the wrong end. And I want to tell you two reasons why here, and my testimony highlights some of the threats that we've been dealing with. But I just want to give you an example of why I thought, all right, we have to change the way we're thinking. We can't continue to do it the same way and expect a different outcome here.

There was an OIG inspection of a particular agency of which we would all be concerned about if that data were exposed. And what they found is they found about 25 serious changes that needed to be made. This was in 2019. And here is the conclusion. So, remember, outside firm hired to come in and say these are the things you're doing wrong. We'll be back next year to see if you've corrected them.

Next year, right? A year in cyberspace is a lifetime. A quarterly report is a lifetime. That means we've got lots of exposure there.

And this was the one that got me. Here is one of their recommendations. If this agency continues a delay in corrective actions, a material weakness in information technology security control may be reported in 2020. That tells me we are not prepared for the threat that is knocking on our door today.

And part of the reason is they have to coordinate through a whole series of bodies. Let me just give you a little bit. It's OMB. They have to do with DHS. They have to coordinate with all of these different agencies to come up with what the guidelines are to move out.

All of those agencies are under their own attacks, by the way. They all have their own cyber operations, by the way. And there is no person, no organization set over top of it to say I'm going to be either the cavalry to help you in your deficiencies, or I'm going to help you find out what's wrong and how we fix it in a short order.

Nothing is steering that. So, yep, we're going to need—we're going to need help on the fact that we are going to have incidents, that we are one keystroke away from an incident that has major consequences in the United States. Why? Because we just under siege.

The Chinese has been highlighted in intellectual property theft and now disruption. They're changing their policy. They'd like to disrupt things. Remember, if American people stop trusting their institutions to the point where it's not governable, guess what? Bad guys win. China wins. Russia wins. Iran wins. North Korea wins. And they all know it.

Matter of fact, I just want to read you this quick quote, if I may, Madam Chair. And this was done by General Gerasimov of Russia. "A perfectly thriving state can in a matter of months, even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war. The role of nonmilitary means of achieving political and strategic goals has grown." And he's talking about cybersecurity and cyber influence operations and disruption cyber activities for the public to lose trust.

"And in many cases, these tools have exceeded the power and force of weapons in their effectiveness." That was 2013.

Fast forward, what's happened since 2013? We've watched the Russians engage in aggressive information operations, including the attempts to penetrate networks of which our concern to disrupt things. And public reports show that the electric grid was attempted to be penetrated. There are reports that they tried to penetrate our stock market.

Why? Disruption leads to chaos, leads to distrust in American institutions. This is as serious a problem as we can get.

And that conclusion that I came to, and I'm going to have to eat crow with my good friends Mr. Langevin and Mr. Ruppersberger, is that if we don't have something—and I don't agree with a big agency. If we don't have something that doesn't expand Government but focuses our cybersecurity efforts, we are going to be in for a long run.

We've had these conversations. We've admired the problem. We've worshipped the problem. Now we have to do something about it.

I think that this agency will help all of the agencies get to where they need to go, and that's why I'm before the committee today, offering my support for this legislation.

Chairwoman MALONEY. Thank you so much, Chairman Rogers. That was a very, very powerful and moving presentation.

And Mr. Daniel, you are now recognized.

**STATEMENT OF J. MICHAEL DANIEL, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CYBER THREAT ALLIANCE; FORMER WHITE HOUSE CYBERSECURITY COORDINATOR**

Mr. DANIEL. Thank you. Good afternoon.

Thank you, Chairwoman Maloney, Ranking Member Comer, and other distinguished members of the committee, for the opportunity to testify before you today on the topic of this legislation and the National Cyber Director.

I'm also happy to be on the panel with people that I consider friends and colleagues, all of whom we've worked together and have known each other for many years.

As you might imagine, I think about this issue a lot. I served for 4 1/2 years as the special assistant to the President and cybersecurity coordinator on President Obama's National Security Council staff. And since then, I've served as the president and CEO of the Cyber Threat Alliance, which is a nonprofit threat and talent sharing organization.

And cybersecurity is a tough issue for almost any organization to manage, and that is certainly true for the Federal Government. Yet as our digital dependence continues to increase, something we've actually talked about this morning—this afternoon already, the imperative for the Federal Government to get better at managing cybersecurity also increases. The rapid shift of certain economic activities online as a result of the pandemic has only heightened this need.

One aspect that makes cybersecurity particularly tough for the Federal Government is that it doesn't fit neatly into one bureaucratic bucket. Cybersecurity is a national security, economic security, commercial, intelligence, law enforcement, public safety, military, foreign policy issue all rolled into one.

Yet at the same time, cybersecurity is highly interdependent. Just like the Internet, all of those aspects that I just mentioned are all connected, and they all affect each other. And they affect each other in some unanticipated ways many times, and that means all of these disparate pieces have to coordinate and work together in order for the whole to be effective and not undermine each other.

And we've actually—to some of the questions and commentary from the first panel, we have made excellent progress over the last few years—actually, over the last two decades—in laying the foundation for better cybersecurity. We've put in place better policies. We've enacted laws that have been mentioned, including like the Cybersecurity Information Sharing Act from 2015.

We've put in place organizational structures like CISA at the Department of Homeland Security and U.S. Cyber Command. But we still face certain structural impediments to improving our cybersecurity, and these include cybersecurity's cross-cutting nature, the lack of incentives for coordination across agencies, and the need for incident response coordination, as well as the issue's complexity and its effect on major policy decisions.

So, after wrestling with these issues for several years, I have come to the conclusion that we need a strong position along the lines of a National Cyber Director like the Solarium Commission recommends and like the bill that Representative Langevin is sponsoring. And I don't come to this conclusion lightly.

Prior to serving as the cybersecurity coordinator, I spent 17 1/2 years at the Office of Management and Budget, and I have a career OMBer's natural skepticism for creating new entities in the Federal Government. But in this case, I think it's really the only viable approach that we have. In particular, an EOP-level organization is really the only one that's going to be able to overcome a very significant factor in the Federal bureaucracy, and that's the "You're not the boss of me" problem. And that is just rampant among the Federal agencies, and only something centered at the White House can overcome that.

That said, I would urge Congress to think through the scope and authorities for this position very carefully. It would be very easy to get something—to get it wrong and to end up with something that does take up bureaucratic bandwidth and does not focus things like Congressman Rogers recommended.

Most importantly, this position has to cover all of the aspects of cybersecurity and not just some of them. It has to have oversight of law enforcement, military, and intelligence-related offensive and defensive cyber activities, in addition to network defense. We cannot exclude those positions and expect the position to be a success.

It has to tightly integrate with the OMB budget process and the NSC policy process, or even in the EOP, it won't be effective. It has to have a big enough office to get the job done, but not so big that it is tempted to become operational. And it needs to have a clear relationship with the Federal CIO and the Federal CISO.

At the end of the day, we need a position like the National Cybersecurity Director. Cybersecurity is not just a technical problem. It's also an organizational problem. So, as a result, we're going to need to take some additional organizational steps to address it. We've taken the first few steps along that path, and now it's time to create a position that can bring it all together.

Thank you for giving me the opportunity to testify for you today, and I'm looking forward to your questions.

Thank you very much.

Chairwoman MALONEY. Thank you. And now, Mr. Yoran, you are now recognized.

**STATEMENT OF AMIT YORAN, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, TENABLE, FOUNDING DIRECTOR, U.S. COMPUTER EMERGENCY READINESS TEAM**

Mr. YORAN. Chairwoman Maloney, Ranking Member Comer, members of the committee, thank you for the opportunity to testify today.

I'd like to thank Representatives Langevin and Gallagher for their leadership on the Cyberspace Solarium Commission, the development of the commission's report, and for introducing H.R. 7331.

I'd also like to thank Chairwoman Maloney for serving as cosponsor on the bill.

I'm Amit Yoran, chairman and CEO of Tenable, the world's leading provider of vulnerability management technologies. Tenable empowers organizations of all sizes to understand and reduce their cyber risk. Our solutions serve just about every department and agency in the Federal Government and many state and local governments.

Our customers include over 50 percent of the Fortune 500 and over 25 percent of the Global 2000 and tens of thousands of mid-sized companies in every major industry. Simply put, we're instrumental to helping the Nation and organizations around the world quantify and understand and reduce their cyber risk.

In H.R. 7331, the committee has the opportunity to significantly improve the Nation's cyber preparedness. The creation of the Office of the National Cyber Director within the Executive Office of the President is a critical step forward. My support for this office centers on the need for stronger enterprise risk management practices across the Federal Government and across the Nation.

A whole of nation risk requires a whole of nation response, and indeed, a new, expanded attack surface stretches across the entire nation. This includes every aspect of government as well as private industry. None are immune from the threat of cyber-attacks that imperil our national security, Government services, and the critical functions that citizens rely on.

An accountable executive at the White House would also be helpful in coordinating a whole of government understanding of cyber risk and efforts to proactively reduce cyber risk and coordinate responses when needed. A National Cyber Director is needed to ensure that Government holds itself and industry accountable for baseline standards of care with regard to cybersecurity.

Today, there remains a lackadaisical approach toward understanding cyber risk and proactively maintaining good cyber hygiene, resulting in the vast super majority of today's breaches and associated losses. This is negligent behavior through learned helplessness on the part of individuals, Federal Government agencies, and private industry.

Many of the needed authorities have been outlined in the proposed legislation. In my written testimony, I recommend augmenting the National Cyber Director's authorities under 7331 to include establishing a national encryption policy that balances the needs of law enforcement with those of cybersecurity and public safety; overseeing the vulnerabilities equities process; coordinating with regulatory agencies to set policies and practices which can improve understanding of cyber risk, increase transparency, and implement plans to adequately manage risk; focus efforts on cyber work force development initiatives, with emphasis on greater inclusiveness; and develop and maintain an international cyber strategy for the Nation and lead international cyber engagement efforts.

It would be difficult to overstate the cyber risk that we face today. Governments and businesses utilize cloud computing, Internet of Things, and operational technologies. While these technologies optimize production, drive innovation, and increase sustainability, they also expand the overall cybersecurity attack surface and need to be an integral part of our risk management practices.

These risk management practices must include services and industries essential to our public safety and well-being, such as power, water, transportation, and healthcare, as well as our industrial production. The risk is more than a technical one. It's political, it's social, it's physical, and it's economic.

Cybersecurity can existentially threaten our way of life. There are important steps that we can take to improve our cybersecurity posture in advance of a national crisis, and those steps include the creation of an Office of the National Cyber Director at the White House.

I'd like to thank Chairwoman Maloney, Ranking Member Comer, and members of the committee for their attention to this important topic, and I'll be happy to respond to your questions.

Chairwoman MALONEY. Thank you. Ms. Spaulding, you are now recognized.

**STATEMENT OF SUZANNE SPAULDING, SENIOR ADVISER, HOMELAND SECURITY, INTERNATIONAL SECURITY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, COMMISSIONER, U.S. CYBERSPACE SOLARIUM COMMISSION**

Ms. SPAULDING. Thank you, Chairwoman Maloney, Ranking Member Comer, and members of the committee. Thank you for this opportunity to be here today to testify in support of the Cyberspace Solarium Commission's recommendation to establish a National Cyber Director.

It's really an honor to be here with my fellow distinguished witnesses and former colleagues, and it was a particular honor to serve on the commission alongside Representative Gallagher, Representative Langevin, and the other commissioners and inspiring to see the bipartisan and really nonpartisan approach that all of the commissioners brought to the work of the commission. And this recommendation is no exception.

As has been noted, the commission considered alternative approaches to address what we all agreed was an urgent need for stronger coordination across the many entities engaged in cybersecurity for better integration of effort and for more robust strategic planning and prioritization to guide those efforts.

The first panel addressed the alternatives that we considered. So, I won't go through all of them again, but I did want to emphasize the arguments against the alternative of pulling the various cyber entities out of the departments and agencies where they currently reside and putting them together in a new Department of Cybersecurity. I am strongly opposed to the creation of such a department because it would not solve our key coordination challenges and would cause huge disruption with little to no gain.

The most important and challenging coordination issues in the interagency in my experience arise between DOD elements, including NSA; law enforcement, especially the FBI; and DHS. DOD and the IC are not going to relinquish their cyber activities to a new department. Nor is FBI going to turn over its law enforcement activity. Thus, the new department would still face those key coordination challenges.

A National Cyber Director, on the other hand, could and must be empowered to address these key coordination challenges, with the backing of the President. To do this, the NCD must have the authority to convene and get information from law enforcement, the military, and the intelligence community, as well as DHS and the sector-specific agencies, about their operational plans and strategies.

Another important reason I have opposed a new cybersecurity department is the risk that it would become singularly focused on technology. I watched this happen with our WMD efforts in the 1990's when I was at the Central Intelligence Agency, where folks working nuclear nonproliferation, for example, focused entirely on the technical aspects and failed to adequately integrate the regional experts and those studying the leadership and political dynamics within the various countries.

I see these same tendencies in cyber. We tend to turn to technical experts, and they, not surprisingly, focus on the technical aspects, even though we know that understanding and mitigating cyber risks requires a much broader approach that fully recognizes the human element, integrates cyber and physical risks, including knowledge of the operational environment—whether it's financial services, electricity, or election infrastructure—and that incorporates knowledge of each of our adversaries and what drives them.

I've always warned that a new cyber department would be staffed by technical experts and too focused on technical aspects. This could happen to the Office of the National Cyber Director as well, and it is something we must guard against. But sitting within the White House structure, having responsibility for interagency coordination, and working closely with the other elements like the NSC and the Council of Economic Advisers should help guard against that tendency.

Another of the key recommendations from the commission is strengthening and reinforcing the great work that is being done by the group I used to lead at DHS now called Cybersecurity and Infrastructure Security Agency, or CISA. But at present, one of CISA's greatest barriers to effective operations is that numerous Federal departments and agencies often compete for resources and authorities. The NCD can support and enable CISA by pushing to a decision those ongoing battles that cloud the Federal Government in cybersecurity.

The NCD is not intended to direct or manage day-to-day implementation of strategy by any Federal agency, but responsible for overall integration and execution of defensive strategy across the executive branch through strategic policy operations and budget. A National Cyber Director should do only what the agency and department leads cannot do themselves, de-conflict and align cyber missions with national priorities, ensure visibility across the interagency on operational activities, and help push the process to active—into actual decisions.

The NCD will fail if it adds further stovepiping and bureaucracy to our Nation's efforts to reduce cyber risks. Instead, the NCD needs to help empower, prioritize, and provide much-needed support for existing cyber entities within the U.S. Government.

Thank you very much, and I look forward to your questions.

Chairwoman MALONEY. Thank you. Mr. Jaffer, you are now recognized. What?

Voice. Go to questions.

Chairwoman MALONEY. Go to questions?

Voice. Yes.

Chairwoman MALONEY. OK. I now recognize myself for five minutes for questions.

Thank you very much to all of the panelists for your testimony, and I want to dig a little deeper into the 2017 malware attack executed by North Korea. This attack disabled hundreds of thousands of computers in hospitals, schools, businesses, and homes in more than 150 countries. It even shut down a portion of Britain's National Health Service for a week.

So, Chairman Rogers, can you describe the potential effect a cyber-attack on critical infrastructure like this could have in the United States?

Mr. ROGERS [continuing]. Fortunate it was North Korea. It was a ransomware-based attack that in some ways didn't even have a way to pay back the—pay the ransom. So, it was probably the least-capable actor, even at a high end, that was able to infect these systems.

And it was—it had a global-wide impact, and sometimes surgeries were turned off because they couldn't actually access the right and appropriate records for the surgeons to do a surgery. So, you can imagine it had both health impacts of that sort, financial impacts, and as you said, schools. It was really, really dangerous, and it was very widespread. And part of it was they couldn't control it. It kind of fed on itself and spread without them directing it, which is a whole problem of probably not a top-tier nation-state actor.

They've gotten better since then. That's the scary part. So, I would say that when you look at what the threats are, we know where our biggest adversaries are coming. So, China uses all of its state power to do and set themselves up for influence around the world. They use diplomacy.

And if you look at the fact that they've confiscated masks from rightful contract owners that they were going to be delivered to, gave them to entities in China so they could deliver them in a way to try to get credit for their influence operations. They use military, defense, and intelligence cyber operations. They use cyber operations for espionage.

I would look at all the ways they're coming at us. What we know is they'd love to get access to people's data from a nation-state perspective, but also cyber criminals, organized cyber criminals and others who would love to get the data that the U.S. Government collects from U.S. citizens. Everything from food stamp participation—think of all the information you have to give in order to get that program and qualify for that program. It's sitting in a repository at the Federal Government. That's valuable to a cyber thief.

So, I would look at this. I mean, that was a massive attack by a nation-state, but we have all of these other attacks underneath it. And again, that's my argument for the Cyber Director is you

want somebody not just to incident respond, you want somebody for pre-crisis.

How do you help these agencies? Not hurt them, not hit with a club when they're not doing it right. But help them through what they need to look like in their cyber shops and the kind of tools that we do, and by the way, can we do this with a collective defense mentality so that when one gets attacked, everybody knows what that threat is moving forward?

That's the way I would look at this. Let's try to be pre-crisis. And having that Director whose sole job every day is to get up and she needs to think through all of those problems, my argument would be we're going to be better off.

Because there is lots of talent. I think Mr. Gallagher and Mr. Langevin highlighted it, lots of great talent out there. We need to now coordinate it. Remember, not expanding it in Government, but focus it on the problem that helps us the most.

Chairwoman MALONEY. Mr. Yoran, I was shocked by the statistic from Tenable's 2019 report that 90 percent of critical infrastructure operators witnessed at least one damaging cyber-attack in the past two years. I understand that much of our Nation's critical infrastructure is managed by an array of different companies that are responsible for different parts of the process.

Mr. Yoran, what would happen if one of these companies was compromised? Can you talk about these attacks and enlighten us more?

Mr. YORAN. Yes, I think the effects of the attack can vary—of these attacks vary greatly. In many cases, outage can certainly ensue. In other cases, it's more of a preparation where systems are being compromised, information is being stolen, but the adversary has no desire to create an outage, unless perhaps it's during time of crisis.

So, I think the impacts here could vary greatly, and it's one of the reasons why we need a systemic understanding of risk and why a National Cyber Director needs to work closely with the regulatory agencies that do exist to make sure that we're implementing a standard of care that makes sense, that we don't see the continued sort of negligent behavior where enterprises are not maintaining good hygiene of their systems. They're not providing patches and updates and doing the maintenance that's required to keep them in a secure state.

And this sort of poor hygiene results in a vast super majority of the breaches, including the ones that were cited earlier perpetrated by North Korea and a lot of the damaging ones that we've read about in many of these high-profile cases.

Chairwoman MALONEY. Do you believe that this bill, H.R. 7331, would help the Federal Government address these concerns more effectively?

Mr. YORAN. I think there's no question in my mind, having done cybersecurity now for over 25 years and having spent time in multiple departments of the Federal Government, as well as serving with cybersecurity products to private sector and now also helping the Federal Government with technologies to protect itself. A role like this would help provide a coordinating capability and bring the

maximum understanding and appropriate resources to bear in a coordinated fashion as the Federal Government.

So, I think it was either Representative Langevin or Gallagher who said, you know, the preparation work that we do now can have a significant impact on the crisis that we face or how we deal with the crisis we might face down the road. So, I think the creation of the office and this role are absolutely critical steps forward.

Chairwoman MALONEY. Thank you.

I now want to call on Jamil Jaffer—who disappeared for a while, but he is back with us—for his testimony. Mr. Jaffer?

**STATEMENT OF JAMIL N. JAFFER, FOUNDER AND EXECUTIVE DIRECTOR, NATIONAL SECURITY INSTITUTE, GEORGE MASON UNIVERSITY**

Mr. JAFFER. Ms. Chairwoman, thank you so much for the opportunity, and apologies for the technical difficulties.

Chairwoman Maloney, Ranking Member Comer, members of the committee, thank you for inviting me here today to discuss our Nation's cybersecurity preparedness and the proposed legislation to establish a new Cyber Director.

As the members of this committee all too well know, the cyber threats facing the United States, including our public and private sector, are, in a word, massive. It is no overstatement to say that for all practical intents and purposes, we are at war in cyberspace. And unfortunately, as a Nation, we remain woefully underprepared to deal with this serious and ongoing conflict.

Now lawyers may quibble with whether we're actually at war, and they may point out that the United States nor any of our enemies actually declare that we're at war, but the fact is that for the better part of a decade, our Nation has been involved in a consistent and ongoing series of conflicts in cyberspace, albeit fairly low level. And regardless of whether we call this a war or not, there can be no question that it's had a huge impact on our Nation and its allies.

Cyber-enabled economic warfare conducted by China, primarily focused on the U.S. private sector, drains private companies of billions of dollars a year, with total damages ranging into the trillions. Former NSA Director General Keith Alexander says that this activity represents the greatest transfer of wealth in human history.

Chairman Rogers on this panel nearly a decade ago called attention to this economic threat posed by China and referred to the fact that we were actually in an economic cyber war nearly 10 years ago. And that there are two types of companies in this country, those that have been hacked and know it, and those that have been hacked and simply don't know it yet.

We have also seen countries like North Korea and Iran engage in the destruction of data and bricking of computer systems here in the United States in the last half decade. We know that the DNI has told us that Iran is actively preparing for cyber-attacks against the U.S. and our allies. We've seen the highly corrosive effects of Russia's ongoing active measures campaign on the American body politic, undermining our elected officials, our rule of law institu-

tions, including the Justice Department, the FBI, and the intelligence community.

And to be sure, while we played a role in some of this, the Russians have paid very little price for this, and the Chinese and Russians both know this. We've already seen them mucking around with more covert operations on the COVID virus and the killing of George Floyd.

Now we may see these same players become more active in the upcoming election cycle. In fact, as Chairwoman Maloney noted over three years ago, cybersecurity poses a greater and greater risk to the safety and soundness of our financial system. We know what a serious threat cyber poses to our economy and to our people, and with the current coronavirus situation and the new work from home environment with over 300 million workers around the globe working from home, including 90 percent of banking and insurance employees, these efforts represent a uniquely challenging threat to our economy and to our way of life.

So, then the question becomes what should we do about it, and how much of a role can creating a new Cyber Director at the White House play in this process? While I completely agree with all the members of my panel as well as Congressman Gallagher and Congressman Langevin, who I've had the pleasure to work with in the past, that having a key strategic leader at the White House is critically important, I'm skeptical of the need for a large office of 75 people, fully one-third of the size of the existing entire National Security Council, and the need to have that individual Senate-confirmed.

We know that almost any White House, whether Republican or Democrat, this administration or another, regardless of what you think about this administration, will be opposed to the creation of a new, yet one more Senate-confirmed individual in the White House office.

Indeed, there are other alternatives for the committee to consider, right? The committee may consider creating a position in the White House office, but not making it Senate-confirmed. They may consider creating an office that is smaller and more leadership oriented, a 5-to 10-to 15-person office.

The committee could work with the President to ensure that that person has the rank and stature of a Deputy Assistant to the President and is able to effectively work through the National Security Adviser, has full responsibility for the full range of issues in this space to ensure that we have unity of effort.

There is no doubt with all the cooks in the kitchen from DHS, CISA, to NSA, to U.S. Cyber Command, to the FBI, better coordination, more aggressive coordination with the White House is necessary. The only question for the committee to consider is whether that requires Senate confirmation and a 75-person office. On that note, I am somewhat skeptical, but I recognize that there is a lot of—a lot of my friends and colleagues, my former boss Chairman Rogers, who support this, and I have a lot of respect for that position.

With that, thank you, Ms. Chairwoman. Again, apologies for the technical difficulties earlier, and I yield back the balance.

Chairwoman MALONEY. Thank you. Thank you for your testimony.

And I would like to ask you about the 2017 Russian cyber-attack known as NotPetya. It froze computer systems around the world in exchange for ransom. And in Ukraine, the attacks hit hospitals, power companies, airports, banks, and practically every Federal agency. The U.S. was not immune. This attack hit FedEx and the drug company Merck, costing each more than $300 million in lost business and clean-up.

So, Mr. Jaffer, how great is the risk of a large-scale ransom attack hitting the United States today?

Mr. JAFFER. Chairwoman Maloney, I think it's a huge issue. What you see there in that case was a very carefully crafted attack by Russia against Ukraine. So, a sophisticated actor.

What happened was we had collateral damage, right? These American companies, $10 billion worldwide, the most destructive attack in the history of humankind. And as you mentioned, over five international companies, mostly in the West, who suffered between $250 million to $350 million of damage.

What that demonstrates is that even if you think as a company you're not likely to be affected by a nation-state attack, the reality is you may very well be because you may be collateral damage in an attack by a sophisticated attacker against another nation-state as was the case of NotPetya, Russia against Ukraine.

Chairwoman MALONEY. Thank you. OK, thank you. And a centralized cybersecurity coordinator at the White House seems essential to ensure the swiftness and agility needed to respond to cyber-attacks.

I now recognize the Ranking Member Comer for his questions.

Mr. COMER. Thank you, Chairwoman.

My first question would be for Mr. Daniel. Could you walk me through how a major cyber incident currently proceeds through the Federal Government and how it might change with the advent of a National Cyber Director?

Mr. DANIEL. Sure. I think that right now, it really depends on who first becomes aware of that incident, right? It depends on if that incident is actually disclosed by a private sector entity and how it comes in, whether they disclose it to CISA or to the FBI or to the NSA.

But then at some point, if it gets big enough, that those entities would eventually probably share that information with some of the other elements of the U.S. Government. And then the Government would need to do an assessment on how—whether that incident actually represents something that is more systemic. In other words, is it going to turn into a WannaCry or a NotPetya, where it is going to proliferate across more of the economy, or is it more limited?

And then the Government would need to do an assessment on, you know, whether or not a response is warranted, based on that incident. I think in that case, that's where you would want—when you start to look at how the U.S. Government responds, that's where you really want that coordination, that intense level of coordination to actually come together.

Just because an attack comes through cyberspace does not mean that the only response needs to be back at the adversary through cyberspace. You might want to use other policy tools and means to respond, and that's why that coordination factor across all the different elements of national power is so important.

Mr. COMER. OK. My next question will be for Mr. Jaffer. Earlier this month, in a joint public service announcement by the FBI and DHS's Cybersecurity and Infrastructure Security Agency, the FBI reported it is investigating—and I quote—"targeting and compromise of U.S. organizations conducting COVID–19-related research, PRC-affiliated cyber actors, and nontraditional collectors."

So, in other words, there is reason to believe China is attempting to exploit the recent pandemic to hack into U.S. businesses conducting research on the very virus originating in its own country. So, Mr. Jaffer, could you please explain some of the methods China is using to try to steal our Nation's critical research into this virus or, if you have no insight into current methods, the various ways China accomplishes its many cyber intrusions?

Mr. JAFFER. Thank you, Ranking Member Comer.

You know, the Chinese have been engaged in this effort to steal American intellectual property for the better part of a decade and a half. We didn't talk about it publicly for a long time, and it was only until Chairman Rogers and General Alexander came out and started talking about what was happening with China that the public became really aware of it.

And it's only in recent weeks and months that we've really become aware of our supply chain dependence upon China when it comes to things like PPE and pharmaceuticals. We now realize that that has also expanded well beyond the semi-conductors, quantum, and the like. So, what China is doing is they have literally built their economy on the backs of American innovation, on the backs of American R&D.

You wonder why a Huawei router often looks like a Cisco router? It's because, sir, it essentially is a Cisco router. They stole intellectual property, re-purposed it in China, and then sold it as a good.

Now they've built on that for sure. They are trying to do the same thing in the COVID arena. They're trying to get out ahead of this, trying to have the vaccine first, and essentially grow their economy on the backs of our challenges, and they're going to steal our intellectual property to do that. We simply cannot allow that to happen.

This has been a national-level issue. The President has been very aggressive in pursuing China on this front. We ought not let a trade deal get in the way of ensuring that we hold the line and stop the Chinese from conducting this continuing effort of economic espionage that has allowed them to build their economy on the backs of American R&D.

Mr. COMER. Madam Chair, we had this hearing, and it has become—you know, it has always been clear that cybersecurity is a huge threat to the United States. We talk about China being one of the worst actors with respect to cybersecurity threats and cybersecurity violations. You look more at China, and you see they've been stealing our patents for years, our intellectual property.

Who knows what all they've done with respect to COVID–19? I think we would like to get to know that. I know the Select Committee is delving into that supposedly.

We spend a lot of time in this committee investigating Russia. I believe that the American people, the American taxpayers would be better served if we spent a little bit of time investigating China. So, in closing, I would really encourage you to consider devoting a little bit of time on this committee to investigating China, whether it be COVID–19, whether it be our intellectual property or our patents, whether it be cybersecurity hacks, threats, things of that nature.

So, that is my encouragement to you as we proceed and hopefully work together in a bipartisan way. But I want to thank all the witnesses for being here today, and I look forward to further discussion on this proposal. With that, I yield back.

Voice. Thank you, Mr. Comer.

Next we will go to Ms. Norton. Ms. Norton, you are unmuted.

Ms. NORTON. I want to thank the chair. Can you hear me and see me? I want to thank the chair for this really important and timely hearing.

Because I represent the Nation's capital, I have a special interest in this hearing. We are, of course, like most big cities, but we are not just any big city. And my question goes to what has already happened to some big cities.

I don't know who is going to answer this. Perhaps starting with Mr. Rogers, I am not certain. But we have already seen that another big city, New Orleans, has actually had its—ransomware shut down altogether, grounding all their operations to a halt. Imagine if that happened to the capital of the United States.

So, I must ask if we are fortified here in, for that matter, the Nation's capital and in other cities against similar shutdowns of all operations, blacking out the city altogether? So, I would—any number of you are likely to be qualified to answer this question, but I would begin with Mr. Rogers.

Mr. ROGERS. Thank you, Congresswoman. I appreciate the question.

You know, we've seen this ransomware activity for multiple years now, and it became more aggressive and more aggressive, meaning that it was spreading amongst organized crime, international organized crime groups and others seeking to gain revenue from this, including, by the way, the North Koreans, who used ransomware attacks to gain revenue for the government.

Early on, I hate to say about my brethren in the FBI, their early recommendations to some of these companies were you probably should just pay it because we don't have any way to intercede in the interim to do anything about it. So, you had major hospital organizations, the Los Angeles hospital system comes to mind on one of the early, early cases, where they ended up, you know, distastefully to have to pay for this.

So, it is a real threat. And this is one of the problems with cyber protection writ large. We have to remember that the NSA doesn't protect the private sector in the country. It's a common myth that they're protecting everybody. They're not. They're protecting the Government, and then they're doing collection activities targeted at

our overseas adversaries trying to do something bad to the United States.

So, we have this really uneven ability to stop this in cities across America. And candidly, Congresswoman, I think most cities in America are not prepared for this, and they have old systems. They have legacy systems. They haven't spent the money to upgrade their systems and then provide a level of protection that would keep that data safe.

That's why people are going to cities because they believe that they're the most vulnerable. And again, remember it's not the NSA's job to protect New Orleans or Detroit, Michigan. That's not what they do. So, it is really up to the private sector and those cities trying to develop systems that they can put in place, private systems much like the companies I'm involved with who are looking at collective defense and other things to try to protect it.

This is why, in my mind, a coordinated effort out of the White House with all of our agencies in the right direction and maybe even helps the Department of Homeland Security get the word out to these cities the problems that they really have. So, we are a long way, I guess is the short answer to this. We're a long way from those cities being protected.

And as more international organized crime organizations take on nation-state quality tradecraft, meaning you say the Russian tradecraft depended on the method used, the more susceptible we are. And we're seeing that. We're seeing that leaching of nation-state quality in the tradecraft in cyberspace leach into these organizations.

I argue we're up for a really bumpy road coming up in cyber the next few years outside of the U.S. Government across both private sector and local and state governments.

Ms. NORTON. I guess New Orleans did pay off. I mean, it is really unnerving to hear you say at the moment the vulnerability is so great that you pay off——

Mr. ROGERS. Exactly. And we all know what happens, Madam—Madam Congresswoman. When you pay it, guess what? More people are deciding they want to get into the business and try and extract you from your money, and that's the problem we're running into.

Ms. NORTON. Exactly. That makes us all now vulnerable to paying up.

Mr. ROGERS. Yes.

Ms. NORTON. In the time I have remaining, I really can't help but ask about the election. We have already had perhaps most of our primaries, and I am wondering if any of you, perhaps beginning with you, Mr. Rogers, have seen any interference, any evidence of interference with our elections? I mean, we have seen it with financial institutions worldwide. How about interference with our elections such as, for example, any alteration in election results would occur?

Mr. ROGERS. I can tell you in my work in some of the private work that I do, including being vice chairman of Mitre Corporation, we haven't seen any, you know, flip one vote to another vote. Have not seen that.

We have, in fact, writ large—let's talk about writ large—seen going into 2018 that our adversaries, nation-state adversaries tried to influence elections by creating chaos, and I think we need to be really careful about saying Republican versus Democrat. What they're trying to do is create chaos. They don't care.

They don't like Democrat Americans any more than they like Republican Americans. They don't like either one. So, they're trying to create this chaos in these elections.

General Nakasone and his team I thought did a phenomenal job in 2018 kind of playing that whack-a-mole game to push them back, but we know it's a tactic of which they will use because they've announced that they, the Russians, the Chinese have said, hey, this is very effective, very low consequences. So, we're going to kind of ramp up our engagement in trying to create this chaos going forward.

It is something that I think we absolutely have to pay attention to. Remember, it's very cheap for them. They don't have to go out and buy a new carrier. They don't have to develop a naval fleet and then stock it with——

Ms. NORTON. Are states and cities—are states and cities aware enough so that when they see this, right now it is just interference. It has not had consequences. Are states equipped to fight back in November? We only have a couple of months to be tested.

Mr. ROGERS. Yes. I think it's difficult for states and local governments to do this. I do think we need to look—we need to ask ourselves what do we want our high-tier performing national, Federal agencies to do for us?

I think this is where the National Security Agency and other high-level performers can be very helpful in trying to stop this across the United States, mainly because it is a very sophisticated nation-state actor activity. Now there are some other groups out there that are trying to get into this game that are just—that are worrisome. But I think we should employ all the tools that we have.

And this is where I think congressional oversight is so important. Know what it is, talk to them about what they're doing, and then encourage them because it's not always going to go the way we want. But you have to encourage them to get out there and help push back on these activities.

Chairwoman MALONEY. The gentlewoman's time has expired.

Mr. YORAN. Yes, just we've got a lot——

Chairwoman MALONEY. I now call on——

Mr. YORAN. Sorry. I just wanted to followup on that. I think we have a lot of tools at our disposal. I would just be careful to try and solve all problems with the NSA. I know the Department of Homeland Security and CISA in particular, working with nonprofits like the Center for Internet Security, have done a tremendous job laying the groundwork for paving election security and election security response capabilities for the—each of those jurisdictions.

But there are other things. I mean, the state and local governments have very significantly limited expertise. They have limited resources, and those that have resource restrictions have been exacerbated by their response to corona and with a heightened threat

provided. So, I think this is an area where even a modest amount of funding, additional coordination, and policy directed from the Federal Government can have a disproportionately huge impact on better protecting the Nation.

Ms. NORTON. Thank you very much.

[Pause.]

Ms. NORTON. Madam Chair, I yield back.

Chairwoman MALONEY. Mr. Gosar?

Mr. GOSAR. Thank you, Madam——

Chairwoman MALONEY. Can staff tell me who I should call on if Mr. Gosar is not here?

Mr. GOSAR. I am here.

Chairwoman MALONEY. OK, good. Good. You are recognized.

Mr. GOSAR. Thank you, Chairwoman.

I am going to go back to you, Mr. Jaffer. I want to have you walk through. You made some—gave us some ideas of maybe this wouldn't be appropriate at the Presidential level. Can you walk us through that a little bit more?

Mr. JAFFER. Sure. So, Mr. Gosar, as you may know, there are four Senate-confirmed individuals today in the White House office—the Director of OMB, the U.S. Trade Rep, the head of the Office of National Drug Control Policy, and the head of the Office of Science and Technology Policy. Of those, two really focus on things that Congress and the President really share—trade, on one hand, and the power of the purse, OMB, right?

That's why those two have been very successful. The two that have been a lot less successful, ONDCP and OSTP, are largely less successful because they're not really a shared relationship. On this one, the challenge you have is that this is an area where the President feels strongly. This is a national security responsibility. Like this is like war-making in a lot of ways, right, and there are non-war making components.

The idea that any President—Democrat, Republican, Trump or otherwise—would be willing to give up a significant portion of authority I think is going to be a challenge. I think you're going to face significant challenge with the White House.

So, I think the better approach here is to find the path forward to work with the President, emphasize the importance. Look, the Congress did this here just in the last few years with the issue of interference in elections and the like, and they've prioritized it. They put statutory language in. They made it a responsibility of the National Security Council, and they required a coordinator to be appointed by the President.

That's a good example of the way that Congress was able to work with the White House on solving these problems rather than trying to get a Senate-confirmed individual with a large 75-person office.

Mr. GOSAR. Gotcha. So, Mike Rogers, you know, looking from the outside, you have been part of the matrix of Congress. Do you agree with anything that Mr. Jaffer has brought forward in that aspect?

Mr. ROGERS. I mean, I do. I had the same sensitivities about do we—do we really want to impose on a President some structure on national security within the National Security Council at the White House? And I wrestled with this a lot.

The reason I think I have come full circle on this is because I have seen it from the private sector side as well as being chairman of Intel when, candidly, I thought, no, we can do this. And this really isn't a Republican or a Democrat thing. The Bush Administration had an effort at this. The Obama Administration had an effort at this. The Trump administration took a very different take on how they wanted to do it. And my argument is none of it really worked to our advantage.

So, when you look at the series of challenges—and this is why. This is not, to me, some kind of semantic argument about should we or shouldn't we? Every major adversary—China, Russia, North Korea, Iran—there are others, but those are our main cyber adversaries—are ramping up the use of cyber because they know it has low consequence and high impact.

And if you look at Kim Jong Un, who said the thing that's going to keep me in charge are nuclear weapons and cybersecurity, offensive cybersecurity. So, he's investing in it. We know that the Chinese are spending billions of dollars. Matter of fact, they've announced they're going to spend $1 trillion to try to have a technological edge in quantum computing, 5G buildout, AI and AI research, including, by the way, cyber capability and data control.

So, they're looking—they're moving away from building large defensive military posture, and don't get me wrong, I'm for that. But what they're doing is trying to spend it targeting us. And my concern is if we keep doing it the same way, we are going to keep having the same response. And the IG response that we have now is basically I caught you for the last 12 months doing something wrong. I'll come see you in the next 12 months to see if you get it right.

That is not working. It will not work. We will get our lunch ate. I argue we are getting our lunch ate under that plan. Let's have some office that has that authority—and by the way, it takes it. You have some big personality DOD, NSA organizations. I'm not talking about the individual leaders. It's just they're big personalities to deal in this.

Nobody wants to listen to anybody. You have to have a committee to settle on the way forward. I think you need somebody to say I'm here to help you. We're going to get that piece right. We're going to fix this piece. We're going to coordinate resources. I'm going to reach over to NSA talent and who knows? Department of Agriculture figured this out last week. We're going to—we're going to include all that to help all.

We don't have that today in that really in that regard. And that, to me, has to change. If we could figure out another way, great, but I like this idea because it is a radical change and really puts it at the feet of an individual to fix this problem.

Mr. GOSAR. OK. Now I am going to finish with my last question to you. Then looking at the legislation as is, do you see any additions or subtractions to it that would keep it on a desired pathway, Mike?

Mr. ROGERS. I mean, and here is where I agree with Jamil. And he and I had these conversations often when we were working together in the Intelligence Committee. You want to make sure we're not propping a bureaucracy here. If everybody in this bureaucracy

gets to say no and everybody gets to sign off, we lose. It has to be smaller and more agile. I would worry about the body count.

Now maybe 75 is right. I don't know. Maybe it's 50. I don't know. But we need to make sure that it is agile enough in its strategic advice that it can actually do something. It needs to say, "Department X, you haven't performed. Not that I'm going to beat you with a stick or have you hauled before Congress, I'm going to help you get where you want to go." That's what this needs to be.

And you know, how it looks in text and legislation, as we all know, the devil is in those details. And I would flyspeck those to death. I'm for that. But if we don't do something pretty radical, we are already behind the eight ball.

And I'm talking even offensive policy, defensive policy, and then all these agencies that nobody even knows are out there working that have all this sensitive data that nobody thinks that loves them are great targets for cybersecurity. So, all of that I think—that's why you need somebody to pay attention to it every single day.

Mr. GOSAR. Thank you, Chairwoman. I yield back.

Chairwoman MALONEY. The time of the gentleman has expired. Chairman Connolly? Chairman Connolly is recognized.

Mr. CONNOLLY. Thank you, Madam Chairwoman, and thank you to our panel. Fascinating conversation.

And I don't know if Jim Langevin is still with us, but congratulations on the work of the Cyberspace Solarium Commission and this piece of legislation.

I want to go to practicality. I have spent all 12 years of my life in Congress focused on Federal IT, modernizing Federal IT. And you know, we spend $96 billion a year on IT at least, 80 percent of which is spent simply maintaining legacy systems, many of which cannot be encrypted. They can't be updated for 21st century cyber protection.

And I want to raise some concerns, and Mr. Daniel and Ms. Spaulding, you both kind of touched on it, as did Mr. Jaffer. Mr. Daniel, you were in the White House. We have a CIO in the White House. We have a CTO in the White House. We have a Chief Information Security Officer in the White House, and we have the Office of Science and Technology Adviser. All right?

All four of those offices right now, their responsibility in some measure for IT investments in the Federal Government, they're trying to modernize and to protect in terms of cyber. How will the creation of a cyber czar work with those other offices, and what authority will he or she have to help upgrade?

I mean, to upgrade a legacy system is going to cost at least billions of dollars multiple years. We have been trying for five years through the FITARA legislation that came out of our committee to exhort Federal agencies to make those investments. Will the cyber czar have superseding authority with respect to the kinds of investments that they make? Will he or she be required to coordinate with the CTO or the CIO, who are charged with setting certain sets of goals for the Federal Government that include cyber, but are not limited to cyber?

And I say all of this supportive of the attempt in the legislation, but worried about its execution, worried about overlap and what could go wrong with this in terms of coordination. And maybe I

could start with you, Mr. Daniel, given your experience. Presumably, those are real concerns. Do you share them, and what protections can we take in creating this position to avoid the inevitable conflict, bureaucratic conflict that could ensue?

Mr. DANIEL. Well, thank you, Congressman.

I certainly agree that this position would need to work very closely with the Federal CIO and the Federal CISO, and the way that I look at it is that you would want to have this position work with—those offices are designed to focus exclusively on the security of Federal networks, and that would be one, one element of a National Cyber Director's portfolio.

So, what you would want is you would want that position working very closely with those individuals to be able to highlight the threats to Federal networks across the broader policy space, to advocate on behalf of investments. Certainly one of the challenges that agencies have is that it is relatively easier to get operational money to keep the old stuff going, and it's much, much harder to get procurement money to actually upgrade things.

So, there's a structural problem in the budget process for how we—how we go about funding, you know, upgrades in IT. And that creates an incentive for agencies to keep old stuff around forever, which is inherently harder to secure.

What you would hope is that a National Cyber Director would also be able to help bring in expertise from the private sector to help the Federal Government do better. And then, last, to look at what are the structural changes we can make across the Federal Government? At some level, it's kind of ridiculous to expect the Denali Commission to really focus and be good at cybersecurity. We need to continue working on much more cross-agency support for cybersecurity so that we're not expecting every agency to be really, really good at their cybersecurity and instead think about the—you know, the economic principle of comparative advantage.

Mr. CONNOLLY. Well, I certainly agree with you that we would hope and expect that they would work closely together. But we are addressing a bill here. We are codifying a position. And I want to do more than hope that they coordinate. I want to make sure we get it right so that this person, this position can hit the ground running with defined responsibilities.

Because if we don't get this right, you're going to buildup bureaucratic resistance. So, instead of getting cooperation in cybersecurity, you actually get bureaucratic resistance. We certainly have seen that in CIOs. You mentioned bringing people in from the outside. We have done that with CIOs, and their lunch gets eaten.

You know, the bureaucracy just gangs up on them because they are outsiders. They are alien. They are grafted on. They are presuming to tell me what to do, and as a result, they fail. Not all of them, but you know, I——

Chairwoman MALONEY. The gentleman's time has expired, but the gentleman——

Mr. CONNOLLY [continuing]. Just wanted to share that concern. Thank you, Madam Chairman.

Chairwoman MALONEY. OK. The gentleman's time has expired, but the witness can respond to your question.

Mr. DANIEL. Well, thank you. Yes, I mean, I certainly agree that, you know, requiring some coordination with the Federal CIO and the Federal CISO, whose job it is to focus on Federal agency cybersecurity, you know, could be useful because it's those individuals who should really focus specifically on that task. And that—again, this would just be one aspect of something that a National Cyber Director would have to be concerned about.

Chairwoman MALONEY. Thank you. Mr. Massie is now recognized.

Mr. MASSIE. Thank you, Madam Chairwoman.

My first question, which I think should be everybody's first question, is what is the budget for this proposed Office of the National Cyber Director? And the second part of that question is, in addition to the 75 employees that are anticipated, how many—what percent of the money is going to go to contractors?

And anybody can answer that question, if there is an answer to it.

Mr. JAFFER. Well, Mr. Massie, it's Jamil Jaffer.

We don't know what the budget is. There's no authorization for appropriations in the bill, as far as I can tell, and we don't know what the committees will give it. That being said, the 75 FTE that are in there are a significant number. There is also authority to bring billets in from other parts of the Government, as well as to hire outside experts and the like. So, this number, 75, could actually grow beyond that.

Now to be fair, the legislation does just say "up to 75" for the full-time equivalent, but there's a lot of other room in there. And depending on what the various committees of jurisdiction appropriate and authorize, that may make a big difference, sir.

Mr. MASSIE. OK. That is a question I would like to get an answer to. Let me go on to my next question. This is for Ms. Spaulding.

You were on the commission that recommended this position. Is that correct, Ms. Spaulding?

Ms. SPAULDING. That's correct, yes.

Mr. MASSIE. OK. Was there an advocate for civil liberties and privacy on that commission, and if so, why is there not in this proposed legislation? I know you probably didn't write the legislation, but there is two Deputy Directors, but I don't see a Deputy Director for Civil Liberties or an advocate for privacy in here. Should there be one, and was that discussed in the commission?

Ms. SPAULDING. So, it's an excellent question, Congressman, and I have a long record of being an advocate for civil liberties and for privacy throughout my career. I think a number of us on the commission came to the table with those sensitivities and those equities very much in mind. There was no specific person designated for that, but a number of us, as I say, brought those sensitivities to the discussion.

And I think, you know, certainly privacy is one of the values and interests that cybersecurity is very much intended to protect. So, I think in many respects privacy is very much built into the efforts to strengthen our cybersecurity. But there are times in which the way in which you approach security issues may have implications in other contexts for privacy and civil liberties, and I think your point is very well taken.

And I think there ought to be an emphasis. I'm not sure a Director specifically for that, but certainly, when I was at the Department of Homeland Security as the Under Secretary for what is now CISA, I valued very highly having a specific individual and staff focused on privacy and civil liberties issues, as did the Department as a whole, and found their input and insights extremely important and valuable.

Mr. MASSIE. Well, I would like to see that, if we create this office, defined legislatively because there always seems to be a bias in the other direction. So, I think we need an advocate there. Thank you for being one.

Mr. Jaffer, what does it mean to have a list of trusted vendors when those vendors are putting backdoors intentionally into their hardware and software? How can you have a secure cyber system in the Government when we were actually even sometimes encouraging those vendors to put backdoors in?

Mr. JAFFER. No, I think it's an important question that you raise, Congressman Massie. At the end of the day, you know, we have legislation that permits the Government to obtain certain access to telecommunication systems, the Communications Assistance for Law Enforcement Act. That's typically the way in which law enforcement gets access to telecoms.

Now if we're talking about other systems, that's a harder question. More often than not, what typically happens in Government is, is the Government will come to a provider with a court order, either from the Foreign Intelligence Surveillance Court or from a Federal court or a subpoena authorized by Congress to get access. It's not typically happening in a cooperative manner. Typically, it's through some sort of legal process because the companies have learned that it's important to have that kind of process that if they ever get—if it comes out or they're sued, they have the protection of the law to help protect them.

So, that's typically how we see it happening. There is usually a judge involved. If not, some sort of administrative process that Congress oversees, sir.

Mr. MASSIE. OK. Well, I think there is a little bit of an oxymoron of creating a list of trusted vendors and then asking them to put backdoors in their products. So, I am concerned about that.

My final question is, what is the real responsibility of the Government to provide security for a company like Sony, who has over 8 trillion yen in revenue every year? And yes, Mr. Jaffer?

Chairwoman MALONEY. The gentleman's time has expired. The gentleman may answer the question.

Mr. JAFFER. Yes. So, it's a great question, Congressman Massie. You know, one of the challenges we have is that today in our country, we expect every company, whether it's a large Sony, the JPMorgan Chase, or the small mom-and-pop bake shop, we expect every single one of those companies and all that part of American small business that run our economy and that are the real engines of innovation, we expect all of them to defend themselves against nation-sanctioned actors in Russia, China, Iran, North Korea that have virtually unlimited human and monetary resources to throw at this problem. It's an unwinnable battle.

We've got to get those companies to come together with one another to create a collective defense structure with multiple industries working with one another, and the Government, frankly, takes all this intelligence it collects and provides it back to industry in an actual form to help them defend themselves. If we're going to put them on the front lines, we owe them better, and we're not doing that right now, sir.

Mr. YORAN. Well, if I can interrupt here? I think that there is maybe a misperception being created here. I don't think they're dealing with sophisticated adversaries. Many of these companies are falling victim through simple negligence. They're not applying a standard of care with their system, and I think the line of questioning is important.

And why I think it's important to have this Cyber Director position is to balance the equities of law enforcement where there are proposals, sponsored proposals to create backdoors and weakness, and weaken the encryption in commercial products. There are intelligence gain/loss decisions that are made on a daily basis. There are law enforcement considerations in creating norms of behavior and interactional norms of behavior here.

And all of these things are being done without having a national policy thought through at the White House level that can balance and consider all of these different equities. It's sort of each department and agency off and running on their own in a fairly uncoordinated fashion.

Mr. MASSIE. Thank you, Madam Chairwoman, I yield back.

Chairwoman MALONEY. Representative Raskin is now recognized.

Mr. RASKIN. Thank you, Madam Chair. And I want to salute our colleagues Mr. Langevin and Mr. Gallagher for an extremely compelling presentation and for their hard bipartisan work on this legislation.

I am kind of puzzled by the history of this, and I was hoping that Mr. Rogers might start off by clarifying some things for me. We got hit in 2014 with the massive cyber breach at OPM by China, and that caused massive damage to our country.

In 2016, we experienced a sweeping and systematic cyber-attack on our election by Vladimir Putin's Internet Research Agency that caused incalculable damage to our democracy and to social cohesion in the United States of America.

Now, of course, in 2020, we have been caught totally unaware and seemingly unprepared for the coronavirus epidemic, which was denied and dismissed and trivialized and wrapped in magical thinking. And now we lead the world in case count and death count. While our European allies totally have the virus on the run, we are spiraling out of control.

So, if everybody is responsible for something, nobody is responsible. And it seems overwhelmingly compelling and clear to me that the purpose of this legislation is absolutely right. We need someone who is coordinating our cyber defenses at a time when all of these weaknesses and vulnerabilities have been repeatedly demonstrated by different attacks.

So, I guess my first question for you, Mr. Rogers, is why has it taken us so long to get to this point? What has slowed us down?

Mr. ROGERS. Oh, boy, that may be the million-dollar question, Congressman. When we went back and looked—think about this. The first time that China was publicly named as this increased actor in cyber intellectual property theft, even though we had known it was going on for years, was 2010.

Why? Because the Bush Administration had said, oh, we can't. No way. Not disclosing it yet. Even the early days of the Obama Administration, they said it's too early. We've got to figure out a way around it. So, Dutch Ruppersberger and I at the time, we gave a pretty forceful argument about making this public. So, we've only been talking about it publicly for 10 years, and I think the public is slowly coming around.

Now there was a recent Gallup Poll I think last week that said 81 percent of Americans believe that there will be a cyber-attack of significance on the United States. We didn't have anything like that in 2010. People thought we were crazy. I mean, they didn't even understand what we were talking about. So, public opinion has been slow to catch up.

I think we're in a very different place now. Public opinion is probably more with us now than it's ever been to try to defeat this thing. And remember, there is no system out there that is completely impenetrable, none. I mean, if it's connected to the Internet, you are vulnerable.

So, any time we break up our efforts to try to do this, meaning if the NSA has one mission set and the FBI has another, and they're not talking to each other, guess what? That scene means somebody is going to win, and that happens in private sector, it happens in local and state government, and it happens in the Federal Government.

And if you look at what the Chinese were able to do, this was very typical in the OMB breach, a typical espionage activity where they're going to take I think it was—I forget what the number is now—17 million records of SF–86, right, the very sensitive information to get a clearance. I got a letter saying mine was breached. All of that information was taken back, and think about what they're doing now with their ability through AI algorithms to collate that data and find out people that they're interested in spying on.

Either you're with the Government and have a classification, or you've moved on to the defense realm and have a classification. That was, unfortunately, a brilliant government espionage activity. So, we have to—we really have to change the way we think about these threats. They are looking at——

Mr. RASKIN. Can I followup with you just for 1 second?

Mr. ROGERS. Yes.

Mr. RASKIN. I have got time for maybe one more question. I mean, what is terrifying to me is that our failed response to the coronavirus pandemic has exposed a lot of vulnerabilities to foreign governments that may mean to do us harm, and they may figure we don't have the governmental preparedness, we don't have the social cohesion to respond to a massive threat on our infrastructure.

So, if you would just put this in a geopolitical competitive context, what is the imperative here to act now?

Mr. ROGERS. Well, I think that's two conversations. One is on the supply chain and security of the supply chain.

Chairwoman MALONEY. The gentleman's time has expired, but the witness may answer the question. Answer the question.

Mr. ROGERS. Whoops. Security is, I think, a very important discussion Congress is going to have to weigh in on. I wouldn't kill international trade, but I would protect our ability to surge on critical items.

Second, the other reason on this is that these nation-states, our big adversaries, have refocused their efforts. Remember the quote I used from Gerasimov in Russia? They've realized I don't need to build an aircraft carrier. I'm going to invest in cyber operations. If I can shut down their electricity or I can cause distrust of the American people with their government, we win. It has an outsized impact on what they're trying to do.

And all of them have stepped up their game. Russia, China, Iran, North Korea, others. That's why, to me, this is so important.

And candidly, we're in a cyber war today. Most people don't realize it. And folks who say it's not really a war, I don't—I disagree. They are causing destruction, disruption, and adding chaos. I don't know what else you call it. And we need to act that way, and I think we ought to have one focus on this so that we can coordinate all the good activities around the Government and focus—don't expand Government—focus it on the solution.

Mr. RASKIN. Thank you, Madam Chair.

Ms. SPAULDING. If I could just very quickly? The other lesson from the pandemic, of course, is the—is what happens if we don't have strong coordination and a coherent response in a crisis.

Chairwoman MALONEY. Thank you. Mr. Grothman? Mr. Grothman?

[Pause.]

Chairwoman MALONEY. Congressman Grothman, are you there?

Mr. GROTHMAN. Can you hear me? Yep, can you hear me? Can you hear me?

Chairwoman MALONEY. Yes. Yes.

[Pause.]

Chairwoman MALONEY. Unmute. Unmute. Can you unmute?

Mr. GROTHMAN. Can you hear me now?

Chairwoman MALONEY. I can hear you now.

Mr. GROTHMAN. OK. OK, I have a question here. First question is when we confront China or Russia about this, what do they say? You know, what is their response when we bring this up to them?

Mr. DANIEL. Well, Congressman, I can—having engaged them on this topic directly, I can tell you that most of the time, of course, they deny it. And they say that——

Mr. GROTHMAN. And we never catch them red-handed, either them or China?

Mr. DANIEL. Oh, of course. And you know, naturally, they deny it, and they will—at most, they would say it must be—we must be mistaken, and could we please provide them all of the detailed evidence for how we, you know, found that out so we could expose our intelligence methods to them so they could prevent us from doing it in the future. And you know, then at most they might say it's

some sort of rogue element that they weren't really in control of, and it wasn't really them.

They, of course, never will accept responsibility for doing that. That said, we have engaged with them in other ways to try to push forward and push back on their activity.

Mr. GROTHMAN. That is fine. Now I have a question for Ms. Spaulding. We asked this earlier, how a major cyber incident proceeds through the Government. I want to kind of expand a little bit on that. I want to know step by step, based on your experience, what happens when an incident is reported by either the private sector or a Government agency?

You know, what happens from discovery to response? Kind of walk me through the U.S. Cyber Command authorities that are triggered, and how would this change if we got a National Cyber Director?

Ms. SPAULDING. Thank you, Congressman.

As Michael Daniel explained, some of it depends on how this information first comes into the Government. So, it might come in first to the NCCIC, which is the National Cybersecurity Communications Integration Center, or the ops center, at the Department of Homeland Security. We would often get reports, usually from private sector companies, that they are seeing malicious activity. But it's equally likely to come into the FBI, for example.

And then the players, the DHS, the CISA, the Bureau—FBI—and usually the NSA would get on the phone together, though there are often reps sitting at the ops center at DHS. But the information would be shared.

And then a decision has to be made very quickly, depending on the nature of the event and if the Government is going to step in, on what is most important. Do we go first—and sometimes you will try as you can to do these at the same time, but you often have to prioritize. Are we going to try to go in and mitigate the problem, address the malicious cyber activity and the damage that's being done to that private sector business, for example? Or are we going to put our priority on getting law enforcement in there to do attribution, to figure out who's behind this?

And both of those are legitimate equities, but sometimes they can't both happen at once. So, conversations ensue to determine how to prioritize that.

The advantage that a National Cyber Director can bring to bear on this, obviously, is to deconflict those competing equities quickly. Time is of the essence to make sure that we can get in there and do what is most important first, even as we're trying to accomplish all of the other equities.

Mr. GROTHMAN. Thank you. Next question.

One of you mentioned, you know, you talked about Russia and China, North Korea and Iran, and then you said "other countries," one of you. Can you expand what other countries we have to worry about other than those four?

Does anybody want to take it?

Mr. ROGERS. Yes, I mean, I can take it, take a shot at that.

Mr. GROTHMAN. One of you said there was more than the four, so I just ask.

Mr. ROGERS. There are—there are countries who are engaged in ramping up their cyber capabilities that might not be friendly to the United States. I think Belarus comes to mind. Leaked nation-state capability from Russia into former Eastern Bloc criminal organizations perform like a state. They may not look like a state, but they perform like a state when it comes in cyberspace.

And there are other countries that are probably best not discussed in an open forum that some aren't very friendly countries, and you would——

Mr. GROTHMAN. OK. We won't discuss them, if you don't want to discuss them.

Next question. One of you said they were involved in this George Floyd incident, that some of our enemies were involved in that. Could you expand on that?

Mr. JAFFER. It was me, Congressman. What we've seen is we've seen some reporting that the Chinese—you know, you saw the Chinese Foreign Ministry from the platform in open setting refer to the plight of black Americans. Obviously, we know the Chinese don't actually care about black Americans. They are interning a million Muslims in the Xinjiang Province. So, we know that these people actually don't care. It's an effort to influence our own—our own discussions here in the United States.

We know what they're doing overtly. We have seen them operate covertly in very similar related spaces, and we have every reason to believe that both they and the Russians, having watched the Russians do it successfully in our 2016 elections, are involved in this effort. They're essentially gaslighting these debates, playing both sides——

Mr. GROTHMAN. Could you give us a specific example? Could you give us a specific example?

Mr. JAFFER. So, I don't—I don't know that we've seen sort of, you know, point-on-point examples, but I would bet dime to dollars that in the next six months we will see very specific examples coming out of Facebook, Twitter, and the like. I can't prove it to you right now today, sir, but I'd put my—I'd put my life on it.

Mr. GROTHMAN. OK.

Chairwoman MALONEY. The gentleman's time has expired, and now——

Mr. GROTHMAN. Thank you much.

Chairwoman MALONEY.—Congressman Rouda is recognized.

Mr. ROUDA. Madam Chair, did you recognize me?

Chairwoman MALONEY. Yes, I did.

Mr. ROUDA. Thank you, too. I apologize. I did not hear you. But thank you, Madam Chairwoman, for convening this hearing, and I would also like to thank the commission for their detailed report.

And I want to focus on one key area that had been previously discussed, but I would like to dig in a little bit deeper, and it is about the loss of hundreds of billions of dollars in intellectual property theft to nation-state sponsored cyber espionage. Obviously, the chief country responsible for that cyber IP theft has been China.

We know China actively works with both state-owned and civilian corporations and universities to steal IP from foreign sources, including the United States. And according to a 2018 report released by the United States Trade Representative, theft of U.S. in-

tellectual property by China cost our economy up to $600 billion a year. Let me repeat that, $600 billion a year.

The long-term damage of these losses, however, simply cannot be fully quantified. So, Ms. Spaulding, let me turn to you first. In developing your recommendations for the National Cyber Director, did the commission structure the role and its office with this persistent problem in mind, and can you provide any specifics as to how the Director would address this issue?

Ms. SPAULDING. Yes, absolutely, we did. And the situation that you've described really is addressed by a number of recommendations in the report. The private sector and the Government both have a critical role to play in stopping this theft of intellectual property, and it requires a true collaboration.

We need to—we are the ones in Government that have the national technical means and the exquisite intelligence capabilities to collect information about what nation-states like China are engaged in and the kind of tactics and techniques that they're using, as does the private sector research community. The private sector businesses that are—that are developing this intellectual property are in the best position to defend their networks, armed with information from the Government.

So, we have a number of recommendations to make sure that we are—that the Government is obligated to get that information to those private sector companies, and the National Cyber Director will have a key role in making sure that that's happening. That has to be part of the metrics, right, that is evaluated by this National Cyber Director.

We need to have proactive plans, strategies for addressing this, and that planning capability across the interagency has been lacking. That is another key role for this National Cyber Director, largely using the joint planning organization at CISA.

Mr. ROUDA. Thank you. Chairman Rogers, you have talked about how long America has been struggling to protect its IP. Virtually every administration deals with this issue, has dealt with this issue, and candidly, we have not been successful. Do you envision this bill would finally allow us to successfully defend and protect our IP?

Mr. ROGERS. I think it would put us in a better position. I would hate to say "finally." I think this is something we're going to have to continue to invent a better way to defend ourselves as we get into 5G and what that means for pushing what we use to defend the core out to the edge of a 5G network, quantum, AI. All of that is going to change the way we look at security.

So, I think it gives us the best possibility to take all these new challenges and bring everyone in the Federal enterprise up to snuff. Everybody keeps talking about that one incident. We want to prevent that incident.

And here is the other piece, and I agree with Ms. Spaulding on everything she said. I would argue if you look at the recent level of arrests by the FBI for Chinese espionage in the United States, the number—the interesting high level of taskings for those assets, those spies targeting America or American enterprise, is to steal credentials to get around firewalls so they can steal more information.

It's really interesting. The nature of espionage is changing dramatically. They don't want you to just steal the secrets. They figure that's probably maybe too hard to do. They want you to steal the guy next to you's credentials to get into the network so that they can be passed back for a more sophisticated penetration of your network. That's what makes this——

Mr. ROUDA. Thank you.

Mr. ROGERS. Yes, this is what really makes it hard to put your arms around.

Mr. ROUDA. One last question for Mr. Jaffer. Is there a concern that if we, as a country, are unsuccessful at providing appropriate protection that we could see companies move their IP and businesses to foreign countries that do provide protection?

Mr. JAFFER. Thank you, Congressman.

Look, I think that there are so many benefits to being an American company, whether it's our labor laws or our tax policies or our investment base, that it's unlikely to see a tremendous flood of intellectual property that comes out of the United States. That being said, we have to recognize this is the core of our innovation base in this country. We have moved to an innovation economy.

If we allow it to walk out the backdoor, whether to China or anywhere else, we are undermining the capability of our economy to survive and make it to the next stage. So, even as we think about rehoming American technology and bringing some of those jobs back here and starting to build stuff here, we've got to protect that core thing that makes America so productive as a country, which is that innovation, that ability to invent and reinvent and modify ourselves over time. If that walks out the backdoor, we've got nothing.

Mr. ROUDA. Thank you. I yield back, Chairwoman.

Chairwoman MALONEY. The gentleman's time has expired. Representative Ro Khanna is now recognized. Ro Khanna, are you with us?

Mr. KHANNA. Yes, I am. Thank you, Madam Chair.

I appreciate and want to just thank Representative Langevin and Representative Gallagher for their extraordinary work in helping come up with such a detailed proposal and their work with the commission on a bipartisan basis. I know in particular Representative Langevin has been working on this for many, many years, and this is a passion of his that he has talked about often. So, I am glad to see it come to fruition.

Let me ask the panel, are there additional authorities that you think the National Cyber Director should have?

Mr. DANIEL. Well, certainly, Representative, I think that it is important that as we structure this position that we make sure that it not be just restricted to looking at network defense. It's got to be able to have the full suite of capabilities that the Federal Government can bring to bear.

So, including military operations and intelligence and the law enforcement and all the way across the board. We cannot just restrict this position to looking at the kinds of things that CISA already does. Chris Krebs does not need another boss. You know, he's got one in the Secretary of Homeland Security. This really has to be

able to look across the entire Federal Government and all of the tools of national power that we have.

Ms. SPAULDING. And if I might, Congressman? I totally agree with Michael on this point, and I think the distinction here is between having visibility. The National Cyber Director has to have visibility across the entire Government cybersecurity activities in order to make sure and deconflict even between offensive and defensive operations.

That's different from giving the National Cyber Director directive authority, right? You don't want law enforcement activities being directed out of the White House, for example.

Mr. KHANNA. No.

Ms. SPAULDING. And you don't want this Director either in the way of warfighting plans or daily intelligence collection, those kinds of activities. But it's critical that they not be excluded from the meetings and the conversations at the White House where these offensive, for example, activities are being discussed and that they have visibility.

Because they need to be able to deconflict. They can never deconflict in this way, and I'll give you an example. Let's say our banks are fending off—they're in the middle of fending off lots of malicious activity from North Korea trying to steal money from their system. That might not be—in the midst of that crisis might not be the best time to ask the banks to impose sanctions, to implement sanctions to implement—new sanctions against Iran because we know Iran retaliated in the past against our banks with malicious cyber activity.

So, that kind of deconfliction is something that the National Cyber Director needs to be at the table to help with.

Mr. KHANNA. Right. Thank you. And are there additional cybersecurity recommendations that you think we should be considering, including for many that the Solarium Commission report came up with?

Mr. JAFFER. Yes, I think, Congressman, there are a couple of really important ones, in particular the ones that revolve around collective defense like establishing a joint collaborative environment where both NSA and DHS can come together and share classified and unclassified information and then share that in real time at meetings with industry. That was something we've been talking about forever.

Information sharing isn't enough, though. You've got to collaborate in real time. That's something that the commission was very focused on, too. I think that part of the report is really critical. I think more work could be done there, and the commission has got some great recommendations in that space, as well as on continuity of the economy and a variety of other areas. The critical infrastructure entities also, I think some good recommendations there from the commission.

Mr. ROGERS. I 100 percent agree. Just a couple of things that we just haven't talked about. The interim, the brush-cleaning that we can do to make us more competitive would be huge. Congress needs to pay attention. Chairman Pai has done the spectrum clearing. Outrageously important if we're going to compete in 5G and push back on Chinese expansion there.

Rip and replace. We have lots of gear around the country, and I know people want to beat on them for it. It was legal at one point. There's lots of great effort in Congress today about how do we get rid of that? It does two things. Helps our own infrastructure ecosystem, people who are trusted vendors, to do that, No. 1. And No. 2, it gets out Huawei gear much, much quicker.

Those are kinds of things that we can do almost immediately that are in the process that you're all dealing with now that would have a huge advantage for us, putting us in a competitive position to do all the things that my other panelists just talked about.

Mr. YORAN. As Suzanne Spaulding said, each organization, each enterprise, each company is in the best position to defend themselves. They understand which of their systems are most critical and represent the greatest risk.

There are opportunities, and I think some of the recommendations of the commission, things like increasing transparency, having the interpretation by the SEC requiring an attestation from public company CEOs not on the level of security they have, but just the fact that they've looked at their cyber risk and that they are adequately or proactively managing cyber risk associated with their business.

When you get things like that in place, you will have—you will increase the level of hygiene, increase the level of attention. It will increase each enterprise's ability to defend themselves, and the amount of noise and the amount of economic loss will go way down. It's probably the single greatest move that we can do as a nation to improve our cyber resilience and preparedness.

Mr. KHANNA. I appreciate all of your expert testimony. I just want to thank again Representative Langevin and Gallagher. Representative Gallagher had come out to my district, and I remember at Stanford they were talking about a "cyber Pearl Harbor" as the big fear. So, many of the companies have talked about how we shouldn't have every company in this country required to have basically private armies to safeguard ourselves. We need a national response.

So, I certainly will be supporting this legislation and appreciate everyone who helped put it together.

Chairwoman MALONEY. Thank you. And Representative Sarbanes, you are recognized. Representative John Sarbanes?

Mr. SARBANES. Thanks very much, Madam Chair. Can you hear me?

Chairwoman MALONEY. Yes.

Mr. SARBANES. Excellent. Well, I appreciate the panel. I certainly want to thank my colleagues, Congressman Langevin and Congressman Gallagher, not just for their testimony this morning, but for their efforts on this proposal, which I support very strongly.

I want to welcome back Chairman Rogers and thank the rest of the panelists for their testimony.

Obviously, one key responsibility of the National Cyber Director is establishing and implementing a National Cyber Strategy. In 2018, the Trump administration released a National Cyber Strategy that aims to "integrate cyber into all elements of national power."

Chairman Rogers, could you speak to how the 2018 National Cyber Strategy has been successful or not successful in that goal, and how would the National Cyber Strategy that is required by this bill that we are talking about today be different from that? So, could you maybe compare and contrast those a little bit for us?

Mr. ROGERS. I think what that strategy was meant to do in 2018 for sure was bring us to a better place about coordination and understanding that our adversaries are using all the nation-state power they can bring to bear. So, diplomacy, military defense, intelligence, cyber, and kind of using that capability—oh, and economic. The most—I argue probably the most important.

So, we know that China steals economic data to try to influence its trade negotiations as an example. So, they're using cyber and intelligence as a way to influence all of those pressure points that a government has to bring to bear on a country, and it's my understanding that that 2018 rule was to say, OK, we're finally getting to understand that it is multi-domain, right?

We tend to separate diplomacy and the economy to a great degree in this country. So, how do we try not to do that? How do we have everybody rowing the boat in the same direction, understanding our adversaries are using that against us? I think that's what they were trying to do.

I think it's still a work in progress. And a part of that, by the way, we debated when I was chairman, and prior to me being chairman—and Mr. Langevin can comment on this as well, and certainly, Jamil was part of those discussions as well—about what is offensive cyber? Are we allowed to protect ourselves if we know they're going to shoot at us in cyberspace?

And I have seen lots of folks say we've solved that question over the last 15 years. I don't believe we have yet today solved that question. We had a piecemeal policy, and I think that 2018 policy was trying to say is we're going to, again, use all the nation-state groups of power that I know our adversaries are using and then try to understand what tools in our toolkit do we have?

And I'm not saying every cyber-attack should be—you know, we should have another cyber-attack back. I'm not saying that at all. But we really didn't, and I don't think still to this day have, a good definition of what we can do to prevent, you know?

And I've heard the terms go through the years. Now we call it aggressive defense. OK, whatever we want to call it, but we need to understand what that is.

Mr. SARBANES. Yes. I'm interpreting you to say that the administration's strategy released back in 1918 was heading in the direction that now this Cyber Director with the strategy required under 7331 takes to a new and better and more coordinated and more structural place.

One key difference of the role as envisioned by this bill is that the position would be empowered with new statutory authority to monitor implementation across the Federal Government in terms of strategy, which would include recommending changes to OMB regarding agency organization, personnel, resource allocation. I think that makes a lot of sense. As well as certifying that the annual budget proposal for each Federal department or agency is con-

sistent with the strategy. Again, that makes a lot of sense in terms of coordination.

Mr. Daniel, I understand you spent 17 years at OMB before assuming the cybersecurity coordinator role. Do you think it is important for the National Cyber Director to have this statutory authority, and how do you think the relationship with OMB would actually work in practice?

Mr. DANIEL. Yes, sir. Thank you.

I think that it is critically important that the office have a very good understanding of the budget and be empowered to actually work in that budget process. A former OMB Director once said, "Policy without resources is a hallucination." So, you know, clearly, the ability to influence and shape how we allocate resources is absolutely critically important.

As a practical matter, I think what you would want to see is very close collaboration between any staff associated with this office and the program, the line program examiners at OMB. OMB is at its most effective when it works very closely across the entire White House complex with NSC, with OSTP, with ONDCP, any of those White House elements, to make sure that the budgets support the President's policies.

So, you might even imagine a situation where you have program examiners from OMB detailed over to this office to help provide that connectivity and that reach-back, and you would want them working hand-in-glove with each other to shape that President's budget. So, that's why I think having this lever of the—having a lever like that statutory authority that's in 7331 would be very, very helpful to the position.

Mr. SARBANES. Thanks very much. I yield back.

Chairwoman MALONEY. The gentleman's time has expired. I now yield to Katie Porter. Representative Porter?

Ms. PORTER. Hi. Thank you, Madam Chair.

Under H.R. 7331, the first duty listed for the National Cyber Director is serving as the principal adviser to the President on cybersecurity strategy and policy. Mr. Daniel, having essentially worked to achieve many of those functions yourself, can you give me any concrete examples of how having a principal cybersecurity adviser was essential to the President's work and why it is important to formalize that role, as proposed in the bill?

Mr. DANIEL. Yes, thank you, Representative Porter.

I think that when you look at an issue like cybersecurity that is so cross-cutting, that affects so many different policy areas, from national security policy to our economic policy, you want the President to have an adviser who focuses on this issue as part of her time. You know, the main thing that they focus on every day because it pervades so many of our policy issues now.

So, if you're trying to decide what the U.S. policy should be on everything from 5G to relations with China to how we're dealing with the Middle East, cyber shoots through all of those things. And so you want to be able to have the President be able to draw upon somebody with expertise in those areas that can bring that cyber perspective to those issues so that you make a decision knowing what the effects on our cybersecurity might be, for good or for ill.

Sometimes you're going to make decisions that maybe have a negative effect on that for a greater positive gain somewhere else, but you do that with full knowledge and not by accident. And that's why it's so critically important that a senior adviser in the White House focus on this issue, just given its breadth across so many different policy areas now.

Ms. PORTER. Yes, I appreciate your flagging the importance of expertise in this cybersecurity role, and I want to ask some more questions about how Senate confirmation would help us assure that.

Mr. Jaffer, do you remember anyone who the President appointed as one of his cybersecurity advisers when he took office in 2017?

Mr. JAFFER. Yes, sure. Rob Joyce, obviously, was an excellent appointee, and Tom Bossert, who Rob worked with, was also an excellent appointee. Both very good on cyber.

Ms. PORTER. Yes, both very, very good, and I would agree with you about the importance of expertise. I think the President also appointed Mr. Giuliani, and I think like so many of us—and I think we are seeing this during work from home—technology is frustrating and hard, and we are all struggling to get our level of expertise up to where it needs to be to be cybersecure.

So, I completely relate to the fact that Mr. Giuliani, after being appointed one of the cybersecurity advisers, got frustrated with his iPhone and went into a public Apple store in San Francisco within a month of being appointed a principal cybersecurity adviser because he had entered his password wrong 10 times and was locked out of his iPhone. I think this really indicates the gap between the rest of us, who are trying to do our very level best, and the need for a true expert at the very top of this.

Would you agree with that?

Mr. JAFFER. I completely agree. In fact, we're working on a program funded by the Hewlett Foundation at George Mason, where we're bringing technologists from around the country to D.C. to train them on how policy works so we can get more technologists talking to you about the problems that you have and challenges that you face in policymaking. I mean giving you real advice from people who actually do the work, the data scientists, the coders, and the like.

So, you're exactly right. Having real—there's no substitute for having real experts in this area.

Ms. PORTER. Yes, thank you so much.

Ms. Spaulding, I wanted to turn to you briefly and ask you, I know that H.R. 7331 would require the National Cyber Director position to be Senate-confirmed. Can you explain why the Solarium Commission made that recommendation, and whether you think—or how you would respond to concerns that that has the potential to create distrust between the President and the National Cyber Director, or do you think that concern is misplaced?

Ms. SPAULDING. Thank you, Congresswoman.

Yes, you know, with respect to that latter question about the potential impact on trust in the National Cyber Director within the White House, I would point out that there are lots of Senate-confirmed, a number of Senate-confirmed positions within the White

House, including the OMB Director. And I don't think anybody questions really the level of trust there with respect to that OMB Director.

So, I don't think—I do think that concern is misplaced. And we talked a lot about whether—the pros and cons of having this person Senate-confirmed, and ultimately, the consensus was, yes, we should recommend Senate confirmation.

I think it's critically important that Congress have effective oversight. And given the decentralized nature of cybersecurity, if Congress doesn't have really the ability to hold someone accountable and really to have somebody that they can turn to get a coordinated and coherent picture of what's happening, it's going to be very hard for Congress to do effective oversight. So, I think that's important. That Senate confirmation gives Congress a greater ability to conduct oversight of those activities.

Ms. PORTER. I really appreciate it, Ms. Spaulding, and I think it's important to note that that's bipartisan oversight that Congress would be conducting. So, unfortunately, my time has expired. So, I yield back.

But thank you so much.

Chairwoman MALONEY. Thank you. The gentlelady yields back.

Representative Comer, would you like to ask an additional question or make a closing comment? Representative Comer?

Mr. COMER. I think that just to wrap it up, I want to thank the witnesses again for their testimony. This is certainly an issue that is bipartisan that we all care about when we are talking about cybersecurity. But the question that many of my colleagues have is whether we want to create another Government bureaucracy and what is the total cost going to be? And how is this bureaucracy going to be able to work with the administration, whichever administration that would be moving forward?

So, I do think this was very helpful. I appreciate the conversation, appreciate the questions.

Again, Madam Chair, with all due respect, I hope that we can focus on China. There is a huge demand across America to hold China accountable for not just COVID–19, but also the cybersecurity breaches that are at the hands of China. So, again, I would encourage future hearing with a sole focus on investigating China and determining a path forward to hold them accountable for their violations.

But again, thank you for the hearing today, and with that, I yield back.

Chairwoman MALONEY. Thank you.

Because this August marks 100 years of women's suffrage, I want to close with one final question. Mr. Yoran, your written testimony addresses the lack of diversity in the cybersecurity sector and how it contributes to the overall shortage of talent in the cybersecurity work force.

For example, you point out that women make up just 14 percent of the cybersecurity work force in North America. You say, "The

Nation needs a bold, new cyber work force strategy that develops and advances the ranks of people from all walks of life."

How would the Federal Government—my question is, how would the Federal Government's effort to promote diversity in the cyber work force benefit the private sector? And I mean more minorities, gender diversity. So, how would it benefit the private sector, more diversity?

Mr. YORAN. Well, the most important thing when it comes to cybersecurity is recognizing the fact that what we're doing isn't getting the job done. We can't just have a continuation of the same mode of thinking, the same solutions, the same approach that we've used in years past to deal with the threats that continue to evolve. And as we deploy new technologies, they have new exposures and new vulnerabilities.

So, we need experts to come from diverse backgrounds, and that certainly means people that are trained in the discipline of cyber, but diversity of thinking. People with diverse backgrounds—from minorities and other groups which are underrepresented in the cyber field and in the cyber domain.

I think the Government has an opportunity and a responsibility to help promote the diversity of thinking and the diversity of talent available to the private sector. It will help us innovate faster, think outside the box, and outmaneuver our adversaries. So, there's a series of programs. Love to have a conversation with you about it in perhaps a followup.

Chairwoman MALONEY. Thank you. Ms. Spaulding, do you believe such an effort would advance innovation and give us a competitive edge globally?

Ms. SPAULDING. Absolutely, Chairman. I couldn't agree more with Amit's comments. And of course, the commission has a series of recommendations on building that cyber work force, including diversity.

And I would say just from a very basic perspective from my time at DHS, and we see it, we have an urgent need to build the number of cyber-talented people that we bring—that we have available to come into the work force. We cannot afford to leave any part of our population on the sidelines of this effort.

Chairwoman MALONEY. Well, I agree with you. We can and must do more in this regard.

I truly want to thank all of my colleagues for their participation, particularly Congressmen Langevin and Gallagher for their leadership, and all of our witnesses for your passion and your knowledge and all the information you gave us today. The creation of a National Cyber Director is not something any of us take lightly. After what we have heard here today, I think it is clear this is something we cannot afford to delay.

I also want to thank all of my colleagues across the aisle particularly, for their questions and engagement. It is not every day that we can find areas of bipartisan consensus that—and we have it here. We have to agree on our national security, protecting our innovation, and protecting our people. So, I look forward to working

together to get this bill passed and on other items that were brought up today.

Without objection, all Members have five legislative days within which to submit additional written questions for the witnesses to the chair, which will be forwarded to the witnesses for their response. I ask our witnesses to please respond as promptly as you are able to.

And this hearing is adjourned. Thank you all.

[Whereupon, at 3:11 p.m., the committee was adjourned.]