S. HRG. 116–458

THE FINDINGS AND RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

AUGUST 4, 2020

Printed for the use of the Committee on Armed Services

Available via: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
56–585 PDF WASHINGTON : 2024

COMMITTEE ON ARMED SERVICES

JAMES M. INHOFE, Oklahoma, *Chairman*

ROGER F. WICKER, Mississippi	JACK REED, Rhode Island
DEB FISCHER, Nebraska	JEANNE SHAHEEN, New Hampshire
TOM COTTON, Arkansas	KIRSTEN E. GILLIBRAND, New York
MIKE ROUNDS, South Dakota	RICHARD BLUMENTHAL, Connecticut
JONI ERNST, Iowa	MAZIE K. HIRONO, Hawaii
THOM TILLIS, North Carolina	TIM KAINE, Virginia
DAN SULLIVAN, Alaska	ANGUS S. KING, Jr., Maine
DAVID PERDUE, Georgia	MARTIN HEINRICH, New Mexico
KEVIN CRAMER, North Dakota	ELIZABETH WARREN, Massachusetts
MARTHA MCSALLY, Arizona	GARY C. PETERS, Michigan
RICK SCOTT, Florida	JOE MANCHIN III, West Virginia
MARSHA BLACKBURN, Tennessee	TAMMY DUCKWORTH, Illinois
JOSH HAWLEY, Missouri	DOUG JONES, Alabama

JOHN BONSELL, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	JOE MANCHIN III, West Virginia
DAVID PERDUE, Georgia	KIRSTEN E. GILLIBRAND, New York
RICK SCOTT, Florida	RICHARD BLUMENTHAL, Connecticut
MARSHA BLACKBURN, Tennessee	MARTIN HEINRICH, New Mexico

CONTENTS

AUGUST 4, 2020

	Page
THE FINDINGS AND RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION	1

MEMBER STATEMENTS

Statement of Senator Mike Rounds	1
Statement of Senator Joe Manchin	3

WITNESS STATEMENTS

King, Senator Angus S., Jr., Co-Chair, Cyberspace Solarium Commission	5
Gallagher, Representative Michael J., Co-Chair, Cyberspace Solarium Commission	23
Inglis, Brigadier General John C., ANG (Ret.), Commissioner, Cyberspace Solarium Commission	25
Questions for the Record	38

THE FINDINGS AND RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION

TUESDAY, AUGUST 4, 2020

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:38 p.m. in room SD–106, Dirksen Senate Office Building, Senator Mike Rounds (Chairman of the Subcommittee) presiding.

Members present: Senators Rounds, Wicker, Perdue, Scott, Blackburn, Gillibrand, Blumenthal, King, and Manchin.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. Well, good afternoon.

Senator Manchin, our Ranking Member, should be here shortly. He, unfortunately, had a meeting off the Hill.

Thank you, Senator Blumenthal, for being here. Senator Perdue, as well. We have a number of our other members who are joining us virtually today.

Today, the Cybersecurity Subcommittee welcomes, for the first time, colleagues to present the findings of the Cyberspace Solarium Commission: our friend Senator King, from Maine, and Representative Gallagher, from Wisconsin. They are joined by fellow Commissioner, retired Brigadier General John C. Inglis, Professor of Cybersecurity Studies at the U.S. Naval Academy, and former Deputy Director of the National Security Agency.

Welcome, to all. Thank you for coming to discuss this important topic at today's hearing.

I would like to extend my congratulations, as well, to Mike Gallagher and his wife, Anne, on the recent birth of their baby girl, Grace. Good luck on your greatest adventure yet and all the amazing moments yet to come associated with it.

I would also like to recognize former Senate Armed Services Committee (SASC) Policy Director Mark Montgomery, who serves—or who served as Executive Director of the Commission.

Section 1652 of the Fiscal Year 2019 National Defense Authorization Act (NDAA) established the Cyberspace Solarium Commission to study alternative strategies for defending the United States against malicious cyber activity and advancing its national interests in cyberspace. Among the strategies to be evaluated were cyber deterrents, persistent engagement, and compliance with international norms. The Commission has produced an impressive report that advocates a combination of all three: deterrence by de-

nial and rapid attribution, deliberate shaping of international norms through aggressive diplomacy, and continued persistent engagement of malicious cyber adversaries.

The Commission's report also presents a number of reforms, many in legislative format, for our deliberation. Of particular importance are the following recommendations: that the Department of Defense evaluate the size and capacity of the Cyber Mission Forces; that the Department of Defense takes an expanded role in exercises and planning relevant to protection against cyberattacks of significant consequence; that the Department of Defense and cybersecurity companies hunt on defense industrial base networks; and that the administration establish a National Cyber Director.

These recommendations are valuable contributions to the debate on what policies, programs, and organizational constructs will best advance the Nation's cybersecurity. I am proud that we were able to incorporate 11 of these recommendations into the Committee mark of the NDAA, with several additional recommendations which were, unfortunately, outside of our jurisdiction, but were incorporated later on the floor discussion.

While this hearing comes too late to inform the NDAA mark, three objects of the Commission's study remain relevant for this Subcommittee's oversight of the Department's cyberstrategy and operations, and for the Committee's conferencing of the NDAA. First and foremost, I want to discuss the motivations behind the Commission's recommendation and recent annex further detailing the establishment of a National Cyber Director. How is the interagency planning an execution process, broken today? What authorities, especially those relevant to offensive cyber action, should be available to the Director? How would the National Cyber Director act to direct or coordinate Department of Defense action in response to a cybersecurity incident of significant consequence?

Since its establishment, this Subcommittee has focused on improving coordination among the many relevant entities within the Department of Defense to assure synchronized efforts in implementing and executing their cyberspace missions. I believe that the Principal Cyber Advisor within the Office of the Secretary of Defense has been particularly effective at performing that particular oversight and coordination role, and advising the Secretary of Defense. This has been accomplished without the establishment of a large bureaucracy, and without creation of yet another cyber stovepipe within the DOD.

In this year's NDAA, we included a provision that strengthened the Principal Cyber Advisor's oversight and coordination role. I also sponsored a provision in the Fiscal Year 2020 NDAA that added Principal Cyber Advisors for each Service Secretary to provide them with this critical coordination asset. The Principal Cyber Advisors have a departmental or service role, while the proposal for a National Cyber Advisor concerns a national role. However, I think there may be some similarities between the functions of the Principal Cyber Advisors and the National Cyber Director, as envisioned by this Commission. I would, therefore, appreciate discussion on the similarities and differences between the roles of the DOD Principal Cyber Advisors and the proposed National Cyber Director.

Second, I hope to better understand the recommendations the Commission provided regarding the Department of Defense's cyber targeting. Did the Commission see Cyber Command's current plans and operations as matching the Commission's recommendations in cyber deterrence and 6 persistent engagement? Did it find the Department's aspirations for persistent engagement of adversaries to be realistic?

Finally, I want to hear how the Department of Defense can better execute its mission to protect the Nation against Russian, Chinese, Iranian, and North Korean cyberattacks. What are the Department's capability shortfalls? What should its role be in emergency response actions?

Thank you for your diligent efforts in producing this report, and for agreeing to testify before this Subcommittee.

Senator Manchin, welcome. Senator Blumenthal sat in to check and make sure things were working the way they were supposed to. Welcome. Do you have any opening comments, Senator?

STATEMENT OF SENATOR JOE MANCHIN

Senator MANCHIN. Well, Senator Rounds and Senator Blumenthal, thank you very much. I appreciate that.

Thank you, Senator Rounds.

I, too, welcome our witnesses: Senator Angus King, our dear friend, and Representative Mike Gallagher—I guess Mike's—is he going to be on—okay—who served as co-chairs of the Cyber Solarium Commission at—that this Committee established in last year's NDAA; and the third, retired General Chris Inglis, who served as one of the Commission members.

Senator King, of course, is a distinguished member of this Committee. Representative Gallagher, I want to thank him for his work on this Commission and for your great service in the House, and Chris Inglis is no stranger to this Committee, having previously served as the Deputy Director of the National Security Agency.

Thank you, Chris, for being here, too.

I want to take a moment and speak about the efforts of this Commission, why it has been successful, and what lessons we can learn from the future.

A commission of this type is intended not just to educate Congress, the executive branch, and the public. The intent is to forge a consensus on what needs to be done to fix the problems the Commission identifies. However, too often those recommendations are too vague or difficult for Congress to legislate on. The Commission spent a lot of time and effort turning those recommendations into actual draft legislation text. This was an immensely important decision. If you have to turn an idea into bill language, you have to really think it through, and the result has to be compatible with the main purpose of Congress, which is drafting laws.

To be sure, we have had to modify these recommendations, sometimes significantly. But, without those legislative drafts, much of the Commission's work might already be collecting dust on someone's shelf. Instead, a vast majority of the Commission's recommendations were included, in one form or another, in the NDAA bills passed by the House and Senate, including a significant number of recommendations that crossed the jurisdictional lines of mul-

tiple Committees. This is no mean feat. Getting approval across multiple Committees for legislative amendments on the floor of the House and Senate is extremely hard, something that Senator King and Representative Gallagher know very well and were able to do it.

One of the main and most influential Commission recommendations is the creation of a National Cyber Director. This recommendation is not popular with the administration. Senator Rounds and I also concluded that the proposal needed a bit more polishing by the Commission in order to better understand what this position's role should be. Senator King and Representative Gallagher took this on, and, in the last couple of months, have produced a very, very good proposal, which we will talk about here today. The Commission co-chairs firmly believe that this position is crucial to integrating the response of all the departments and agencies who have to be involved in dealing with major cyberattacks. We must have the military cyber forces, the intelligence collectors, our law enforcement officers, and Homeland Security operating as a team, bringing all their authorities and resources to bear to counter an attack. I hope the President and his senior advisors can be persuaded to not just accept this idea, but to embrace it to improve our national security.

While I am greatly impressed with the Commission's effort, I do have two concerns I would like to address with our witnesses today:

First, the recommendation to require reporting of all critical infrastructure entities to the Department of Homeland Security. While it's important that we do all that we can to effectively respond to cyber threats in the timeliest manner, we must do so without interrupting established cyber threat reporting. As Ranking Member of the Energy and Natural Resources Committee, a prime example are critical energy infrastructure entities. They should still report through their established chains with the Department of Energy, and that intelligence should be made available to the eventual National Cyber Director.

Second, the Commission's report explicitly rejected a model deterring major cyberattacks on our critical infrastructure by assuring adversaries who contemplate such actions with an in-kind response; namely, retaliating against their critical infrastructure through cyberattacks. The Commission's report suggests that a retaliatory doctrine of doing to an adversary what an adversary does to us is immoral, and even inconsistent with international law. A strategy of deterrence based on retaliation in-kind, symmetrical against an adversary is the basis of our nuclear deterrence that has been in place since the end of World War II. We do not consider this strategy illegal, immoral, or ineffective. Moreover, the idea that an adversary would be deterred from hitting our critical infrastructure by a threat that we would disable their computers or their cyber forces does not seem very likely to me. This is even assuming that we will be able to identify and incapacitate their cyber forces, which, I submit, is an uncertain and momentary solution.

Before turning to our witnesses for opening statements, I will close by noting that the Commission has proposed, and this Com-

mittee has endorsed, in the NDAA, an extension of the life of the Commission. This was done for the 9/11 Commission, and I think it is a good idea for Senator King and Congressman Gallagher to be able to observe how the Commission's work is being implemented, and to revisit issues that could not be resolved in this year's budget and legislative cycle.

Thank you, Mr. Chairman. I look forward to hearing from our witnesses.

Senator ROUNDS. Thank you, Senator Manchin.

I think the best way to approach this, probably, since you've done a combined opening statement, which is in the record now—Senator King, would you like to begin, and we'll have you and then Representative Gallagher, and then finish up with General Inglis, if that works, in terms of how you would like to proceed?

STATEMENT OF SENATOR ANGUS S. KING, JR., CO–CHAIR, CYBERSPACE SOLARIUM COMMISSION

Senator KING. Thank you, Mr. Chairman.

There are so many aspects of this, an opening statement could go on all afternoon. I am going to try very hard not to make that happen.

Let me just make one point about the pandemic. Among all the other things we've learned, I think one of the most important things we've learned is that the unthinkable can happen. A year ago, we would not have contemplated where we are now with a disease that we're having to deal with on a worldwide basis. So it is with a cyberattack. It seems unthinkable, it seems the stuff of science fiction, and yet it can and it has happened. In fact, it's happening right at this very moment.

Our basic purpose in the work that we did on this Commission—and I will outline how it was—how we proceeded—was to be the 9/11 Commission, without 9/11. Our whole purpose is to avoid not only a cyber catastrophe, but a death by a thousand cyber cuts. That's really what we want to talk about here today.

The Commission, as you mentioned, Mr. Chairman, was set up almost 2 years ago in the National Defense Authorization Act, and our mission was to develop a comprehensive cyber strategy for the country, and recommend how it should be implemented. There were 14 members. I think part of the success of the Commission rests upon how it was structured. There were 14 members: four members of Congress, and then there were four members from the executive, from the relevant agencies, and six members from the private sector. We had over 30 meetings. We had 90 percent attendance at our meetings. We met in this building, just downstairs, over and over. We had hundreds of documents, witnesses, and an immense amount of literature search and review of all of the ideas that could be brought before us on these subjects.

I am proud to say that the work of this Commission was entirely nonpartisan. In fact, to this day, other than the four members of Congress whose—who wear their party labels on their sleeves, I have no idea of the party affiliation of any of the other 10 members of the Commission, and I can honestly say that, in all of those 30 meetings, there was not a single comment, discussion, question that suggested any partisan content or any kind of partisan point

of view in our Committee's—in our Commission's discussions. Four-hundred interviews, we came up with 82 recommendations; 57, as Senator Manchin mentioned, were turned into actual legislative language.

What are the basic principles of the report? They can be summarized in three words: reorganization, resilience, and response:

Reorganization, I think we're going to talk a lot about today. How are we organized in order to meet this challenge?

Secondly, resilience. How do we build up our defenses so that cyberattacks are ineffective, and that that, in itself, can be a deterrent if our adversaries decide it's simply not worth it?

The final is response. How do we develop a deterrent strategy that will actually work, particularly for attacks below the level of the threshold of use of force? We haven't had a catastrophic cyberattack, probably because of the deterrents that we already have in place. The problem is, we're being attacked in a lower-level way continuously, whether it's the theft of intellectual property, whether it's the theft of the OPM records of millions of American citizens, whether it's the attack on our election in 2016. That's the area where we remain vulnerable, and we haven't developed a deterrent policy.

What is layered cyber deterrence, which is the fundamental theory that we put forth? It's to shape behavior, it's to deny benefits, and it's to impose costs.

I know that we're going to spend a great deal of time in this hearing talking about the National Cyber Director, but I do want to address it briefly in these opening remarks.

The mission and the structure of the National Cyber Director is almost identical of the Principal Cyber Advisor position that we've created at the Department of Defense. The difference is a wider scope. Just as we were preparing for the hearing, I made a quick list of seven or eight or nine Federal agencies, all of which have cyber responsibility outside of the Department of Defense. The fundamental purpose and structure of the National Cyber Director is to provide a person in the administration with the status and the advisory relationship with the President to oversee this diverse and dispersed authority throughout the Federal Government. For the same reason we created the Cyber Advisor in the Department of Defense, we need to do it nationwide, and that's the fundamental purpose. I am sure we'll be able to—we'll go into much more detail on this.

But, before I complete my statement, I have got two written records. One is a very strong letter from the U.S. Chamber of Commerce endorsing the National Cyber Director position. The second is the testimony recently in the House by former Representative Mike Rogers, former chair of the Intelligence Committee, who confesses that he has 180 degrees changed his position on the idea of a National Cyber Director, from steadfast opposition to very strong support.

I would like to introduce both of those documents into the record, with the permission of the Chair.

Senator ROUNDS. Without objection.

Senator KING. Thank you.

[The information referred to follows:]

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

NEIL L. BRADLEY
EXECUTIVE VICE PRESIDENT &
CHIEF POLICY OFFICER

1615 H STREET, NW
WASHINGTON, DC 20062
(202) 463-5310

July 14, 2020

TO THE MEMBERS OF THE UNITED STATES CONGRESS:

The U.S. Chamber of Commerce supports H.R. 7331, the "National Cyber Director Act." This bipartisan legislation would elevate cybersecurity decision-making and coordination at the White House. This legislation would assist in coordinating and deconflicting the U.S. government's planning and preparation for, and response to, cyber threats across government. Equally important, it would codify the requirement for the U.S. government to work as the senior point of contact for the American business community, which finds itself on the front line of the cyber domain.* We believe that H.R. 7331 is an important step in the right direction.

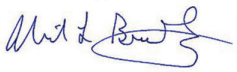
The National Cyber Director (NCD) would fulfill a similar role as the cybersecurity coordinator, but the position would be backed with statutory authority to serve as the president's principal advisor on cybersecurity strategy and policy, review cyber budgets, and coordinate the nation's response to significant cyber incidents.

The creation of an NCD is one of the key recommendations of the U.S. Cyberspace Solarium Commission, a Congressionally-chartered group that includes members of Congress, the Administration, and private-sector leaders. We believe that the codification of this position which has existed in some form across several presidential administrations would assist the American business community in navigating federal policy initiatives and interagency processes, as well as in responding to future cyber events.

Further, businesses would rely on the NCD to help negotiate with federal agencies on key domestic and international cyber priorities. The NCD would send a signal to the public, including U.S. allies, that the White House prioritizes cybersecurity in the attention of the National Security Council and the president.

Congress' leadership is crucial as the business community collaborates with policymakers to strengthen the cybersecurity of American businesses and governmental bodies against malicious actors. We look forward to the passage of H.R. 7331.

Sincerely,



Neil L. Bradley

---

* Legislation is also needed to prioritize a high-level cyber coordinator at the Department of State. This individual would direct U.S. engagement with the international community on issues including investigation, attribution, threat information sharing, response, capacity building, standards, and norms.

15 July 2020

Testimony from the Honorable Mike J. Rogers

Former Chairman, House Permanent Select Committee on Intelligence
Former Representative of the 8th District of Michigan

Chairwoman Maloney, Ranking Member Comer, distinguished Representatives, I am both delighted and honored to testify before you on Rep. Langevin's bill to create the National Cyber Director.

It is heartening to see so many of my distinguished former colleagues listed on this bill: Congressman Jim Langevin (D-RI), Congressman Mike Gallagher (R-WI), House Oversight and Congresswoman Carolyn Maloney (D-NY), Congressman John Katko (R-NY), Congressman C. A. Dutch Ruppersberger (D-MD), and Congressman Will Hurd (R-TX). Truly a bipartisan dream team of congressional cyber experts.

In the testimony that follows, I will outline why I believe the National Cyber Director is necessary for our Nation's cybersecurity now and into the future. I am basing this testimony on the four areas of responsibility outlined by the Cyberspace Solarium Commission: (1) principal advisor to the president; (2) national-level coordination; (3) driving the inter-agency process; and (4) budgetary oversight.

The cybersecurity challenge we face as a nation is both daunting and complex. Just when we think we have a handle on it, something new comes along and disrupts our frame of reference. Quantum computing, machine learning, artificial intelligence, 5G technology, and more, are just the tip of the cyber iceberg that is heading our way.

The 2018 National Defense Strategy rightly noted that "the re-emergence of long-term, strategic competition between nations"[1] was the primary threat to America's security. We are seeing this play out in technology and innovation as much as we are watching it in overt and covert military activities. In 2017, Russia's President Vladimir Putin said, "Artificial intelligence is the future, not only for Russia, but for all humankind… It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."[2]

China, for its part, aims to "occupy the commanding heights of AI technology" by 2030[3] and is aggressively pursuing 5G dominance—the next generation of mobile communications that will revolutionize how we live and work. North Korea understands the value of technology and cyber capabilities, too. Kim Jong-Un said, "Cyberwarfare, along with nuclear weapons and missiles, is an 'all-purpose sword' that guarantees our military's capability to strike relentlessly."[4] Iran is

---

[1] https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf
[2] https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world
[3] https://thediplomat.com/2017/07/chinas-artificial-intelligence-revolution/
[4] https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html

also developing its cyber weapons and Tehran's past behavior indicates its willingness to use these tools to attack its adversaries.[5]

If we do not get our national-level policy sorted now, and if we do not empower the right person and the right office with the responsibility today, I fear we will have a different type of Commission soon—one that looks at why a national cyber incident happened at the hands of China, Russia, or North Korea, and what could have been (or should have been) done to prevent it in the first place.

1. *Be the President's principal advisor on cybersecurity and associated emerging technology issues and the lead national-level coordinator for national cyber strategy and policy*

The current and previous administrations have struggled to handle and manage cybersecurity policy and emerging technologies. This is not a failing inherent to the composition or structure or political ideology of these administrations, but a result of the rapidly changing and complex digital world clashing with the information era.

Our federal government is an industrial era design. Its departments and agencies are structured to focus on narrow areas and their legal remits. This system worked well, for a time. It delivered us a victory in World War II, put a man on the Moon, implemented the Great Society programs, and more. To be sure, it is far from a perfect system and it has a lot of redundancies and could operate a lot smoother and faster, but it largely—in a broad sense—does the job.

But that industrial-era structure is woefully inadequate for the speed of the information-era, its threats, and its opportunities. Cybersecurity is an issue that affects all agencies and all departments and necessitates a unified approach. Expecting them now, and in the future, to develop appropriate policies and respond to emerging technologies is setting them up for failure.

The lack of consistent and indeed institutionalized leadership on cyber issues prevents addressing this government-wide challenge. In my view this is not a transitory issue; it is an issue that will remain front and center, will continue to become more challenging, and will only become more important as American society becomes more and more reliant on data.

It is an overused cliché, but in this case, it is appropriate—data is the new oil, and just like oil needs pipelines and secure networks to power industry, so too does data need security, confidence, and assurance to support the business of business and the business of government.

The government needs data to ensure that Americans receive the services and support they need to live their lives and pursue a better future for themselves and their families. The Department of Education has over 49 million student loan borrowers.[6] Another 38 million receive Supplemental

---

[5] https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
[6] https://www.americanprogress.org/issues/education-postsecondary/reports/2019/06/12/470893/addressing-1-5-trillion-federal-student-loan-debt/

Nutrition Assistance[7] benefits administered by the Department of Agriculture. Another 44 million Americans receive Medicare benefits from the government, roughly 15% of the population,[8] and nearly one in six Americans receive social security benefits (63 million people).[9] Think of the amount of data about each individual that is needed to accurately process and record those benefits. Now think about how attractive that data is to cybercriminals and nation-states alike.

2. *Oversee and coordinate federal government activities to defend against adversary cyber operations inside the United States*

The absence of central coordination for the nation's cybersecurity is a significant vulnerability. With each agency and department pursuing independent cybersecurity policies and practices, significant gaps emerge—gaps that are ripe for exploitation by America's adversaries. Hackers, whether criminal, nation-state, or some flavor of both, aim to find the path of least resistance. The absence of consistency across agencies and departments creates multiple pathways that are ripe for exploitation.

This is not an abstract problem. In April 2015, IT staffers at the Office of Personnel and Management (OPM) discovered that their systems were breached by hackers, ultimately linked to China, that extracted millions of sensitive SF-86 personnel security clearance forms and millions of fingerprint cards. This is not to say that had the National Cyber Director been in place that the OPM hack would not have happened—but it is to say that there would have been a person responsible for ensuring that the nation's cybersecurity posture was as strong and robust as possible, and whom Congress could hold accountable for failings and shortcomings.

The fragmented nature of the federal government's approach to cybersecurity has stood in the way of best practices, efficiency, and effective management for too long. Individual departments and agencies have pursued their cyber policies, best practices, and software resulting in duplicative programs, gaps between and among networks, and significant inefficiencies.

This is to say nothing of the vulnerable position in which the lack of central coordination puts the country. China and Russia are aiming to dominate the next generation of technology—artificial intelligence, quantum computing, 5G, and more. They are not going to sit idly and use those capabilities for purely domestic and benevolent activities. Rather they will use these capabilities against the United States and our allies, just as they are using current technologies against our country. Whether it is intellectual property theft[10] and economic espionage,[11] or electoral

---

[7] https://www.cbpp.org/research/food-assistance/a-closer-look-at-who-benefits-from-snap-state-by-state-fact-sheets
[8] https://assets.aarp.org/rgcenter/health/fs149_medicare.pdf
[9] https://www.cbpp.org/research/social-security/policy-basics-top-ten-facts-about-social-security
[10] https://www.cnbc.com/2019/02/28/1-in-5-companies-say-china-stole-their-ip-within-the-last-year-cnbc.html
[11] https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat

interference[12] via social media and the probing of electrical grids,[13] both Beijing and Moscow have shown their willingness to use cyber capabilities against our country.

What is needed is both a whole-of-government approach and a whole-of-nation approach to cybersecurity. This must go beyond the interagency process and, to do so effectively, needs the National Cyber Director. The Director would coordinate the federal government's domestic cybersecurity posture, ensuring the application of best practices, implementing the latest technologies, and eliminating redundancies, duplicative effort, and—with the budgetary oversight—wasteful spending.

Beyond that, having a National Cyber Director would serve as a focal point for cooperation and collaboration with the private sector. Here, the relationship is not as strong as it could be and indeed should be. The speed with which Silicon Valley companies are conceived, born, grow, and die is unfathomable to the Federal bureaucracy.

When the tech industry looks at Washington, it sees a byzantine structure that is inefficient, does not know what it wants (let alone what it needs) and believes that process is progress for its own sake. In many ways, industry is not wrong. Establishing an individual and an office with the responsibility of leveraging the tech sector, academia, and think tanks towards national cybersecurity policy would—with the right person—give the private sector a measure of confidence that hitherto has been sadly lacking.

Perhaps the greatest challenge is finding the right person to fill this critical slot. That is a task I do not envy. You need someone technically savvy, bureaucratically agile, and can provide confidence to both the government and the private sector. Putting the wrong person in this position would be detrimental not only to the office but to the Nation's cybersecurity posture as well.

If we look at government like a business, it is akin to having the finance department operating one system, human resources another, and logistics ignoring the problem entirely. A simplistic shorthand to be sure, but it is illustrative of what is happening in the absence of a single person coordinating the cybersecurity practices of the organization as a whole.

There is also something to be said about the importance of Congressional oversight of cyber affairs. With the fragmented and uncoordinated approach to the government's cybersecurity policy that exists today, there is no single person accountable for the country's posture. This is a severe limitation on Congressional oversight. As a former committee chairman, I know the importance of being able to call the right person before a committee to answer Congress' questions.

---

[12] https://www.dni.gov/files/documents/ICA_2017_01.pdf

[13] https://www.npr.org/2018/03/23/596044821/russia-hacked-u-s-power-grid-so-what-will-the-trump-administration-do-about-it

3. *With concurrence from the National Security Advisor or the National Economic Advisor, would convene cabinet-level or National Security Council Principals-Committee level meetings and associated preparatory meetings*

Cyber issues are just as important as national security and national economic affairs. It is an issue, perhaps one of a handful, that crosses both security and economic lines. Without a solid cybersecurity posture, we will not be able to maintain our country's security or economic future. As such, a mechanism must exist to ensure that the principals are aware of and decide upon critical national cyber policy issues. Here, the National Cyber Director would play a critical role in ensuring that these issues are addressed in the White House through cabinet-level meetings.

Responding to this dynamic threat and opportunity environment necessitates the development and implementation of a National Cyber Strategy. The current administration released its latest version in 2018,[14] but in the absence of a National Cyber Director, each agency and department is largely left to its own devices to implement the White House's guidance. This renders the strategy largely aspirational, a dynamic that is untenable going forward.

While the White House may be reluctant to accept Congressional creation of offices within the Executive Office of the President, I would think that the National Cyber Director, with its coordination, budgetary, and convening powers would prove to be an invaluable tool for this and future presidents. It would give future administrations a single person and their associate office the responsibility of implementing a strategy across the whole of the federal government.

4. *Would provide budgetary review of designated agency or cybersecurity budgets*

The most powerful Congressional tool, as the Committee well knows, is the power of the purse. In the cyber realm, we have seen a great deal of money spent on various fixes, programs, and initiatives aimed at addressing vulnerabilities. Unfortunately, these expenditures have not been the most efficient or effective. Each agency and department is pursuing its program, unguided by a central mission or priority.

The National Cyber Director would solve this problem by providing not just a clear mission set through the National Cyber Strategy, but also providing oversight of agency and departmental budgets, the Director will ensure that resources are allocated against the threat and the opportunity. By directing spending, lining out programs that are wasteful or inefficient, or simply ensuring—as the National Cyber Director would—that the expenditures align with the strategy, the nation's cybersecurity posture will be better coordinated.

As we have seen, China and Russia are aligning their budgets to pursue their goals of digital, 5G, and artificial intelligence dominance. We need to ensure that our cybersecurity budgets are aligned towards a common goal. If we fail to do so and continue to act and spend in the manner we have to date, we will find ourselves in a strategically weakened position.

This budgetary oversight authority will become even more important when, as it certainly seems now, the Nation will need to tighten its purse strings in response to COVID-19. One of the most

[14] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

significant threats to our national security is our debt and the current economic downturn is exacerbating that pressure. When added with the external threats from Russia and China, and the speed with which future technologies are approaching, we cannot afford to spend needlessly or carelessly.

Conclusion

As my great friend and former colleague Rep. Dutch Ruppersberger put it, "We have great leaders in cybersecurity throughout the federal government, but we need a cyber quarterback."[15] He is 100% right; we need a serious wakeup call We need to get away from the approach of a seven-year-old's soccer game (to mix sports metaphors) where everyone is chasing the ball and get to American football where everyone knows their job and it's the quarterback's task to call the plays.

Put simply, we cannot afford to continue to do business as we have and expect the situation to improve. Our adversaries are not resting, and the industry continues to innovate, and if we expect to be prepared for the future and to fully seize upon the benefits of the information age tomorrow, we need to organize ourselves accordingly. We cannot afford to sit idly and expect the situation to resolve itself or hope that our adversaries will be cowed by our current capabilities. The time for smart action is now. I believe that the National Cyber Director is a critical step towards that reorganization and a smart, sensible policy that I fully support.

[15] https://langevin.house.gov/press-release/congressional-cybersecurity-leaders-introduce-bipartisan-legislation-establish

Senator KING. I will end my comments now, and we will be able to really discuss more of the details, particularly on the National Cyber Director recommendation, as the hearing progresses.

Thank you, Mr. Chair.

[The combined statement of Senator King, Representative Gallagher, and General Inglis follows:]

JOINT PREPARED STATEMENT BY THE HONORABLE ANGUS KING, THE HONORABLE MIKE GALLAGHER, AND MR. CHRIS INGLIS

INTRODUCTION—INTENT OF THE COMMISSION AND FOCUS OF OUR EFFORT

Our American way of life depends on a global, interconnected, and interdependent cyberspace which has created the modern United States' economy and society. At the same time, cyberspace creates political and strategic opportunities for malicious actors seeking to undermine our national security, economy, and political system. For these reasons, the Cyberspace Solarium Commission was established by the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences."

The Commission is composed of fourteen Commissioners, including four currently serving legislators, four executive branch leaders, and six recognized experts with backgrounds in industry, academia, and government service, and this composition is unique to this Commission. Led by Senator Angus King and Representative Mike Gallagher, the Commission spent the past thirteen months studying the challenges facing the United States in cyberspace, developing potential solutions, and deliberating courses of action to produce a comprehensive report. Our Commissioners convened nearly every Monday that Congress was in session for over a year, conducting a total of 30 meetings. The staff conducted more than 400 engagements with industry; federal, state, and local governments; academia; non-governmental organizations; and international partners. The Commission also recruited our nation's leading cybersecurity professionals and academic minds to rigorously stress test the findings and red team the different policy options in an effort to distill the optimal approach to securing the United States in cyberspace.

The Commission's final report was presented to the public on March 11, 2020, and identified 82 specific recommendations. These bi-partisan recommendations were then subsequently turned into 54 legislative proposals that have been shared with the appropriate Committees in the Senate and the House of Representatives. Our Commissioners have now testified before Congress five times to impress upon you the urgency of the cyber threat faced by the United States today.

In addressing the NDAA's tasking, the Commission found that our critical infrastructure—the systems, assets, and entities that underpin our national security, economic security, and public health and safety—are increasingly threatened by malicious cyber actors. Effective critical infrastructure security and resilience requires reducing the consequences of disruption, minimizing vulnerability, and disrupting adversary operations that seek to hold our assets at risk. Not only does our critical infrastructure provide the foundation for our economic and societal strength, but without functioning logistics networks, power generation and distribution, and other critical functions, our military would be debilitated. In short, resilience is national defense.

The Commission identified a number of DOD specific proposals, all of which were taken up by your Committee and edited and improved by your staff, these include: conducting a force structure assessment of the Cyber Mission Force; reviewing delegation of DOD authorities to enable more rapid decision-making to conduct cyber campaigns; requiring companies within the defense industrial base (DIB) to participate in a threat intelligence sharing program and mandatory threat hunting on DIB networks, examining the establishment of a cyber reserve force; and, clarifying the cyber capabilities and strengthen the interoperability of the National Guard, all of these have been included in both the House and the Senate versions of the NDAA. In addition, several recommendations are only in the Senate version, these include: creating a major force program funding category for the U.S. Cyber Command, conducting a cybersecurity vulnerability assessment of all segments of the nuclear control system and continual assessment of our conventional weapon systems' cyber vulnerabilities.

While we do not want to lose sight of the responsibility that this Committee has to focus on military issues, we also recognize that our national security—particularly with respect to cyberspace—cannot rely on the Department of Defense as the only stakeholder. To that end, we urge the Committee to consider the full scope of the 82 recommendations that the Commission proposed in our full report.

The future of our national security requires both the executive branch and Congress to work in tandem to prioritize and implement the key Commission recommendations to build a more effective government cybersecurity capability. These include establishing a National Cyber Director in the Executive Office of the President; strengthening the Cybersecurity and Infrastructure Security Agency (CISA) to lead interagency coordination and coordination between the Federal Government

and private sector; developing a Continuity of the Economy Plan to ensure the public and private sectors are prepared to rapidly restart our economy after a major disruption; recruiting, developing, and retaining a stronger Federal workforce, planning and executing a national-level cyber table-top exercise on a biennial basis that involves senior leaders from the executive branch, Congress, state governments, and the private sector, as well as international partners; and fostering public-private collaboration to ensure coherence, agility and speed in the nation's response to cyber attacks. [1]

A second critical line of effort is building a more robust system for private-public collaboration, this includes recommendations such as establishing an Integrated Cyber Center within CISA, creating a Joint Cyber Planning Office (JCPO) to coordinate cybersecurity planning and readiness across the Federal Government and between the public and private sectors; establishing and funding a Joint Collaborative Environment for sharing and fusing threat information; and establishing authority for CISA to threat hunt on .gov networks. These all also can work in concert to create a more resilient infrastructure, a significant improvement from what we have today. [2]

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

THE CHALLENGE

The Commission's final report made clear that while the United States has, to date, successfully deterred strategic cyberattacks that rise to the level of an armed attack, below that threshold, there is a significant set of adversary behavior that the United States has not prevented. In the past few decades, adversaries have used cyberspace to attack American power and interests. We must be clear—if adversaries attack the U.S. in cyberspace, they will pay a price. The more connected and prosperous our society has become, the more vulnerable we are to aspiring great power rivals, rogue states, extremists, and criminals. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the private sector and the public at large.

The American public relies on critical infrastructure, roughly 85 percent of which—according to the Government Accountability Office—is owned and operated by the private sector. Increasingly, institutions Americans rely on—from water treatment facilities to hospitals—are connected and vulnerable. Securing the nation in the 21st Century requires an interconnected system composed of both public and private networks that is secure from state and non-state threats. China commits rampant intellectual property theft to help its businesses close the technological gap, costing non-Chinese firms over $300 billion per year. Massive data breaches, including those suffered by Equifax, Marriott, and the Office of Personnel Management (OPM), enable Chinese spies to collect data on hundreds of millions of Americans.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In spring 2014, Russian-linked groups launched a campaign to disrupt Ukrainian elections that included attempts at altering vote tallies, disrupting election results through distributed-denial-of-service (DDoS) attacks, and smearing candidates by releasing hacked emails. They continue to spread hate and disinformation on social media to polarize free societies. But they have not stopped there. The 2017 NotPetya malware attack spread globally, temporarily shutting down major international businesses and affecting critical infrastructure. Russian groups have even been found surveilling nuclear power plants in the United States. In Ukraine in 2015 and 2016, they demonstrated the capability and willingness to disrupt power generation and distribution through a cyber operation.

---

[1] The National Cyber Director and strengthening CISA recommendations are in both the House and Senate Fiscal Year 2021 NDAAs; the CotE and stronger cyber workforce recommendations are only in the Senate Fiscal Year 2021 NDAA; and the table-top exercise recommendation is only in the House Fiscal Year 2021 NDAA.

[2] All four of these recommendations: the Integrated Cyber Center, the JCPO, the Joint Collaborative Environment, and CISA threat hunting on .gov are only included in the House Fiscal Year 2021 NDAA.

Iran and North Korea attack United States and allied interests through cyberspace. Iranian cyber operations have targeted the energy industry, entertainment sector, and financial institutions.

There are also documented cases of Iranian APTs targeting dams in the United States with DDoS attacks. North Korea exploits global connectivity to skirt sanctions and sustain an isolated, corrupt regime. The 2017 WannaCry ransomware attacks hit over 300,000 computers in 150 countries, and temporarily disrupted a number of UK hospitals. According to United Nations estimates, North Korean cyber operations earn $2 billion in illicit funds for the regime each year.

Beyond nation-states, a new class of criminal thrives in this environment. Taking advantage of widespread cyber capabilities revealed by major state intrusions, criminal groups are migrating toward a "crime-as-a-service" model in which threat groups purchase and exchange easily deployable malicious code on the dark web. In 2019, ransomware incidents grew by over 300 percent compared to 2018 and hit over 40 U.S. municipalities. More recently, opportunistic hackers have hijacked hospitals and healthcare systems during the COVID–19 pandemic, taking advantage of poorly protected systems when they were most vulnerable.

STRATEGIC APPROACH

The strategy put forth by the Commission, layered cyber deterrence, combines a number of traditional deterrence mechanisms and extends their use beyond the government to develop a whole-of-nation approach. It also updates and strengthens our declaratory policy for cyberattacks both above and below the level of armed attack. The United States must demonstrate its ability to impose costs while establishing a clear declaratory policy that signals to rival states the costs and risks associated with attacking America in cyberspace. Since America relies on critical infrastructure that is primarily owned and operated by the private sector, the government cannot defend the nation alone.

Cyber deterrence is not nuclear deterrence. The fact is, no action will stop every hack. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly to successfully attack American interests through cyberspace. Layered cyber deterrence consists of three layers, each of which are underpinned by broad reformation of the way the U.S. Government approaches cybersecurity. The outer layer consists of shaping behavior by leveraging non-military instruments of power and building partnerships. The second layer focuses on denying adversaries the benefits of attacks by building greater resilience in our critical infrastructure, networks, and systems and reshaping the overall cyber ecosystem towards greater defensibility and security. The inner layer consists of imposing costs on adversaries when they do attack us. While each layer adds an essential dimension to the defense of the nation, they form an interlocking and mutually reinforcing set of activities that concurrently increase the difficulty, costs, and ultimately the will of aggressors who seek to attack our nation in and through cyberspace.

Layered cyber deterrence combines traditional methods of altering the cost-benefit calculus of adversaries (e.g., denial and cost imposition) with forms of influence optimized for a connected era, such as promoting norms that encourage restraint and incentivize responsible behavior in cyberspace. Strategic discussions all too often prioritize narrow definitions of deterrence that fail to consider how technology is changing society. In a connected world, those states that harness the power of cooperative, networked relationships gain a position of advantage and inherent leverage. The more connected a state is to others and the more resilient its infrastructure, the more powerful it becomes. This power requires secure connections and stable expectations between leading states about what is and is not acceptable behavior in cyberspace. It requires shaping adversary behavior not only by imposing costs but also by changing the ecosystem in which competition occurs.

Core to layered cyber deterrence is public-private collaboration to efficiently coordinate how the nation responds with speed and agility to emerging threats, not just on an ad hoc basis, but also in an institutionalized, practiced way. The Federal Government alone cannot solve the challenge of adversaries attacking the networks on which America and its allies and partners rely. It requires collaboration with state and local authorities, leading business sectors, and international partners, all within the rule of law. This strategy also outlines the planning needed to ensure the continuity of the economy and the ability of the United States to rebound in the aftermath of a major, nationwide cyberattack of significant consequence. Such planning adds depth to deterrence by assuring the American people, allies, and even our adversaries that the United States will have both the will and capability to respond to any attack on our interests.

SPECIFIC RECOMMENDATION FOR A NATIONAL CYBER DIRECTOR

For the past 20 years, commissions, initiatives, studies, and even four Presidential Administrations have been challenged to define and establish an effective national-level mechanism for coordinating cyber strategy, policy, and operations. It is imperative that the executive branch have a strong, stable, and expert-led cyber office and leader within the White House. To fill this gap, the Commission recommended the creation of a National Cyber Director. Similar to the way in which the Secretary of Defense's Principal Cyber Advisor (PCA) supports the DOD, the National Cyber Director would support the President by formulating, recommending, integrating, and implementing policies and strategies to improve the nation's ability to operate in cyberspace.

Former House Intelligence Committee Chairman, Mike Rogers, testified to the House Oversight and Reform Committee that "this is not an abstract problem. In April 2015, IT staffers at the Office of Personnel and Management (OPM) discovered that their systems were breached by hackers, ultimately linked to China, that extracted millions of sensitive SF–86 personnel security clearance forms and millions of fingerprint cards. This is not to say that had the National Cyber Director been in place that the OPM hack would not have happened—but it is to say that there would have been a person responsible for ensuring that the nation's cybersecurity posture was as strong and robust as possible, and whom Congress could hold accountable for failings and shortcomings." Establishing a National Cyber Director within the Executive Office of the President would consolidate accountability for harmonizing the executive branch's policies, budgets, and responsibilities in cyberspace while implementing strategic guidance from the President and Congress. [3]

Situated within the Executive Office of the President, the Senate-confirmed National Cyber Director would be supported by the Office of the National Cyber Director and fill several important roles:

1. Act as the President's principal advisor on cybersecurity and associated emerging technology issues and lead development of a National Cyber Strategy and associated policies;
2. Ensure the implementation of the National Cyber Strategy across departments and agencies to include the effective integration of interagency efforts, and providing for the review of designated department and agency cybersecurity budgets.
3. Oversee and coordinate Federal Government activities to defend against adversary cyber operations inside the United States, to include coordination with private sector and state, local, tribal, and territorial (SLTT) entities;
4. With concurrence from the National Security Advisor or the National Economic Advisor, convene and coordinate Cabinet-level or National Security Council (NSC) Principals Committee—level meetings and associated preparatory meetings.

Recommendation Development

Early in this process, Commissioners identified the need to create a leadership position but were faced with three key decision points: (1) how to address the gap in national leadership, coordination, and consistent prioritization, (2) whether to recommend Senate confirmation for the coordination and leadership position, and (3) the size, structure, and scope of authorities.

The Commission explored other options for cybersecurity structure like the creation of a new cabinet department for cyber, but ultimately decided to strengthen the existing agency (CISA), rather than the creating a new department, as the protracted development of a new department would prevent much-needed near-term progress. Like the DOD's PCA, it is imperative that the National Cyber Director get appropriate access to the right leadership, and be institutionalized to be successful. In contemplating the stature of the position, the Commission determined that it must sit within the EOP and be Senate confirmed to not only signal Congress' commitment to cyber issues, but also afford them a level of political support that bipartisan endorsement would bring, and ensure effective oversight. Senate-confirmation of EOP leadership is not without precedent. The heads of the Office of Management and Budget, the Office of the National Drug Control Policy, Office of Science and Technology Policy, and the Office of the United States Trade Representative are all Senate-confirmed. The Director's focus must be on creating and implementing na-

[3] The recommendation for the creation of a National Cyber Director was introduced as a standalone bill in the House as H.R.7331 and is also included in the House Fiscal Year 2021 NDAA. A provision for an independent assessment of establishment of a National Cyber Director is included in the Senate Fiscal Year 2021 NDAA bill.

tional strategy, which further instilled the Commission's conviction that the National Cyber Director must sit apart from departments and agencies, both of which focus on the day-to-day responsibilities of their given mission set. The Office of the PCA at DOD, which the Commission also looked to for guidance, similarly has an office and staff to support their efforts to establish and oversee the implementation of DOD cyberspace policy and strategy.

Recommendation Details

Structure and Size of Office. The National Cyber Director should oversee and manage the Office of the National Cyber Director, and be assisted in their duties by two Deputy National Cyber Directors: the Deputy National Cyber Director for Strategy, Capabilities, and Budget and the Deputy National Cyber Director for Plans and Operations. To fulfill the full range of functions and responsibilities envisioned in the recommendation, the Commission recommends the Office of the National Cyber Director be staffed with approximately 75 to 100 full-time employees,[4] a size similar to that of existing, comparable EOP organizations. A mix of rotating detailees from other federal departments of agencies and direct-hire, full-time employees would comprise those employees.

Policy and Strategy Development and Coordination. The National Cyber Director should be the President's primary advisor on issues involving cyber, cybersecurity, federal information security, and associated emerging technologies, and statutorily appointed to the NSC. Akin to the structure Congress gave the PCA in DOD, the NCD-developed strategy would establish a clear vision, priorities, and objectives to advance the cybersecurity posture of the United States. As such, the National Cyber Director would be responsible for policy and strategy development relevant to these issues, including the development of a National Cyber Strategy, in coordination with other appropriate offices within the Executive Office of the President.

If implemented as envisioned, the National Cyber Director's primary responsibility for cyber and associated emerging technology-related policy and strategy development is not expected to limit or constrain the ability of other White House principals, such as the National Security Advisor, Homeland Security Advisor, or the National Economic Advisor, to address similar issues. However, as a statutory member of the National Security Council and as an Assistant to the President, the National Cyber Director would likely participate in Principal's Committee meetings with the President where these issues are under consideration. Given this reality, the Commission recommends that White House offices avail themselves of the expertise, participation, and guidance of the National Cyber Director (and staff) early and throughout their respective policymaking processes for issues within or related to the National Cyber Director's remit. This should serve to reduce uncoordinated, parallel processes that could undermine the overall aim of a unified, cohesive cyber strategy.

While the policy coordination authorities and responsibilities outlined above are sufficient to empower the National Cyber Director in developing a National Cyber Strategy and implementing its relevant policy changes, they alone would have limited effectiveness in driving implementation through department and agency budgetary and programmatic priorities. Congress itself has acknowledged the need for budget authority for effective execution of programmatic leadership in the authorities it gave the DOD PCA to advise, advocate for, and identify shortfalls in DOD budgets with respect to DOD cyber planning. Additionally, the lack of any oversight authority for performance, programs, and budget would significantly limit the National Cyber Director's ability to negotiate compromises among departments and agencies, forge consensus, and drive the President's agenda, something the DOD PCA authorizing legislation (Fiscal Year 202014 NDAA as amended in Fiscal Year 2020 NDAA) addressed by providing the PCA the ability to provide recommendations on addressing such shortfalls in the Program Budget Review process. The Commission recommends that the National Cyber Director be granted, in coordination with the Office of Management and Budget, similar budget and oversight responsibilities in the implementation of a National Cyber Strategy, to include an annual assessment and report to Congress and the President on departments and agencies' implementation of the strategy and its relevant policies and programs.

The National Cyber Director should have the authority to act as a certifier for department and agency budgets. This authority would grant the National Cyber Director the power to review the annual budget proposal for each federal department or agency and certify to heads of these organizations and the Director of the Office

[4] While the Commission's March 2020 report recommended the Office of the National Cyber Director to be staffed by 50 persons, follow-up interviews with various experts consistently and strongly supported increasing the staff number to 75 to 100.

of Management and Budget whether the department or agency proposal is consistent with the National Cyber Strategy. It is expected that the National Cyber Director and the relevant examiners in the Office of Management and Budget would work closely together early and throughout the entire budgetary process to identify inconsistencies, gaps, and redundancies in budget and programs and negotiate resolutions with relevant departments and agencies. Additionally, the Director would have the authority to review department and agency transfer or reprogramming requests to the Office of Management and Budget that would increase or decrease funding for cybersecurity programs, projects, or activities by more than five percent. This authority would allow the Director to ensure transfer and reprogramming actions are also consistent with the National Cyber Strategy.

Defensive Cyber Operations Planning, Coordination, and Execution. The National Cyber Director should lead the coordination and integration of U.S. Government defensive cyber activities, such as a Federal Government response to a significant cyber incident affecting the U.S. Homeland and "defensive cyber campaigns," or whole-of-government efforts designed to deter, defend against, mitigate, or limit the scope of an identified malicious cyber campaign. The National Cyber Director should act primarily as a convening authority in planning and coordinating these operations, ensuring that they are fully integrated, taking full advantage of participating department and agency authorities and capabilities, and reflecting the President's priorities, similar to the authority of the DOD PCA. Day-to-day execution of cybersecurity responsibilities should be carried-out by appropriate federal departments and agencies, such as CISA, the Federal Bureau of Investigation (FBI), the Department of Defense (DOD), Sector Specific Agencies (SSAs), and others as appropriate. The National Cyber Director is intended to ensure that they are appropriately and effectively deconflicted, integrated, and mutually-supporting in their approaches, and receive necessary support in furtherance of broader government-wide efforts. The DOD PCA, in the authorizing legislation, was granted the authority to assist in the overall supervision of Department defensive cyber operations, including activities of component-level cybersecurity service providers and the integration of such activities with activities of the Cyber Mission Force. Similar to DOD's use of the Chairman Joint Chiefs of Staff (CJCS) position to effect cohesion among the operational COCOM's, the NCD would not serve as the operational commander but would ensure that tasking to the individual agencies is mapped to national strategy, coherent across departments and agencies, mutually supporting, and properly resourced to ensure success.

While the National Cyber Director plays the lead role in coordinating the whole-of-government response to a significant cyber incident, the National Cyber Director should play a supporting role in instances where the incident evolves into a national emergency with broader physical consequences. The Department of Homeland Security, and the Homeland Security Advisor, play leading roles in executing and coordinating government responses for emergencies and disasters. Where these emergencies or disasters are a result of a significant cyber incident, or have caused cyber-or cybersecurity-related consequences of their own, the National Cyber Director would support and coordinate with the Department of Homeland Security and the Homeland Security Advisor within the scope of their authorities and responsibilities.

The Commission recommends that the National Cyber Director be made aware of cyber-related Title 10 and Title 50 operations at the discretion of the National Security Advisor. The NCD, like the PCA at DOD, has a legitimate need for comprehensive situational awareness, and therefore should be given the same insight into offensive operations. Given the complexity of cyber operations, and the potential for retaliation in ways that could affect the Homeland, the National Cyber Director should be made aware of relevant U.S. operations in order to plan, coordinate, and balance preparatory defensive efforts with such offensive operations. Furthermore, it is expected that, as a constituent member of the National Security Council, the director would participate in any Principal's Committee meeting where offensive cyber operations are under consideration and provide perspective as appropriate.

Coordination with the Private Sector and International Partners. The National Cyber Director would be the foremost spokesperson for the U.S. Government for cybersecurity and emerging technology issues. As an Assistant to the President and the senior-most official in the government focused on cyber and cybersecurity, the National Cyber Director would speak with the President's voice and represent the President's priorities in engagement with the general public, the private sector, and the international community. The National Cyber Director is not intended to overstep or interfere with the traditional roles played by other federal agencies, elements of the Intelligence Community, and others. In any activity where the National Cyber Director engages with the private sector, SLTT leaders, foreign coun-

tries, or the general public, it is expected the National Cyber Director would coordinate and work closely with relevant departments and agencies.

The National Cyber Director, and their office, would serve as the principal touchpoint for senior private sector leadership on cyber, cybersecurity, and related emerging technology issues. The National Cyber Director, like the PCA Office for DOD, would complement and coordinate with CISA in developing and building an effective public-private partnership. The Commission recommends that CISA, and other agencies as applicable, include and coordinate with the National Cyber Director in senior-level meetings of sector coordinating councils, cross-sector coordinating councils, and other meetings of the Critical Infrastructure Partnership Advisory Council. The National Cyber Director should also work in conjunction with and complement the Joint Cyber Planning Office (JCPO) within the Cybersecurity and Infrastructure Security Agency, charged with drafting and coordinating plans and playbooks across departments and agencies at the working level under the guidance, processes, and priorities set by the National Cyber Director.[5]

It is expected that the National Cyber Director would participate in meetings with international allies and partners on topics of cybersecurity and emerging technologies to implement the National Cyber Strategy and advance the President's international priorities. The Commission recommends that the National Cyber Director be included as a participant in preparations for and execution of cybersecurity summits and other international meetings at which cybersecurity or related emerging technologies are a major topic.

OTHER NOTABLE RECOMMENDATIONS

CMF Force Structure Assessment: The Commission recommends that Congress direct the Department of Defense (DOD) to conduct a force structure assessment of the Cyber Mission Force (CMF) to ensure appropriate force structure, capabilities, and resources for DOD's numerous missions in cyberspace. The CMF is the operational arm of U.S. Cyber Command, and CMF teams defend the nation in cyberspace, provide support to geographic combatant command, defend the DOD Information Network, as well as serve analysis and planning functions. A force structure assessment of the CMF, as well as an assessment of the resource implications for the various intelligence community agencies that provide tactical intelligence in their capacity as combat support agencies, will work to ensure the CMF has sufficient forces, capabilities, streamlined decision-making processes and appropriately delegated authorities to achieve its objectives.[6]

Vulnerability Assessment of Nuclear Control Systems and conventional weapons programs: A priority of the Commission was developing recommendations to ensure the United States could continue to maintain credible deterrence above the level of war using the full spectrum of DOD response capabilities, and to prevail in crisis and conflict if deterrence fails. This requires the reliability and resilience of our weapons systems–that they will work when needed, and as intended. Our Commission sought to ensure that our adversaries cannot exploit cyber vulnerabilities to hold our weapon systems, both conventional and nuclear, at risk and that these capabilities are resilient to adversary actions in cyberspace both during conflict as well as below the level of war in day-to-day competition. This is why the Commission recommends that Congress direct the DOD to conduct a cybersecurity vulnerability assessment of all segments of the nuclear control system and continually assess our conventional weapon systems' cyber vulnerabilities. Recently, the DOD has taken critical steps to address this issue. As directed by Congress in the Fiscal Year 2016 NDAA, DOD began assessing the cyber vulnerabilities of each major weapon system. However, barriers to effective cybersecurity remain. There is no permanent process to periodically assess the cybersecurity of fielded systems. Additionally, it is also crucial to evaluate how a cyber intrusion or attack on one system could affect the entire mission, assessing vulnerabilities at a systemic level.[7]

Defense Industrial Base Threat Intelligence Sharing: The Commission recognized that there are gaps in current efforts to address cyber vulnerabilities in the defense industrial base (DIB), where adversary threats continue to cause the loss of national security information and intellectual property. They also generate the risk that, through cyber means, U.S. military systems could be rendered ineffective or their intended uses distorted. This is why one of the critical recommendations the Com-

[5] The Joint Planning Office (JCPO) recommendation is included in only the House Fiscal Year 2021 NDAA.

[6] The CMF Force Structure Assessment recommendation is included in both the House and Senate Fiscal Year 2021 NDAA.

[7] Vulnerability Assessment of Nuclear Control Systems and conventional weapon systems recommendations are only included in the Senate Fiscal Year 21 NDAA.

mission makes in the report is to require companies within the DIB to participate in a threat intelligence sharing program. Today, there is no truly shared and comprehensive picture of the threat environment facing the DIB, and this recommendation works to remedy that. [8]

Delegation of DOD Authorities: The Commission also recommends reviewing the delegation of DOD authorities to ensure they are sufficiently delegated down to enable more rapid decision-making to conduct cyber campaigns. In particular, the Commission recommends a review of the conditions under which information warfare authorities should be delegated to U.S. Cyber Command. While information is not explicitly discussed in the 2018 DOD Cyber Strategy, the Commission recognizes that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making. [9]

Cyber Reserve Force: A final critical element of supporting defend forward is the establishment of a "cyber reserve force" to provide a surge capability that the DOD can mobilize in times of crisis or conflict. The Commission believes this should be a non-traditional military reserve force, with less restrictive and burdensome requirements for drilling, grooming, physical fitness, and other standards. This is meant to address issues of talent management, particularly retention, within the current active and reserve force. [10]

Threat Hunting: To identify vulnerabilities on networks critical to national security, the Commission also recommends that there should be a mechanism for mandatory threat hunting on DIB networks. Actions such as improving detection and mitigation of adversary cyber threats to the DIB are critical to providing for the proper functioning and resilience of key military systems and functions. It is also critical to establish authority for CISA to threat hunt on .gov networks for the same reasons. Congress must also establish authority for CISA to threat hunt on .gov networks. Actions such as improving detection and mitigation of adversary cyber threats to the DIB and the .gov are critical to providing for the proper functioning and resilience of key systems and functions. [11]

Joint Cyber Planning Office and Tabletop Exercises: Elements of the U.S. Government and the private sector often lack the institutions and tools necessary for successful collaboration to counter and mitigate malicious nation-state cyber campaigns. To address this shortcoming, the executive branch should establish a Joint Cyber Planning Office under CISA to coordinate cybersecurity planning and readiness across the Federal Government and between the public and private sectors for significant cyber incidents and malicious cyber campaigns. In a similar vein, Congress should direct the U.S. Government to plan and execute a national-level cyber table-top exercise on a biennial basis that involves senior leaders from the executive branch, Congress, state governments, and the private sector, as well as international partners, to build muscle memory for key decision makers, develop new solutions, and strengthen our collective defense. [12]

National Guard: Congress should also clarify the cyber capabilities and strengthen the interoperability of the National Guard. States have increasingly relied on National Guard units under state Active Duty and Title 32 of the U.S. Code to prepare for, respond to, and recover from cybersecurity incidents that overwhelm state and local assets. [13]

Strategy to Secure Foundational Internet Protocol and Email: To help reduce vulnerabilities in government networks and critical infrastructure, Congress should require the National Telecommunications and Information Administration and CISA to work with private stakeholders to develop a strategy to secure foundational internet protocols. In parallel, CISA should work with private sector partners to implement a more secure standard for email across all U.S.-based email providers. [14]

---

[8] DIB Threat Intelligence Sharing recommendation is included in both the Senate and House Fiscal Year 2021 NDAA.

[9] Delegation of DOD Authorities recommendation is included in both the Senate and House Fiscal Year 2021 NDAA.

[10] The Cyber Reserve Force recommendation is included in both the Senate and House Fiscal Year 2021 NDAA.

[11] The DOD threat hunting recommendation is included in both House and Senate Fiscal Year 2021 NDAA, the CISA threat Hunting recommendation is included in only the House Fiscal Year 2021 NDAA.

[12] The JCPO and tabletop exercise recommendations are included in only the House Fiscal Year 2021 NDAA.

[13] The National Guard recommendation is included in both the Senate and House Fiscal Year 2021 NDAA.

[14] The Strategy to Secure Foundational Internet Protocol and Email recommendation is included in only the House Fiscal Year 2021 NDAA.

Continuity of the Economy Planning: The United States must take immediate steps to ensure our critical infrastructure sectors can withstand and quickly respond to and recover from a significant cyber incident. As a whole, the government should more thoroughly plan for what we know to be an eventuality, as we currently do for military planning. Congress should direct the executive branch to develop a Continuity of the Economy plan. As the COVID–19 pandemic has demonstrated, the United States does not currently possess sufficient planning to ensure the continuity of the economy in the face of disruption. This plan should include the Federal Government; state, local, territorial, and tribal (SLTT) entities; and private stakeholders who can collectively identify the resources and authorities needed to rapidly restart our economy after a major disruption. [15]

Codify Sector Risk Management Agencies and Establish a National Risk Management Cycle: The Commission recommends that Congress codify sector-specific agencies in law as "sector risk management agencies" to ensure consistency of effort across critical infrastructure sectors and ensure that these agencies are resourced to meet growing needs. In conjunction with this codification, the Commission recommends establishing a four-year cycle of risk identification and assessment led by DHS, in coordination with sector risk management agencies, that prompts and supports a National Critical Infrastructure Resilience Strategy led by the President. [16]

Joint Collaborative Environment and Integrated Cyber Center: Effectively ensuring U.S. defense in cyberspace also requires creating a robust public-private collaboration to protect national critical infrastructure through sharing and fusing threat information, insights, and other relevant data in a joint collaborative environment. This will require an effective integrated cyber center within CISA which will improve integration of the numerous existing federal cybersecurity centers, sustaining and supporting the National Security Agency Cybersecurity Directorate's collaboration with and support to other federal departments and agencies, and facilitate a more robust relationship between the Intelligence Community and the private sector. Such an effort would work hand in hand with the Commission's recommendation to review existing authorities for providing intelligence support to the private sector and, where appropriate, codify processes for identifying private sector cyber intelligence needs and priorities. More generally, it is also critical for Congress to institutionalize DOD participation in public-private cybersecurity initiatives following the model of the Pathfinder program. Such initiatives allow public-private collaboration to move beyond threat information sharing toward better human-to-human collaboration. [17]

Assistant Secretary of State: Congress should create an Assistant Secretary of State in the Department of State, within a new Bureau of Cyberspace Security and Emerging Technologies, who will lead the U.S. Government effort to strengthen international norms in cyberspace and build a coalition of like-minded allies and partners to enforce those norms. This high-level leadership is required to coordinate efforts to shape behavior in cyberspace and ensure the future internet reflects the tenets of freedom, interoperability, security, reliability, and openness.

Not only do these values best support democracy, but they also foster the economic environment in which our open and competitive market thrives. [18]

Cyber Insurance: Insurance could be a means to improve cyber risk management at scale, but the market for insurance to protect against cyber risk is immature and therefore failing to deliver on this public policy potential. To help improve the reliability of cyber insurance risk management and unlock the market, Congress should fund a Federally Funded Research and Development Center to serve as the focal point for the development of training and certification programs for cyber insurance underwriters and claims adjusters. [19]

CONCLUSION

The number of cyberattacks that the United States and its allies and partners have experienced clearly indicate the vulnerabilities we face in defending our critical infrastructure. Today, the nation faces a different challenge in the form of the pan-

---

[15] The CotE Planning recommendation is included in only the Senate Fiscal Year 2021 NDAA.

[16] Codifying Sector Risk Management responsibilities is included in only the House Fiscal Year 2021 NDAA.

[17] The Integrated Cyber Center within CISA and funding for a Joint Collaborative Environment recommendations are included in only the House Fiscal Year 2021 NDAA.

[18] The Assistant Secretary of State recommendation is not included in either the House or Senate Fiscal Year 2021 NDAA due to disagreements over where to place the position, not opposition to the concept.

[19] The Cyber Insurance FFRDC recommendation is included in only the House Fiscal Year 2021 NDAA.

demic, a non-traditional national security emergency, which has demonstrated the critical need we face in the cyber domain for both strategic leadership at the White House, and the need to build resilience in our networks to withstand and rapidly recover from a significant critical infrastructure attack.

We believe this Committee, in addition to its traditional DOD oversight responsibilities, should continue to lead in the cyber domain by supporting national security related NDAA cyber provisions, and work to incorporate key Cyberspace Solarium Commission recommendations that strengthen and prepare the nation for cyberattacks, including the recommendations for the National Cyber Director and Continuity of the Economy Planning efforts.

The 2019 NDAA charted the U.S. Cyberspace Solarium Commission to address two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequence? What policies and legislation are required to implement that strategy? The Commission has completed its assigned tasks and provided the executive branch and Congress with a number of legislative and policy proposals. We now need your leadership to review and enact these key legislative proposals and empower and resource the government and the private sector to prepare ahead of the crisis, and to act with speed and agility to secure our cyber future.

Senator ROUNDS. Thank you, Senator King.

Representative Michael Gallagher, I believe you'll be joining us virtually here. Are you ready, sir?

Representative GALLAGHER. I am. Can you hear me?

[Laughter.]

Senator ROUNDS. Ah. Just back off a little bit. Hang on a second. We're going to bring that volume down just a little bit, here.

All right, let's try that again.

Representative GALLAGHER. Okay. Hopefully, that's a little bit better, not too jarring.

Senator ROUNDS. Much, much better. Thank you.

Welcome.

STATEMENT OF REPRESENTATIVE MICHAEL J. GALLAGHER, CO–CHAIR, CYBERSPACE SOLARIUM COMMISSION

Representative GALLAGHER. Thank you, Mr. Chairman. Thank you for, not only your leadership, but for the kind words about my baby daughter. We truly do feel blessed, and, to my good friend, Ranking Member Manchin, thank you, sir, and all the distinguished Members of the Committee, for allowing us to testify on behalf of our report.

I have enormous respect for this Committee in the Senate, because, before I was a member of the House, I was a staffer in the Senate, which is to say there was a time when I actually used to wield real power.

[Laughter.]

Representative GALLAGHER. So, thank you for letting me return to my roots in the Senate.

As Angus, my—as Senator King laid out, our adversaries' cyber operations continue to increase in sophistication and frequency, creating what is really an unacceptable risk to our national security. Given what we know, the state of our defenses and our adversaries' intentions, a major disruptive cyberattack to critical infrastructure at this point is almost something to be expected. Therefore, I would say we have no choice but to hope for the best while planning for the worst.

With this in mind, I would like to emphasize at least two of our critical proposals as we look ahead to the NDAA conference.

First, I strongly agree with my co-chair, Senator King, on the importance of establishing a National Cyber Director. The country needs strategic leadership on cybersecurity, and we all believe this is the right balance of authority, responsibility, and necessary prominence. A Senate-confirmed National Cyber Director within the Executive Office of the President that wields both budget and policy authority, to coordinate cyber policy across the Federal Government, in my opinion, and in the opinion of the Commission, would bring the focus that cybersecurity desperately needs at the highest levels of the Federal Government.

Secondly, I would like to highlight the necessity for continuity-of-the-economy planning. We need resilience and redundancy in our critical infrastructure, and national resilience necessitates planning. I would submit that the pandemic has shown, not only that our economy is vulnerable to widespread disruption, but to the potential impact that economic disruption has on Americans. Just as we thought through the unthinkable in the earliest parts of the Cold War, so, too, now we need to think through the unthinkable, in terms of how we would rapidly recover in the wake of a massive cyberattack so that we have the ability to strike back with speed and agility against whoever chooses to test us.

I would also say that, to ensure the U.S. Government reduces vulnerabilities across critical infrastructure, Congress must address a number of issues that impact multiple agencies that currently work together to protect our national security in cyberspace. Just a few of our key recommendations on that front include: one, the institutionalizing of DOD participation in public/private cybersecurity initiatives; two, establishing and funding a joint collaborative environment for sharing and fusing threat information; three, establishing an integrated cyber center within the Cybersecurity and Infrastructure Security Agency (CISA) to host that collaborative environment and integrate our seven existing Federal cyber centers; four, creating a joint cyber planning office; five, conducting a biennial senior-leader cyber exercise to test our plans, playbooks, and integration efforts; and finally, and sixth, establishing authority for CISA to do threat-hunting on all dot-gov networks. All of these provisions are included in the House version of the NDAA.

Perhaps our most important conclusion, and what I will close on, and a recommendation from the Commission, is that failure to act is not an option. While we've made remarkable progress in the last few years, the status quo is simply not getting the job done, and the time to act is now.

Thank you again for the opportunity to testify before you today, and for your commitment to American cybersecurity.

Senator ROUNDS. Representative Gallagher, thank you very much for your opening statement.

Now we'll turn to Brigadier General, Retired, John Inglis.

Mr. Inglis, please proceed.

STATEMENT OF BRIGADIER GENERAL JOHN C. INGLIS, ANG (RET.), COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Brigadier General INGLIS. Thank you, Chairman Rounds, Ranking Member Manchin, and all the distinguished Committee Members, for the privilege of testifying before you today on the recommendations from the Cyberspace Solarium Commission.

I agree with my fellow commissioners that this last year has been, for me, an honor and the opportunity of a lifetime to hear from the expert counsel of a broad array of experts in cyber technology, policy, and operations across the continuum of private and public sectors, to include consideration of how both allies and adversaries approach the challenge of defining and executing a national cyberstrategy.

I fully back my colleagues here in supporting both the overall report, to include its 82 recommendations, and to urge you to, in particular, swiftly pass the provisions that we'll probably discuss in great detail today, not least of which, the National Cyber Director. To that extent, I would like to focus my opening remarks on the National Cyber Director.

This Committee has done much to improve both the Nation's understanding and the military's preparedness to deal with the challenges of cyberspace, and yet we must do still more, for military cyber power is only one of the many instruments of power that must be applied to achieve our aims in and through cyberspace. As you well know, cyberspace is inextricably linked to every other domain of human interest, such that, while cyber, comprised of both technology and the humans who make use of it, is an instrument of power in its own right, all other instruments of power increasingly depend upon a properly functioning cyberspace for their efficient and effective operation.

The reverse is also true, namely that the proper functioning of cyberspace relies upon the effective employment of a diverse array of authorities, tools, and expertise. These tools and authorities are not held by one person, one organization, or one sector, and they do not self-organize into the coherent whole we require to ensure that cyberspace is appropriately robust, resilient, and well-defended against the increasing threats posed by transgressors who often operate with impunity, holding both cyberspace and, in turn, our nation's security at risk.

Our adversaries have gone to school on us. They routinely seize the initiative of choosing the time, the place, the manner of their transgressions without regard to imagined or commonly accepted boundaries between the pervasively interconnected swaths of cyberspace that are, again, operated by individuals, the private sector, and governments, as a collective whole. Absent a consistent, proactive, and joined-up effort on our side that gives a premium to preparation, integration, and collaboration, we will fall further behind.

To that end, the United States needs a leader to act as the President's principal advisor on cybersecurity and associated emergency technology issues, and to coordinate the Federal Government response. Our experiencing—our experience as a Nation in preparing for kinetic attacks has richly informed doctrine and plans on how

the military will respond to kinetic attack, to include the supported and supporting roles that other instruments of national power would play under various scenarios. We're not in the same place with respect to cyberattack, where the military instrument may not be the singular, or even the supported, instrument of national power, let alone the need to consider the actions of the private sector, which typically maintains and operates the front line of cyberattacks as they maintain and operate over 85 percent of what we know as cyberspace.

To that end, there is a rough, but useful, analogy to be drawn between what we're recommending here, in the National Cyber Director, and the Department of Defense's use of the Principal Cyber Advisor and/or even the Chairman of the Joint Chiefs of Staff. Both positions are used to effect cohesion amongst the operational combatant commanders without usurping the efficient execution of the operational authority of those commanders.

While installing another player, the National Cyber Director, into the coordination of already complex cyber operations could be a concern, I think it's important to note how this functions in the Department of Defense. Importantly, neither the Principal Cyber Advisor or the Chairman of the Joint Chiefs of Staff serve as operational commanders in their distinct and separate roles. The Cyber Advisor ensures coherent planning for cyber capability and doctrine, and the Chairman ensures the tasking of the individual combatant commanders is mapped to national strategy, is coherent across COCOMs, and is mutually supporting and properly resourced. These are useful force multipliers for forces that are often outnumbered but never outmatched by our adversaries. National Cyber Director would fulfill analogous functions across agencies, similar to the role these two roles that are already well-established and very useful within the Department of Defense.

Finally, I would simply note that cyberspace exists inexorably in the presence of adversaries. The contested nature of cyberspace, where the U.S. is challenged by adversaries who can and do attack us on every front—in our homes, in our places of business, and within our critical infrastructure—names—needs the same essential coherence in national strategy, defined roles and responsibilities, and in the propensity to collaborate based on leadership that connects and supports the various players to a national strategy.

I would simply close by saying, while it remains difficult to propose or to name the time and place adversary action will take place in cyberspace, we can be certain that it will take place. A failure to warn, prepare, and respond will result in sure and certain costs that we can ill afford in a future where our dependence on digital infrastructure will only grow. The time to act is now.

I close my opening remarks, again, with the thanks for promoting this hearing and an opportunity to discuss these in greater detail.

Senator ROUNDS. Thank you very much for your testimony.

I think—let me begin. I do appreciate the work that this Commission has done. You've not only started out with a whole series of proposals, but, when we asked you to go back and to flesh out, in particular, the authorities and responsibilities of what a Cyber

Director would look like, I have really appreciated the responsiveness to—from the Commission back to the Committee.

It is our intent to use this information to discuss and to, basically, provide information during the markup of the reconciliation between the House and the Senate versions of the NDAA in conference, and the House Committee has laid out what their vision is. The concern that we had expressed was one that we believe that the Principal Cyber Advisors, as laid out within the Department of Defense, have allowed for technical knowledge and for professional expertise to be available and deliverable to our chief executive officers immediately, and that, with that additional expertise, they could facilitate the use of cyber activities, offensive and defensively, where needed.

The concern that we had was that, if, at the national level, you created a silo, a location where there could be authority or, for that matter, responsibilities and the ability to simply have one more stop along the way in deciding before policy could be executed, that we risk making those cyber responses more challenging.

Now, the reason why I lay this out for you this is way is, is that, over the last several years, we have followed what has happened at the executive branch with, originally, a very well-intended PPD–20, Presidential Policy Directive Memorandum 20, which was started in the previous administration. Their intent was to find consensus, but, before cyber activities would be rolled out. Unfortunately, in doing so, it became a consensus, which meant that any one of a number of a different individuals could stop the movement forward of any cyber activity. That was changed a couple of years ago with the creation of NSPM–13, National Security Policy Memorandum 13, in which a clear line was laid out for the decision-making process on the use of cyber tools and the availability of cyber for our warfighters.

The reason why I lay this out is, is we were able to, in coordination with the executive branch, streamline the process, so we were actually able, as—and I wouldn't discuss this, except that President Trump did share a little bit about it—2018 and the fact that we did not have interference in our 2018 election was not by accident, it was because of the clear capabilities of men and women of Cyber Command. It was because they could execute appropriate cyber policy in an expeditious manner.

What I don't want to have happen in—is to have another layer of bureaucracy get in the way. I think you've done an excellent job of laying out for this Subcommittee your vision of what this would look like. But, I think, for the record, I would ask all of you, Would it be your intent that this Cyber Director be identified as much as a Principal Cyber Advisor, similar to the DOD, versus having authority, responsibility, and the ability to silo those areas and create a roadblock for cyber actions in the future?

Senator King?

Senator KING. Mr. Chairman, I would say that our proposal is the anti-silo. The problem is now, as I mentioned, we've got cyber activities and planning and work going on throughout the Federal Government, and the whole idea is to bring some coherence and coordination to that.

To your specific question, which I think is an important one, we do not propose that the National Cyber Director be in the chain of command for cyber actions. It's Cyber Command, Secretary of Defense, President of the United States. We are not talking—and you used the term "policy executed"—we're not talking about adding a layer, in terms of execution of policy. We're talking about adding a coordinating function to bring together the expertise throughout the Federal Government. I think that's a very important distinction. That's a totally valid question, but we view this as a bringing-together of a coherent organization with someone at the top that has oversight and situational awareness of what's going on in all these different agencies. But, in terms of cyber action, such as the action you cite in the 2018 election, this person would be an advisor to the President, yes.

Senator ROUNDS. That's what I am hoping, and that's what I—I just wanted to make it clear so that—and I would sure like to have Representative Gallagher concur with that, if he's available, as well.

Representative GALLAGHER. I do concur with what Senator King expressed. I think I speak for the whole Commission when I say the intent of this proposal was to build interagency integration and not to add bureaucracy. I think, Mr. Chairman, you did a great job of laying out how far we've come in recent years on the offensive side. A lot of this starts 2 years ago with the provisions we put in, as Congress, to make cyber surveillance and reconnaissance a persistent military activity and traditional military activity.

Senator ROUNDS. Correct.

Representative GALLAGHER. NSPM–13 is laid on top of that, and one of the—I think, the primary values of NSPM–13 is that it just establishes clear authority. Right? As my good friend Senator King continually reminds me, you always want one throat to choke, one person to keep accountable. I think our vision for this was to provide the President with that person primarily on the defensive side.

Now, the final thing I would say is just to confess, my bias when I came into this was to resist the creation of new agencies and, you know, positions. Largely, I think, we have avoided that. But, with this, I have come to believe it's actually the least bureaucratic option. One option would be to create a separate agency entirely. I think that's pretty bureaucratic. But, doing nothing I actually think is the most bureaucratic option, because I think it will lead to a catastrophic cyber incident that will require in layering on of new agencies and positions in response to that. So, we really want that National Cyber Director to get to the left of that cyber boom by coordinating and advising the President primarily on the defensive side of the equation.

Senator ROUNDS. Great, and thank you very much.

I am about out of time, but, Mr. Inglis, what would your—very quickly, what would your thought——

Brigadier General INGLIS. I would say that—I think I speak confidently—the Commission would support your sense of the substance and the spirit of the National Cyber Director. The National Security Advisor is busy. He doesn't have the time, or she doesn't have the time, to, on a daily basis, try to figure out what our overall strategy is, vis á vis cyber. Much like this Committee has rec-

onciled how we think about the military instrument of cyberpower, what we asked, I think, 2 years ago, was, of the Nation, What is the context of the application of the military instrument of cyberpower? Is it a traditional military instrument—traditional military activity, or not? Give us the expectations of what, then, it might do, and then let us go do it. I think the National Cyber Director needs to treat all the instruments of power in the same way: provide context, provide expectations, and allow the depth of expertise to then do that in a distributed fashion.

But, absent the sense of the context or the fabric, what we'll have is a series of stovepipes that actually are a jazz band that makes no music worth listening to.

Senator ROUNDS. Thank you.

Senator Manchin.

Senator MANCHIN. Thank you, Mr. Chairman.

I guess, to Senator King and to Congressman Gallagher and to General Inglis, I am understanding that the way we have the 17 different intelligence agencies—and I would assume every intelligence agency has its own cyber—I know that the FBI has a cyber center for law enforcement, DHS has a cyber center for dealing with cyberattacks on the Homeland, DOD, and on and on. So, you're saying that this one person would be gathering all the information. So, I think, if we have a credible threat to the Homeland, if we have a credible threat, they all would have to interact, I would assume, and agree that this is a valid threat to present. Is that the way it's done now, or is it, basically, just each one taking their own different direction and shot at how they're going to——

Senator KING. Well, we've——

Senator MANCHIN.—counter this?

Senator KING. Different agencies have different responsibilities. In addition to the ones that you mentioned, other—the other agencies that have cyber responsibilities are FERC——

Senator MANCHIN. Sure.

Senator KING.—the EPA, the Department of Energy. I mean, it's just so broad. What we're talking about is having an office—and not a big office. We talked about the possibility, as Representative Gallagher mentioned, of creating a new department, but we thought that was too bureaucratic, too heavyhanded, and would take too long. This is a position that's—there are really two models for the position we're talking about. One is the Cyber Advisor in the Department of Defense. I think that's an almost exact analogy, because it was created because there was too many moving parts in the Department of Defense. There needed to be a coordinator. The other model was the U.S. Trade Representative, Office of Management and Budget, the Drug Office, and—I can't think—I think there's one other. But—Science Technology, that's right. These are all presidential-appointed, Senate-confirmed, and it provides them with the status and the ability to have some authority—and budget review authority is part of it—over the range of cyber-involved agencies in the Federal Government.

Senator MANCHIN. Who do these agencies report to now, Senator? Right now. Who do the heads of these agencies, when there is a cyberattack——

Senator KING. Well, they—they're—they would report directly to the President. There's no cyber coordinator. That's the whole problem.

Senator MANCHIN. So, this is, basically, the coordinator you're talking about.

Senator KING. Yes. There was a cyber—one of the arguments is, well, this was—traditionally been a position in the National Security Agency as an appointed position by the National Security Advisor. The problem with that is, it's at the whim of any particular——

Senator MANCHIN. I gotcha.

Senator KING.—National Security Advisor. Two years ago, this position was eliminated by the then National Security Advisor. That's why we're saying, let's elevate this to the status and the organizational status that it needs in order to be effective to defend the country.

Senator MANCHIN. General Inglis, being the military person you are, the Commission report specifically rejected the idea of deterring cyberattacks on critical infrastructure by threatening retaliation against the attacking country's critical infrastructure. So, I understand the desire to be reserved, but how do you feel your—this recommendation is going to be adequate to deter?

Brigadier General INGLIS. Well, first, if I might go a half-step back and answer another question that you asked——

Senator MANCHIN. Okay.

General Inglis:—which was a concern about whether sector-specific agencies might then be thwarted in the intimate and direct relationship they have, very profitably, in terms of outcomes, with their respective sectors. The Commission actually is with you on that. We actually want to strengthen the sector-specific agencies' relationships and allow them, as representatives of the Government, to, on their various faces, continue that strength, and so, the National Cyber Director should benefit from that, but never constrain that; should, essentially, take advantage of that.

To your question about whether the Commission believes it is appropriate or inappropriate to attack the critical infrastructure of other nations, I think that our views on that are perhaps more nuanced than a yes or a no. We would start by, first, saying that we believe, as the United States has long attested, we will follow international law, and we will adhere to the global standards of normal behavior that we attested to in 2015 through the auspices of the State Department, that we wouldn't, in peacetime, attack the critical infrastructure of other nations. That being said, in wartime, it is a political decision of the leadership of this Nation to determine, with necessity and proportionality, how we should array the various instruments of national power that we bring to bear. We shouldn't be in a place where we never say never, we just need to follow the rules of proportionality and necessity and the international laws that govern such things.

I would offer, though, that it's often a discussion that takes place with respect to the use of force or armed attack. What we have found is that our adversaries are operating well below that with impunity; essentially, like termites in the woodwork——

Senator MANCHIN. Right.

General Inglis:—as opposed to this flash and bang that might kind of be effected through kinetic weapons.

Senator MANCHIN. I gotcha.

Brigadier General INGLIS. What we then have to address is whether or not our adversaries are taking inappropriate advantage of our either complacency or perhaps our implicit tolerance of them inserting themselves into our critical infrastructure, and how do we stop that. You know, I think that there are an array of——

Senator MANCHIN. Yes.

General Inglis:—methods, some of which include cyberpower. But, the use of diplomacy, the use of legal methods, the use of, perhaps, public shaming, all of those need to be brought to bear to stop that and to hold them at risk in ways that follow international law, that use necessity and proportionality.

Senator MANCHIN. If I could ask one final question to Congressman Gallagher.

Congressman, I think, in your opening statements, you all have laid out a significant number of Commission legislative recommendations. Am I correct that each of these recommendations that you described appear in some form in either the House or Senate NDAAs, and they'll be part of the issues in play in our conference of the NDAA? So, it's—the Commission's report, the recommendations you make, are they in both?

Representative GALLAGHER. There were——

Senator MANCHIN. Congressman Gallagher?

Representative GALLAGHER. Yes, there were six specific recommendations that I talked about that were—are in the House version of the NDAA, but not in the Senate version of the NDAA. I brought that up just to urge the Senate to consider the House equities when we're in that discussion. I believe there is some ongoing debate about our continuity-of-the-economy proposals. I understand, for various jurisdictional issues in the House and the Senate, there are some other recommendations that made it into neither report. But, we feel fairly good about just the—sort of the baseline of what made it into either the House or the Senate, and hope there is a, you know, collaborative approach in the conference committee processes.

Senator KING. Senator Manchin, I can present to the Committee a chart that exactly answers your question. There are 12 of our provisions in the House National Defense Act that aren't in the Senate version. Okay? There are 12 in the House that aren't in the Senate version. There are 11 in both the House and the Senate versions. So, they match. Then there are six in our version that aren't in the House. So, all together, let's see, we've got 29 provisions, of which 11 are in both and another more than a dozen can be, and hopefully will be, resolved in the conference.

Senator MANCHIN. Are they outside of the jurisdiction? Is that the problem that we have? Some of those are outside the jurisdiction?

Senator KING. No, these are all, we believe, close enough so that——

Senator MANCHIN. So, they can be considered in to the——

Senator KING. Yes.

Senator MANCHIN.—conferees.

Senator KING. Yes. Yes, sir.

Senator MANCHIN. You think that will all be—all 29 will be in play.

Senator KING. Yes. So, they're in the bill, and we hope that they can resolved so that as many as possible—I mean, you know——

Senator MANCHIN. Yes.

Senator KING.—we all know what happens with Commission reports. We were determined to not have that happen.

Senator MANCHIN. I gotcha.

Senator KING. That's why we actually drafted legislation rather than just give you ideas. If we can finalize these documents in the—these amendments in the bill as it comes out of the conference committee, we will have done well more than half of our total recommendations.

Senator MANCHIN. Thank you all. I appreciate it very much.

Senator ROUNDS. Thank you.

Yes, just in looking back over the numbers of—that I have got in front of me, it's been great to see the number of them that were actually put into the—this Subcommittee's mark, and then the other three that were added on the floor. We couldn't do them in Subcommittee, because of jurisdictional issues, but—so, that was good to see, I think, 14 total coming out of the Senate, and then holding a spot for the discussion on the National Cyber Director position, as well. So, I think the Committee has been very successful, and you've done some great work.

Just to follow up a little bit, I did start out—when I first got onto this Committee, I was very interested in a National Cyber Advisor of—or National Cyber Director. Then I kind of came around a little bit, saying there—the one thing I was concerned about is, is that things were starting to work within the Department of Defense. We were actually having some movement forward, getting some things done, and I was concerned that we not create any silos. I am very happy to hear all of you indicate the same, that it is not the intention, and the legislation should not be there, to create that. But, there is clear evidence that the Congress has, in the past, asked for Senate-approved members to advise the President or to participate in the executive branch. I just thought I would take a minute just to make that point here.

Examples of such positions that currently exist, that Congress has put into law, top leaders of the Office of Management and Budget, the Director, the Deputy Director, the Deputy for Management, the Controller, the Office of Federal Financial Management, OMB; Administrator, Office of Information and Regulatory Affairs, OMB; Administrator, Office of Federal Procurement Policy, OMB; Director of Office of National Drug Control Policy; top leaders of the Office of Science and Technology Policy, including the Director and the Associate Directors; Intellectual Property Enforcement Coordinator; Chairman, Council of Economic Advisors; Chair and Members, Council on Environmental Quality; top leaders of the Office of the United States Trade Representative, including the United States Trade Representative, Deputy United States Trade Representatives, Chief Agricultural Negotiator, Chief Innovation and Intellectual Property Negotiator. I understand that, really, a lot of the language that you've put into this proposal comes from

the legislation authorizing and directing the United States Trade Representative, as well. So, there is a format that's been followed here that we can look at to see whether it's successful, or not, in terms of advising the President of the United States.

So, I think you've done your work on it, and most certainly, I would—if there's any part of it, as I say, that we were concerned with, it was that we make sure that we allow what is working within cyber operations of the DOD to continue to work, and that we not create any other silos.

The other thing the Committee—that the Committee talked about a little bit was the direction with regard to our activity in cyberspace, whether there should be—you know, what type of deterrence should be used, whether we should be putting more emphasis on defensive activity, making it more difficult for our adversaries to get in. I would just like to take just a minute, because I—just to give you the opportunity to share a little bit about your thoughts regarding the operations in cyberspace. You've got air, land, sea, space, and cyberspace, and most certainly, the most inexpensive of any to get into and to create havoc everyplace else is cyberspace. We have to be on top of our game. Can you share with me a little bit your thoughts about the questions, concerns that your Commission found or that you wanted to express and maybe haven't had the opportunity to do so, so far?

Senator KING. Thank you, Mr. Chairman.

There are a couple of aspects. One I want to touch on very quickly. One of our major recommendations, which isn't before this Committee, but—is for the creation of an Assistant Secretary of State for Cyber, because international norms and expectations are an important part of this discussion. If we're not at that table, we can lose—when they are talking about standards or whatever, this is a place where we've lost some ground. So, that's one of our recommendations.

But, I think the—what I would like to say about the deterrent issue is that this was a—there was a great deal of discussion about this, and it grow—it grew, for me, out of many of the hearings that you and I have sat through 4 over the last 4 or 5 years, where we haven't had a deterrent policy. We've been purely defensive. What we are saying is that there's a level—everybody knows that there would be a response if there was an attack on critical infrastructure. But, the question is, What happens if there's an attack on our election, or what happens if there's wholesale theft of intellectual property? What's the response? Because there hasn't been, and because, as you point out, this is a cheap way to make war, then we've become a cheap date. We've become an easy target. What the Commission suggests is, there needs to be a new declaratory policy that there will be a response. It may not be cyber. It may not be kinetic. It may be sanctions. It may be any part of the national power toolkit, but that there will be a response.

Another sort of wrinkle of this that's very important is, 85 percent of the target space in cyber is in the private sector. It's not the Army and the Air Force. They will be under attack—cyberattack. But, the target space is in the private sector. That's where we have to really develop relationships. This is a whole new way of thinking. One of the things we talk about is the intelligence

agencies being able to share with the private sector what they're learning about cyberattacks on SCADA systems at power plants.

So, you're absolutely right, the discussion of the deterrent idea was an essential part and a lot of discussion in the Commission, but we concluded that there had to be some deterrent. It can't simply be defensive, patching, make it more difficult, cyber hygiene. All those are important, but we wanted our adversaries, when they're contemplating a cyberattack on the United States, to say, "But, what will they do to us?" We want that to be part of their risk calculus.

A formative moment for me was when we were interviewing the head of National Security Agency (NSA), 3 or 4 years ago in this Committee, and I asked him if there was any deterrent to the—a foreign adversary taking these kinds of actions. His answer, I have never forgotten, was, "Not enough to change their risk calculus." That, to me, is a—is an admonition and a warning to us that we have to, not only defend ourselves, but we—our adversaries have to know that we can and will respond in such a way as to make them regret their attack.

Senator ROUNDS. Thank you, sir.

I am going to turn it over to Senator Manchin.

Senator MANCHIN. Mr. Inglis, one of the Commission's recommendations that was included in the Senate NDAA is to have the Defense Department carefully and comprehensively assess whether the Cyber Mission Force, our military cyber forces, are rightly sized. We included the 6 recommendation in our bill, and it is important. Frankly, this mission is so new, and we had to create everything from scratch 10 years ago. No one really knew how many people it would take to perform this mission, or even, really, the exact mix of skills we needed to get the job done. But, as you know, we also realized that Cyber Command can only get after targets, and clever people can figure out to get inside that target through cyberspace and, if we have infrastructure in the right places, to get access to it. These are really high-end skills, and enabling accesses requires a lot of smart planning by a lot of smart people. If you don't have the accesses to military targets, adding more cyber units are not going to accomplish much.

So, my question is, Did the Commission examine whether Cyber Command has difficulties recruiting, training, and retaining enough people with the requisite skills to generate accesses to support an expansion of the cyber forces?

Brigadier General INGLIS. I think that we did look at that, nationally and then within the various components that constitute those who employ cyber workers within the United States Federal bureaucracy. Our sense of United States Cyber Command is, they've done a great job within the authorities that they have of recruiting, training, and developing for careers the people necessary to do the work that they do. But, as you well know, those forces were set in size in the year 2013. I think we're sitting now with a combined size of that force, the actual, kind of, pointy-end of the force, about 6200, 133 teams, sized in a time and place when our sense of how we use military cyberpower was different, in a time and place when the sense of where that should be used was different. It's time to review that. It's time to take a look at that.

But, to your point, we need to also, at the same time, make sure that we've done everything necessary to create a bigger pie from which we can recruit, and, once we recruit, to focus hard on: How do you retain those people across careers in cyber disciplines?

Senator MANCHIN. If I could follow up with Congressman Gallagher on that.

Congressman, your Commission did make a recommendation that you have not emphasized here today, or Senator King, and, I assume, because it did not get much serious consideration here in Congress. That recommendation is that the House and Senate should establish select committees on cybersecurity, with members drawn mostly from all the committees, and each member that has significant jurisdiction over our national cybersecurity problem. So, maybe next year you can give it another try and see if that goes anywhere. If you want to comment on that, I am happy to 8 hear.

Representative GALLAGHER. Well, I understand the difficulties of trying to reform committee jurisdiction in both the House and the Senate. We view this as a critical recommendation. It was one that we spent a lot of time debating as—just as we want that single point of focus within the executive branch, that person who wakes up every single day thinking, How can we defend the country in cyber? So, too, I think we want a repository of legislators who have the ability to develop true cyber expertise, can hold that person, as well as the other people in the executive branch that work on this issue, accountable, and just creates a space where the executive branch and the legislative branch can work together to keep the country safe. So, I understand the difficulties of this proposal, but I view it as necessary. It's one drawn from Congress's own history of creating permanent select committees on intelligence.

The final thing Iwould say, Senator, is that I think the most forceful advocate for this proposal was my colleague in the House, Congressman Jim Langevin, who presumably has the most to lose, jurisdictionally, given that he chairs the HASC Subcommittee that is analogous to your Committee, and therefore—but, you know, might lose some jurisdictional power. But, he feels very strongly about this proposal, as well.

Senator MANCHIN. Thank you.

Senator King, you might want to follow up, if you will, real quick, on—let me ask you something else.

Senator KING. Well, first, I wanted to——

Senator MANCHIN. Okay.

Senator KING.—follow up. I think, to illustrate the difficulty of the congressional organization, in order to get—I gave you the list of those amendments that had been cleared and put in—we had to get 180 clearances from both sides on multiple committees and subcommittees. I mean, that gives you a flavor of how bifurcated—there's got to be a word—fractioned, or fractured, the congressional process is. So, that's something that we're going to continue to work on.

The analogy is, the Intelligence Committee, which was created in 1976 for the same reason, there was a realization that intelligence was scattered throughout the Federal Government and throughout the Congress, responsibility, and it made sense to put it into one set of expert hands. That's the origin of the Intelligence Committee.

We think the same thing should be done here, and I will continue to pursue the idea.

Senator MANCHIN. With all the expertise you all had on your Commission—it seemed like you had a wide range of people coming from different walks of life that had expertise to add—what was the greatest concern, if we can talk about—maybe we can't in this type of a setting—but, the greatest concern you had with our cybersecurity right now, and what our adversaries are trying to do to us on a daily basis, of the vulnerability we might have that you was really concerned about? Or did all of you agree you had one highly concerned sector of our society that was vulnerable?

Senator KING. I can't identify one sector, but critical sectors, one that doesn't get enough attention, is water. Our water system, there are something like 50,000 different water companies——

Senator MANCHIN. Yes.

Senator KING.—in the United States, and there are vulnerabilities there; all of our financial system, our telecommunication system; of course, electrical energy. This is ongoing. We've talked to utility executives, for example, one of whom told us his system was attacked 3 million times a day.

Senator MANCHIN. Jesus.

Senator KING. Three million times a day, and that gives you the range. Banks, I know, the same—I don't know if it's the same number, but hundreds of thousands of times a day. So, this is an ongoing threat, not only from State actors, but from malign actors who are doing ransomware, sometimes they're just garden-variety crooks, but they're also people that want to undermine our society.

So, I can't give you one specific target that we most worried about. I think our worry was that we just didn't feel that the country was adequately prepared for what could, and likely will, happen.

Brigadier General INGLIS. Sir, could I speak to that, too, then——

Senator MANCHIN. Of course.

Brigadier General INGLIS.—you know, building on that, just to say that there is the insidious threat, which is that our concern was that our adversaries—whether they be criminals or nation-states, or those in between, it could beat one of us, without garnering the attention or the response of the rest of us. We actually have a situation where we've been divided, and we're slowly being conquered one at a time, "The hole's not on my side of the boat, therefore I am not going to help you kind of patch the hole on your side of the boat."

Our view is—and you won't find this line in the report, but if I was stuck in an elevator with somebody and had 10 seconds to get out, what we propose is that, if you're an adversary in this space, henceforth, you're going to have to beat all of us to beat one of us. That actually derives from using all of the talent, all of the expertise, all the authorities that we already have in a more coherent, more joined-up fashion, preparing as one, applying those resources as one, such that, when we execute this in a distributed fashion, much like the Department of Defense has, we're giving the freedom to operate, we know that we're operating according to some larger strategy, consistent with some larger purpose, and that we're help-

ing whatever is to the left of us, to the right of us. That's a fundamental problem for us at this moment in time.

As we made the rounds over 400 different engagements, most of those in the private sector, we heard time and again from the private sector, "I like the part of government that I have an interaction with"—maybe it's a sector-specific agency—"but I am not sure I know what the government strategy overall is. The government's not joined up and, therefore, not in a position where it can be a viable collaborator with me, the private sector, who is bearing, then, the burden of this, kind of, transgression after transgression." They want the government to be joined up, they want it to be coherent, they want it to be a viable partner at the same speed that they enjoy on the edge that they approach that government.

Senator MANCHIN. Thank you.

Senator ROUNDS. Look, I want to take this time to just say thank you to all of our participants. This is critical, that we get this right. Today, I think there's an understanding, somehow, that the Department of Defense has a role to play with regard to coming in and working internally within the United States to defend, and yet they can't really step in unless they coordinate with Homeland. Homeland, basically, requests, and then DOD can, but it's almost like if—in terms of an analogy, if you have archers on the outside shooting arrows in, you can work all day at trying to catch each arrow that's coming in—and you're talking millions of them—or at some point, you have to go after the archer. The challenge on it is, defensively and offensively, how do you do that in the best way possible?

I can't say enough about how important I think it is that the work that you've done on the Commission be recognized, and that we do our best to incorporate what we can into the NDAA.

The second piece that I think we have to recognize—and I want to thank Senator Manchin for being here today—we had a number of other members who were here early on, and then had to leave. It's multiple meetings at the same time. But, we shouldn't leave without recognizing how far our cyber teams have come in just the last few years. The way in which General Nakasone and those teams have really stood up what has been an impressive series of achievements, both offensively and defensively, and yet they will tell you it's still so much more work to be done. Everything we can do to provide them with the tools that they need and the correct public policy that they need in order to do their job, the better off we're going to be. Every other domain, whether you're talking air, land, sea, space, all of them are dependent on our ability to protect them in cyberspace, because it's all connected. It's the least expensive way for our adversaries to get in and actually do damage in any one of the other domains, and so, we have to pay attention to it.

I think the work that you've done is to be commended, and we appreciate your time today.

Senator Manchin, any final thoughts?

Senator MANCHIN. No, I appreciate all the work. I know there's an awful lot of effort that you all have put in this for quite some time, and I appreciate it very much.

Having served with Senator King on Intel Committee, it's kind of opened our eyes. There's a lot of concerns we have. We're still very good at what we do, but we can be a lot better and make sure that we can protect the American people the best we can.

My only thing was—I was wanting to ask the question on—do you see the private sector starting to harden up a little bit? Are we communicating with them well enough to let them know they have a responsibility to harden up, also?

Senator KING. The answer is yes. I would include, when you say "the private sector," also the States, the public—the election system, for example.

Senator MANCHIN. Are they looking to us—I guess, Senator King—are they looking to us, basically, to do it all for them, or do they understand they've got to come to the table, too?

Senator KING. No, no, they're very much engaged in their own——

Senator MANCHIN. Okay.

Senator KING.—in their own processes. But, as I said, this—because 85 percent of the target space is the private sector, and the Chairman, in his very opening remarks, said that we're here to defend the Nation. We've got to help defend them, but they have to——

Senator MANCHIN. Yes.

Senator KING.—do their part.

Senator MANCHIN. Yes.

Senator KING. Building those relationships is very much a part of what we're trying to establish. It's happening, I can assure you. But, we're not there yet.

Senator MANCHIN. Thank you all.

Thank you very much.

Senator ROUNDS. With that, I would like to say thank you to our witnesses today: Senator Angus King, The Honorable Michael Gallagher, and Brigadier General John Inglis, Retired. Thank you, to all of you, for your testimony.

With that, this Subcommittee meeting is adjourned.

Thank you.

[Whereupon, at 3:43 p.m., the SubcCommittee adjourned.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR DAVID PERDUE

POTENTIAL LIABILITY IN THE EVENT OF A MAJOR CYBER ATTACK

1. Senator PERDUE. Mr. Inglis, during a cyber-attack or a physical attack on a critical lifeline sector, the Federal Government may need to order private-sector entities to act (or refrain from acting) alongside the Government to stop the attack. Private-sector companies and utilities in these instances may want to cooperate and often do cooperate in these instances; however, they often assume legal risk in doing so. Recommendation 3.3.2 of the Cyberspace Solarium Commission discusses this issue. It recommends that Congress "clarify liability for Federally directed mitigation, response, and recovery efforts," in order to ensure that our critical lifeline sectors face no barriers whatsoever in cooperating with our Government during a cyberattack. Do you think that there are currently barriers for private-sector companies who are a part of a critical lifeline sector to cooperate with the U.S. Government during a cyberattack or physical attack, and if so, what are those barriers?

Mr. INGLIS. The lack of pre-event planning, trust building activities and substantive collaboration leaves both sides (private sector and USG) without needed relationships and muscle memory to collaborate at speed during a crisis. While Con-

gress made strides towards this end (and attendant liability) with the Cybersecurity Information Sharing Act of 2015, there is still significant resistance to information sharing, trust, and cooperation. We should now work even harder to ensure government held information is shared with the private sector.

The Commission recommends building a more robust system for private-public collaboration, through several recommendations such as establishing an Integrated Cyber Center within the Cybersecurity and Infrastructure Security Agency (CISA) (Recommendation 5.3), creating a Joint Cyber Planning Office (JCPO) (Recommendation 5.4) to coordinate cybersecurity planning and readiness across the Federal Government and between the public and private sectors; establishing and funding a Joint Collaborative Environment (Recommendation 5.2) for sharing and fusing threat information; and establishing authority for CISA to threat hunt on .gov networks (Recommendation 1.4). These all also can work in concert to create a more resilient infrastructure, a significant improvement from what we have today.[1] We can't continue to bank on our ability to forge and leverage coalitions after a cyber campaign is initiated by an adversary. That would condemn us to start and stay behind an adversary who has the advantage of having pre-planned the time, place and manner of their attack. Improving intelligence support to the private sector and codifying processes for identifying private sector cyber intelligence needs and priorities would markedly improve situational awareness across critical infrastructure and allow private sector partners the insight necessary to defend their networks. Identifying the key partners can be done, as we recommend, through a process which identifies and empowers Systemically Important Critical Infrastructure (SICI) entities to this end. As key partners in protecting America's critical infrastructure, the private sector must have full awareness into the severity of the threats we face.

2. Senator PERDUE. Mr. Inglis, how big of a threat is litigation in discouraging private sector companies from complying with an order or request from the U.S. Government during an attack?

Mr. INGLIS. An order based on law or similar (enforceable) executive branch authority is likely sufficient to motivate compliance. However, it is often too late to request information during an attack if it is to be useful to guide efforts designed to counter and curtail that attack. Pre-attack data exchanges are the key to resolving this issue.

To address this shortcoming, Congress should pass a law codifying a "Cyber State of Distress"—a federal declaration that would trigger the availability of additional resources through a "Cyber Response and Recovery Fund"—to assist state, local, tribal, and territorial governments and the private sector beyond what is available through conventional technical assistance and cyber incident response programs (Recommendation 3.3). Creating this emergency declaration would resolve any concerns private industry would have about litigation in response to complying with a request from the government after an attack, as the Stafford Act has done through government directives requiring private sector action during national emergency declarations for natural disasters. The declaration would be used exclusively for responding to, or preemptively preparing for, cyber incidents whose significance is above "routine" but below what would trigger an emergency declaration and for incidents that exceed or are expected to exceed the capacity of federal civilian authorities to effectively support critical infrastructure in response and recovery.

The fund would be used to augment or scale up government technical assistance and incident response efforts in support of public and private critical infrastructure. A key provision is the inclusion of preemptive action and preparation, which accounts for instances when the Federal Government has a reasonable expectation that a significant cyber incident is likely to occur and preemptive action and preparation would reduce potential consequences of disruption or compromise. The declaration would invoke current authority that establishes the Secretary of Homeland Security as the principal federal official responsible for coordinating incident response, recovery, and management efforts on behalf of the entire Federal Government. In addition to addressing response and recovery efforts, this coordination would need to account for, and protect, law enforcement interests, including the preservation of forensic data necessary to attribute the attack and enable subsequent investigations by law enforcement agencies. This coordination role should not supersede other existing department and agency authorities or direct law enforcement activity.

---

[1] All four of these recommendations: the Integrated Cyber Center, the JCPO, the Joint Collaborative Environment, and CISA threat hunting on .gov are only included in the House Fiscal Year 2021 NDAA.

3. Senator PERDUE. Mr. Inglis, do you believe the current statutory framework provides enough of a liability shield for companies that do comply with U.S. Government orders or requests, and if not, what should we take into account as we update this framework?

Mr. INGLIS. The statutory framework for liability coverage for private companies working with the U.S. Government is necessary in order to ensure strong coordination and cooperation between the private sector and the U.S. Government in response to cyber attacks. If the United States were to suffer a significant cyber incident, the Federal Government would undoubtedly require the assistance of private-sector partners in response and recovery. Existing laws to facilitate these activities, such as the Defense Production Act and Federal Power Act, are limited in their ability to provide reliable liability protections for private-sector entities or public utilities that take action, or refrain from taking action, at the direction of the Federal Government. When the Federal Government orders a private entity to take action or refrain from taking action in pursuit of national cybersecurity, shielding that entity from liability related to that action or inaction is crucial.

Building better public-private collaboration will require more active and deeper collaboration between the Department of Defense (DOD) and other federal departments and agencies and private-sector stakeholders, including owners and operators of systemically important critical infrastructure. DOD brings considerable resources, expertise, and advanced capabilities that, when integrated appropriately with new or existing public-private initiatives, can substantially increase the timeliness and effectiveness of U.S. cyber defense and security efforts. The Commission recommends that the executive branch establish a Joint Cyber Planning Cell (Recommendation 5.4) under CISA to coordinate cybersecurity planning and readiness across the Federal Government and between the public and private sectors; joint cyber exercises (Recommendation 3.3.4), intelligence community support (Recommendation 5.1.2), strengthen the Office of the Director of National Intelligence's (ODNI) Cyber Threat Intelligence Integration Center (CTIIC) (Recommendation 1.4.1), and DOD's Integrated Cyber Center and Joint Operations Center (ICC/JOC); strengthen an Integrated Cyber Center within CISA (Recommendation 5.3), and sector-specific agency (SSA) interaction vis á vis the creation and designation of systemically important critical infrastructure (SICI) (Recommendation 5.1).

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) ADVISORY COMMITTEE

4. Senator PERDUE. Mr. Inglis, the Cyberspace Solarium Commission recommended that the Secretary of Homeland Security establish a "Cybersecurity Advisory Committee to advise, consult, and make recommendations to CISA on policies, programs, and rulemakings, among other items, to account for non-Federal interests." Currently, CISA has no formal channels through which the private sector can share information with CISA about cyber threats to our critical infrastructure. I introduced a bill with Senator Kyrsten Sinema to fix this problem. It creates a formal channel for the private sector and our Government to share threat information. It will also ensure that critical insights into our cyber threat environment and develop best practices for deterrence and detection. I am proud that it was included in the National Defense Authorization Act (NDAA) that we recently passed out of the Senate. How important is this provision to achieving that goal of information sharing?

Mr. INGLIS. The Commission fully supports the "Cybersecurity Advisory Committee" provision as it went through the Senate and the Commission's House of Representative members plan to support the motion in the NDAA conference. In addition the Commission believes the U.S. Government has a unique capacity to take in information from disparate sources, including the intelligence community, and integrate that information to produce a more holistic picture of and better insights into the national collective understanding of threats, building on the good work of CISA and the Automated Indicator Sharing (AIS) program. Building on those strengths, Congress should review and update intelligence authorities to increase intelligence support to the broader private sector (Recommendation 5.1.1); establish and fund a Joint Collaborative Environment, a common and interoperable environment for the sharing and fusing of threat information, insight, and other relevant data across the Federal Government and between the public and private sectors (Recommendation 5.2); expand and standardize voluntary threat detection programs (Recommendation 5.2.1); and direct the executive branch to strengthen a public-private, integrated cyber center within CISA in support of the critical infrastructure security and resilience mission as well as conduct a one-year, comprehensive systems analysis review of federal cyber and cybersecurity centers, including plans to develop and improve integration (Recommendation 5.3).

5. Senator PERDUE. Mr. Inglis, what steps can we take to ensure that we're using the expertise of the private sector to protect our cyberspace?

Mr. INGLIS. The private sector, which owns and operates 85 percent of our critical infrastructure and constitutes the lifeblood of our economy, is both an essential partner in our efforts to protect our cyberspace and a main target of adversary cyber operations.

First, we need to foster public-private collaboration to address threats to shared digital infrastructure. The private sector will be more willing to contribute their expertise when the goal is one of common interest. The Commission recommends the creation of a Joint Collaborative Environment to share and fuse threat information, insight, and other relevant data between public and private sectors (Recommendation 5.2); a review of intelligence authorities to increase intelligence support to the broader private sector (Recommendation 5.1.1); the expansion and standardization of voluntary threat detection programs (Recommendation 5.2.1); and the strengthening of a public-private, integrated cyber center within CISA (Recommendation 5.3). Each of these proposals would both enable the Federal Government to better protect the private sector and its assets, and enhance the government's ability to learn from and leverage the expertise of the private sector.

Second, exchange tours between public and private sectors will provide opportunities to deepen this collaborative relationship. In addition to facilitating greater communication and trusted relationships between sectors, such a program would enrich the knowledge base of both sectors, as they gain greater experience in a range of circumstances and encounter variances in threats and tools. This type of ongoing learning opportunity will enhance our cyber workforce by enriching career paths, keeping employees engaged, increasing retention. For these reasons, the Commission recommends a public-private talent exchange program (Recommendation 1.5).

Finally, the Commission supports your recommendation for the creation of a Cybersecurity Advisory Committee (Recommendation 1.4), "to advise, consult, and make recommendations to CISA on policies, programs, and rulemakings, among other items, to account for non-federal interests." Having a formal channel for the private sector to engage with the Federal Government on cybersecurity matters is essential. This will streamline the sharing of information between both sectors and better inform the policies, programs, rules, and regulations that CISA makes.

6. Senator PERDUE. Mr. Inglis, how can we ensure that the Federal Government remains agile enough to respond to our rapidly evolving threat environment?

Mr. INGLIS. We can do so by creating needed coherence of vision through the development of a viable national strategy, and by allocating and collectively exercising appropriate roles and responsibilities to the various departments, agencies, and private sector organizations. This will ensure that we have the cohesion of relationship and unity of effort to adjust on-the-fly to cyber crises. As Eisenhower said, "The plan is nothing. Planning is everything." To that, the Commission would add that the muscle memory and inherent agility of a coalition comes from exercise-derived from the shared work of addressing contingency and crisis and exercises that stress and strengthen plans and relationships across a broad range of scenarios.

The United States must also practice constant vigilance analogous to the DOD's "persistent engagement" strategy across all instruments of national power—to include private sector—with the goal of continuous situational awareness, early discernment of cyber threats, and early and collaborative action to address cyber threats. This can be accomplished through the creation of a Joint Collaborative Environment to share and fuse threat information, insight, and other relevant data between public and private sectors (Recommendation 5.2); strengthening an integrated cyber center within CISA (Recommendation 5.3); strengthened SSAs (Recommendation 3.1), and threat hunting on the DIB and .gov (Recommendations 6.2.2, 1.4).

Investing in human capital will also ensure we broaden the base of talent (both within and external to government), moving away from a strategy reliant on the relative few cyber defenders and towards a strategy where every person play some role in the defense of cyberspace, taking a lesson from the United States Marines Corps who make a similar point in their mantra that "*Every* Marine is a rifleman . . . "

7. Senator PERDUE. Mr. Inglis, with your background at the National Security Agency (NSA), do you think it's important for the private sector to share threat-information with the Federal Government?

Mr. INGLIS. Yes. The Federal Government has assets that can be better employed if it knows more about the threats operating against or inside of private sector assets that the Federal Government cannot, and does not want to, surveil. Consider the example where an information sharing and analysis center (ISAC) relays to the Federal Government that it is experiencing an unusual rate or kind of activity. The

Federal Government would then use its lawfully assigned intelligence powers to reconcile that activity to a particular source beyond the visibility or authority of the private sector. Such sharing from private to public sector allows the public sector to orient and focus on matters that are more closely aligned with private sector needs.

However, the Cyberspace Solarium Commission believes that threat information sharing should not be a one-way street. The private sector is on the front lines protecting our nation's critical infrastructure and the systems that underpin it. We believe that information sharing should be a truly joint collaborative effort between the government and the private sector. This means integrating public and private cyber defense efforts as well as ruthlessly prioritizing government support to private entities.

The Federal Government should not be a black hole to the private sector. Collaboration in threat information sharing can build better situational awareness of cyber threats which can then inform the actions of both the private sector and the government. The U.S. Government has a unique capacity to take in information from disparate sources, including the intelligence community, and integrate that information to produce a more holistic picture of and better insights into the national collective understanding of threats. The CSC has a number of recommendations, most notably codifying systemically important critical infrastructure" (Recommendation 5.1), improving intelligence support to the private sector (Recommendation 5.1.1), strengthening and codifying processes for identifying broader private sector cybersecurity intelligence needs and priorities (Recommendation 5.1.2), and establishing a Joint Collaborative Environment for the sharing and fusing of threat information between the public and private sectors to make collaboration truly joint (Recommendation 5.2).

8. Senator PERDUE. Mr. Inglis, what has the relationship between the private-sector and our Federal Government looked like previously on cybersecurity issues, and how can we strengthen that relationship going forward?

Mr. INGLIS. The Commission devoted considerable time and energy to engaging with the private sector to solicit their feedback on the efficacy, or lack thereof, of public-private collaboration on cybersecurity issues. We found that many in the private sector perceive the Federal Government as incoherent and unable to synthesize the many aspirations and capabilities of government into a cohesive, approachable framework.[2] To address this issue, the Commission recommends the creation of a National Cyber Director (NCD) to coordinate existing federal cybersecurity strategy and policy (Recommendation 1.3); the designation and codification of systemically important critical infrastructure (SICI) to better prioritize and protect our most critical private sector assets (Recommendation 5.1); and the establishment of Continuity of the Economy (COTE) planning to ensure the public and private sectors, in tandem, are prepared to rapidly restart and restore the U.S. economy in the aftermath of a major disruption (Recommendation 3.2).

On the issue of information sharing, specifically, members of the private sector felt that this was a one-way street. While they were expected to, and often made efforts to share threat information with the Federal Government, the information they received was often out-of-date or simply rehashed the same information that was originally provided by the private sector to the government. The Commission recommends the creation of a Joint Collaborative Environment to share and fuse threat information, insight, and other relevant data between public and private sectors (Recommendation 5.2); a review of intelligence authorities to increase U.S. Government intelligence support to the broader private sector (Recommendation 5.1.1); the expansion and standardization of voluntary threat detection programs (Recommendation 5.2.1); and the strengthening of a public-private, integrated cyber center within CISA (Recommendation 5.3). Each of these proposals would not only enable the Federal Government to better protect the private sector and its assets, they would enhance the government's ability to learn from and leverage the expertise of the private sector.

*While there is significant room for improvement, our conversations with the private sector did illuminate instances of success that we must emulate and expand upon. DHS and, in particular, CISA, is increasingly recognized as an effective convening authority for public-private collaboration. The Federal Bureau of Investigation (FBI) and NSA, similarly, are perceived as competent cyber organizations able to share valuable insights on threat actors and cybersecurity trends. The National Institute of Standards and Technology (NIST), as well as other enablers, are viewed

[2] To quote one observer: "Capability, will and authority for cyber action is seldom found in the same place within the Federal Government . . . never in peacetime and seldom even in crisis"

as trusted sources of information and guidelines, such as NIST's Cybersecurity Framework. Again, though, despite these isolated pockets of effectiveness, the whole of the government contribution to the private sector is certainly not seen as greater than the sum of its parts.

In short, the government must be more "joined up"—both to better employ its unique authorities and capabilities, and to be a more reliable and helpful partner to the private sector. It must be more proactive in offering its services and capabilities in support, through an accessible, efficient private-public collaboration system. It must be more aggressive in identifying and remediating the foundational vulnerabilities in the cyber ecosystem, not least of which is restoring a balance between actions—both good and bad—and consequences.

QUESTIONS SUBMITTED BY SENATOR MARSHA BLACKBURN

NATIONAL NUCLEAR SECURITY ADMINISTRATION

9. Senator BLACKBURN. Mr. Inglis, the Cyberspace Solarium Commission's report recommends the Department of Defense (DOD) undertake efforts to secure the defense industrial base (DIB), including hunting on DIB company networks. Can you think of a reason why the Commission's recommendations should not also apply to the National Nuclear Security Agency (NNSA) portions of the DIB, especially for contractors supporting nuclear weapons development?

Mr. INGLIS. No, I cannot. This is a good suggestion. A shared picture of the threat environment within the DIB is essential to proactively and comprehensively address cyber threats and vulnerabilities to this key sector, and that includes nuclear weapons development and maintenance. [3] Just as forother classified areas of the DIB, classification considerations can be addressed. Improving the detection and mitigation of adversary cyber threats to the DIB is foundational to ensuring that key military systems and functions are resilient and can be employed during times of crisis and conflict. The NNSA and nuclear weapons, as one of the most critical components of national defense, cannot be excluded from participation. Congress should therefore direct regulatory action that the executive branch should pursue in order to require companies that make up the Defense Industrial Base, as part of the terms of their contract with DOD, to create a mechanism for mandatory threat hunting on DIB networks (Recommendation 6.2.2).

The Commission recommends that Congress should legislatively require these companies to participate in a threat intelligence sharing program that would be housed at the DOD component level. A DIB threat intelligence sharing program should contain a number of key elements, including:

- Incentives for certain types of specifically delineated information sharing, such as incident reporting.
- A shared and real-time picture of the threat environment; joint, collaborative, and co-located analytics; and investments in technology and capabilities to support automated detection and analysis.
- Consent by DIB entities for the NSA to query in foreign intelligence collection databases on DIB entities [4] and provide focused threat intelligence to them, as well asenable all elements of DOD, including the NSA, to directly tip intelligence to the affected entity.

10. Senator BLACKBURN. Mr. Inglis, what are the unique challenges that would need to be overcome in order to holistically support the NNSA's industrial base?

Mr. INGLIS. Supporting the NNSA's industrial base is an important issue that goes beyond the immediate scope of the Commission's recommendations. Nevertheless, the Commission did promulgate a strategic objective of ensuring the security and resilience of nuclear weapons systems and functions, starting with Congress directing the DOD to conduct cybersecurity vulnerability assessments of all segments

---

[3] This recommendation applies to the DIB, defined as "[t]he Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development and design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements." This recommendation does not include entities such as Defense Critical Infrastructure (DCI), defined as "Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide." Office of the Chairman of the Joint Chiefs of Staff, *DOD Dictionary of Military and Associated Terms* (January 2020), 59, *https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.*

[4] These queries would examine collections already authorized against and focused on adversaries for references to or efforts against DIB entities.

of nuclear command, control, and communications (NC3) systems (Recommendation 6.2). Ensuring the cybersecurity of the NNSA's industrial base therefore plays an important role in contributing to the Commission's broader objectives with respect to the intersection of cybersecurity and nuclear capabilities.

Similar to the recommendations pertaining to the DIB, there are a number of unique challenges that would need to be overcome to support the NNSA's industrial base. Unlike the DIB, which has its own Information Sharing and Analysis Center (ISAC), NNSA should consider convening an ISAC-like entity to promote the sharing of threat information as well as best practices for security across the industry. Additionally, an executive entity could be identified to lead efforts to develop a holistic approach to securing the supply chain for all segments of the NNSA's industrial base, as well as to promote a risk-based approach to threat identified and hunting. Furthermore, NNSA could pursue initiatives in harmonization with the DOD's Cybersecurity Maturity Model Certification (CMMC) to categorize entities within the industrial base by relative levels of maturity and ensuring requirements for maintaining appropriate levels of cybersecurity. Finally, given the strategic significance of this industrial base, direction could be given for the prioritization of foreign intelligence collection against cyber threats to key entities within the NNSA's industrial base and protocols developed for rapid and meaningful sharing of information with affected entities to enable their defense. This type of relationship could be piloted through a Pathfinder-like program, similar to the DOD's Pathfinder programs established for the Energy and Financial Services sectors.

11. Senator BLACKBURN. Mr. Inglis, are there additional authorities needed from Congress to be able to support the NNSA's industrial base?

Mr. INGLIS. The Commission does not specifically address NNSA industrial base requirements and concerns, however, more generally speaking the Commission recommends a comprehensive strategy to ensure the continued availability and trustworthiness of critical technologies (Recommendation 4.6). Specifically, the Commission recommends a strategy that:

1. Identifies key technologies and equipment through government reviews and public-private partnerships to identify risk.
2. Ensures minimum viable manufacturing capacity through strategic investment and the creation of economic clusters.
3. Protects supply chains from compromise through better intelligence and information sharing.
4. Identifies and supports partners around the world and in the public and private sectors.
5. Ensures global competitiveness of American and partner companies in the face of Chinese anti-competitive behavior in global markets.

QUESTIONS SUBMITTED BY SENATOR KIRSTEN GILLIBRAND

ELECTION CYBERSECURITY BUDGET

12. Senator GILLIBRAND. Mr. Inglis, the Elections Assistance Commission is a small organization with a massive mission and its role continues to expand as it assists election officials in dealing with election security, aging and vulnerable technology, and accessibility in the lead-up to the 2020 elections. Elections are the cornerstone of our democracy, making election cybersecurity equivalent to national security. Unfortunately, election cybersecurity lacks a national security budget. How will the Commission's recommendations give the Election Assistance Commission sufficient authority, flexibility, and resources to help election officials face increasingly diverse and sophisticated cyber-threats?

Mr. INGLIS. The EAC suffers from chronic funding shortages and requires a more robust staff to better execute its responsibilities for improving State, Local, Tribal, and Territorial (SLTT) governments election cybersecurity capacity. Further, the EAC commissioners and staff require more technical cybersecurity expertise to enact urgent reforms to protect the integrity of voting systems against malicious cyber activity. Finally, increased funding for SLTT grants will help the EAC ensure SLTT election entities have the means to address cyber threats. By increasing and regularizing the EAC's funding and capacity and adding technical cyber expertise to the Commission, policymakers will ensure that evolving threats to the integrity of our electoral process are better understood and prioritized. Specifically:

- Congress should amend the Help America Vote Act to create a fifth nonpartisan commissioner and add a Senior Cyber Policy Advisor to the staff, both with established cybersecurity backgrounds in order to vote exclusively on issues of or

relating to cybersecurity and strengthen both the technical and cyber policy expertise of the commission.
- Congress should increase and regularlize the EAC's annual operating budget to enable the hiring of new staff to improve the performance of core responsibilities.
- Congress should streamline and modernize sustained grant funding for SLTT entities to improve election systems.
- The EAC itself should finalize and release its long-delayed update to the Voluntary Voting System Guidelines and increase the breadth and frequency of its recommendations and guidance concerning voting systems and processes.

INTERNET OF THINGS

13. Senator GILLIBRAND. Mr. Inglis, since the onset of the COVID–19 pandemic, Americans have relied on technology to stay connected, to do our jobs, and to see our friends and families. Many Americans have transitioned to remote work, often using personal consumer electronics to connect to work from home. Vulnerable personal devices and home networks present an attractive target with significant cybersecurity and data privacy risks. Can you please elaborate on how the Commission's recommendation to pass an internet of things security law will address the challenge of American consumers' widening dependency on global manufacturers with poor security practices who are based beyond American jurisdiction?

Mr. INGLIS. Outside the digital infrastructure common to businesses who build, operate, and defend systems for well defined business environments, Internet-of-Things (IoT) devices, have an outsized impact on security or insecurity (like the routers and smart home hubs common in the homes and other locations drafted as a substitute for traditional workplaces). Today, we know that many routers—and cyber-aware devices like lightbulbs, smart home hubs, thermostats and refrigerators—in peoples' homes do not include rudimentary or baseline security measures and the market for these devices has not yet moved to demand security. Recognizing this shortcoming in the market and the imperative of more secure IoT devices given their increasing importance in our economy and society, the Commission recommended the passage of an IoT security law that mandates minimum or baseline security measures for devices sold in the United States. These standards should be identified and developed in close coordination with relevant industry stakeholders to ensure that they neither place undue burden on the developers of these devices nor undermine innovation.

While the recommendation in our Pandemic report cannot wholly remediate a failure to build out IoT with security as an upfront goal, the sector is too important to not begin to redress those errors of omission and the increasing exploitation of malicious actors. Over time, a combination of government compellence and market forces will create a growing body of IoT that consumers can use with increased, if not absolute, confidence. Mitigation measures will be important throughout and even after this transition to ensure that improved analytics, threat sharing, and enforcement action reduces the benefits that accrue to bad actors across the realm of IoT.

NATIONAL GUARD INTEROPERABILITY

14. Senator GILLIBRAND. Mr. Inglis, the Commission recommended Congress enact legislation to clarify the cyber capabilities and strengthen the interoperability of the National Guard and assess the establishment of a military cyber reserve to provide a surge capacity that could be rapidly mobilized in a time of crisis. The United States currently suffers from a shortage of cybersecurity experts. The public sector faces the additional challenge of trying to recruit and train qualified experts in the field who are often lured to private industry by higher salaries. Can you please elaborate on how these recommendations could bolster the public cybersecurity cadre and what recruiting and retention benefits may be associated with these recommendations?

Mr. INGLIS. As a 20+ year veteran of the Air National Guard and an original sponsor of the standup of the MD ANG's cyber units, I was privileged to witness first-hand the multiplicative effect that Guard service has in leveraging precious skills that are nurtured in one sector, and honed in another. This effect is particularly true in peacetime when the unique authorities and missions of the military offer an attractive outlet to employ skills learned in the private sector, resulting in an exchange and growth of critically short expertise that would not happen in a zero sum world of stovepiped activities separated by the private-public sector boundaries. Despite the fact that the pay and benefits of the Guard and Reserves are easily outmatched by those available in the private sector, the flexible arrangements offered

make it possible for citizen-airmen and soldiers to lend their talents to one without shortchanging the other. Even in crises, the Guard's ability to work across federal (Title 10 and 50) and state (Title 32) boundaries is a great resource in establishing coalitions that derive strength from collaboration as much or more from literal numbers (put another way, if you have too few people to conduct a mission, they are best deployed in the flexible manner akin to what Guard and reserve service offers in leveraging members who hold roles in both the private and public sectors). It's also useful to note that few crises will require full-scale, nation-wide mobilization. The Guard's flexibility in deploying federalized assets across state lines is also useful to support crises that are localized to a particular region, without undermining the security of a region outside the crisis arena.

Moreover, you are completely right that the challenge of achieving effective security and defense in cyberspace depends on people as much as it does on technology or policy. Today, the U.S. Government suffers from a significant shortage in its cyber workforce. Across the public sector more broadly, one in three positions (more than 33,000) remains unfilled.[5] These shortages aredriven by a need for personnel that have specific cybersecurity skills and experience, but they are complicated by government hiring, training, and development pathways that are not well-suited to recruit and retain those personnel.

The good news is that today's cybersecurity skills and experiences can be gained with unusual ease outside standard channels of education and training. That means, however, that the government must more effectively take advantage of those unconventional pathways, especially when they do not include typical college education or prior government experience. Overall government approaches to successfully deepen and diversify this candidate pool should include:

- Developing programs to bring in new employees via apprenticeships, promoting cooperative study, and expanding training programs so that existing workers can enhance their career trajectories.
- Researching and implementing measures of competency alongside more commonly used certifications.
- Streamlining processes and reducing institutional barriers to onboarding cyber talent quickly.
- Identifying opportunities and building hiring pathways for members of underrepresented communities, including the neurodiverse,[6] women, and people of color.

To achieve these objectives for recruiting today's cybersecurity talent into public service, the government should pursue the following:

- Congress should fund research into the current state of the cyber workforce, paths to entry, and demographics in coordination with the ongoing work at the Office of Personnel Management (OPM), DHS, the National Science Foundation (NSF), and the National Institute of Standards and Technology (NIST). This research should align with and/or build on NIST's National Initiative on Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which outlines cybersecurity work roles and the knowledge, skills, abilities, and tasks involved in each role. New research should also build on emerging work from NICE and others on career paths and certifications.
- Congress should resource recruiting programs specifically designed to target cyber talent and expand current programs that have made demonstrated progress in innovating recruitment.
- Congress and the executive branch should reinforce and authorize the role of the NICE in coordinating U.S. Government efforts to advance cybersecurity workforce development nationwide, and resource the office sufficiently for this role.
- Congress should require the Government Accountability Office (GAO) to issue a report within one year: (1) estimating how frequently candidates are deterred from pursuing government careers because of delays in issuing security clearances; (2) assessing the effectiveness of current clearance processes at striking a balance between the national security risk of insider threats, and the national security risk of leaving cyber jobs vacant; and (3) recommending a lead agency for developing and implementing a plan for addressing any shortcomings discovered.

---

[5] "Cybersecurity Supply/Demand Heat Map," CyberSeek, Burning Glass, CompTIA, and the National Initiative for Cybersecurity Education, accessed February 18, 2020, *https://www.cyberseek.org/heatmap.html.*

[6] Kevin Pelphrey, "Autistic People Can Solve Our Cybersecurity Crisis," Wired, November 25, 2016, *https://www.wired.com/2016/11/autistic-people-can-solve-cybersecurity-crisis/*.

Upon entering government, cybersecurity personnel should have rewarding career paths and the education and training opportunities necessary both to keep their skills relevant and up-to-date in a rapidly changing field and to motivate them to continue their careers in public service. To meet these objectives, Congress should:

- Fund DHS, NSF, and OPM to expand the existing CyberCorps: Scholarship for Service program. Since its inception in 2001, this proven program has graduated 3,600 students. The program should be resourced to grow steadily and eventually reach as many as 2,000 students per year.
- Direct and fund CISA to design a process for one- to three-year exchange assignments of cyber experts from both CISA and the private sector. If successful, this model should be expanded to other agencies as well.
- Direct OPM, NICE, and DOD to design cybersecurity-specific upskilling and transition assistance programs for veterans and transitioning military service members to move into federal civilian cybersecurity jobs.
- Direct OPM to require departments and agencies to develop training for managers to cultivate practices that foster a more diverse cyber workforce and more inclusive work environment.
- Require federal cyber contractors to implement known best-practice workplace policies in order to improve employee retention on federal contracts.
- Direct OPM, in partnership with federal departments and agencies including NIST and DHS, to issue a report evaluating the potential for a new Civil Service Cyber: a system of established cyber career paths that allows movement between departments and agencies and into senior leadership positions. In order to facilitate movement between different departments and agencies, this plan should:
- Establish greater standardization and demonstrated equivalences across the government.
- Incorporate competence-based metrics, work-based learning programs, and—after rigorous assessment of their utility and impact—cyber aptitude tests.
- Include standardization tools such as the NICE Cybersecurity Workforce Framework and the Cyber Talent Management System (CTMS). The new CTMS—to be launched at DHS starting in fiscal year 2020—will establish a new DHS cybersecurity service, composed of civilian employees hired using streamlined processes, new assessments, and market-sensitive compensation. If CTMS is successful at DHS, it should be considered for aggressive expansion Federal Government-wide.

It is clear that the pace of malicious cyber incidents is severely outmatching the personnel needed to secure systems. The government needs to act now to strengthen the cyber workforce to meet these threats, and these recommendations will bring us closer to do just that. The Commission appreciates your work in this space and stands ready to work together to make these changes a reality.