[H.A.S.C. No. 116–88]

REVIEW OF THE RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION

HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

HEARING HELD
JULY 30, 2020

U.S. GOVERNMENT PUBLISHING OFFICE
41–410 WASHINGTON : 2021

SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

JAMES R. LANGEVIN, Rhode Island, *Chairman*

RICK LARSEN, Washington
JIM COOPER, Tennessee
TULSI GABBARD, Hawaii
ANTHONY G. BROWN, Maryland
RO KHANNA, California
WILLIAM R. KEATING, Massachusetts
ANDY KIM, New Jersey
CHRISSY HOULAHAN, Pennsylvania
JASON CROW, Colorado, *Vice Chair*
ELISSA SLOTKIN, Michigan
LORI TRAHAN, Massachusetts

ELISE M. STEFANIK, New York
SAM GRAVES, Missouri
RALPH LEE ABRAHAM, Louisiana
K. MICHAEL CONAWAY, Texas
AUSTIN SCOTT, Georgia
SCOTT DESJARLAIS, Tennessee
MIKE GALLAGHER, Wisconsin
MICHAEL WALTZ, Florida
DON BACON, Nebraska
JIM BANKS, Indiana

JOSH STIEFEL, *Professional Staff Member*
ERIC SNELGROVE, *Professional Staff Member*
CAROLINE KEHRLI, *Clerk*

CONTENTS

REVIEW OF THE RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON INTELLIGENCE AND
EMERGING THREATS AND CAPABILITIES,
Washington, DC, Thursday, July 30, 2020.

The subcommittee met, pursuant to call, at 1:01 p.m., in room 2118, Rayburn House Office Building, Hon. James R. Langevin (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, CHAIRMAN, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. The subcommittee will come to order.

I would like to begin by welcoming the members who are joining the hearing remotely.

Just a bit of housekeeping before we get into the actual hearing itself.

To those members—those members are reminded that they must be visible on screen within the software platform for the purposes of identity verification when joining the proceeding, establishing and maintaining a quorum, participating in the proceeding, and voting. Members participating remotely must continue to use the software platform's video function while attending the proceedings, unless they experience connectivity issues or other technical problems that render the member unable to fully participate on camera. If a member who is participating remotely experiences technical difficulties, please contact the committee staff for assistance, and they will help you get recognized.

When recognized, video of remotely attending members' participation will be broadcast in the room and via television internet feeds. Members participating remotely are asked to mute their microphone when they are not speaking. Members participating remotely will be recognized normally for asking their questions—for asking questions, but if they want to speak at another time, they must seek recognition verbally. In all cases, members are reminded to unmute their microphone prior to speaking.

Members should be aware that there is a slight lag of a few seconds between the time you start speaking and the camera shot switching to you.

Members who are participating remotely are reminded to keep the software platform's video function on for the entirety of the time they attend the proceeding. Those members may leave and rejoin the proceeding. If members depart for a short period for reasons other than joining a different proceeding, they should leave

the video function on. If members will be absent for a significant period or depart to join a different proceeding, they should exit the software platform entirely and then rejoin if they return.

Members are also advised that I designated a committee staff member to, if necessary, mute unrecognized members' microphones to cancel any inadvertent background noise that may disrupt the proceeding. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only.

Finally, remotely participating members should see a 5-minute countdown clock on the software platform's display, but, if necessary, I will remind members when their time is up.

So, with the logistics verified, I will want to begin by welcoming everyone to today's hearing on the findings of the Cyberspace Solarium Commission, a congressionally mandated commission created in the fiscal year 2019 NDAA [National Defense Authorization Act] that was charged with developing a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequence.

Inspired by Project Solarium, a task force assembled by President Eisenhower in the early 1950s, the Solarium Commission brought together representatives from academia and the private sector with representatives of the executive branch and legislative branches.

In the spirit of transparency, I want to make clear that I had the distinct privilege of being selected by Speaker Nancy Pelosi to serve as one of the four elected Members of Congress to serve as a commissioner and one of two from the House of Representatives, along with our distinguished subcommittee colleague, Congressman Mike Gallagher, who is appearing as a witness before us today.

Mr. Gallagher, along with Senator King, the junior Senator from Maine, also was a member of the Senate Armed Services Committee and Senate Intelligence Committees, is also with us today. They serve as co-chairs of the Commission, and I am very proud to call them both colleagues and friends.

This subcommittee, more than most, has heard from numerous individuals on the centrality of cyberspace to our modern lives. The novelty of the Solarium's work and its findings is in examining how to secure cyberspace with an emphasis on a whole-of-government approach. Congress is methodical in its views of jurisdiction, and we are often too focused on viewing our oversight responsibilities exclusively through the lens of committee jurisdictions.

What the Solarium Commission has presented in its final report, completed on March 11th of this year, is a blueprint for legislative and executive actions that force the country to break apart the institutional stovepipes.

In this respect, I see the findings of the Solarium Commission as being similar to those of the 9/11 Commission, in that both bodies recognized government silos that had been artificially constructed and harmed the national approach to addressing cost-cutting issues. Whereas the 9/11 Commission applied this to the problem of terrorism, Solarium applies it to cyberspace.

The Commission's recommendations have resulted in more than 20 provisions in this year's National Defense Authorization Act,

passed just last week by the House of Representatives. In that one bill, this chamber was able to address matters as diverse as Reserve support for military cyber operations to the cyber insurance marketplace to the establishment of a Senate-confirmed national cyber director.

While we obviously have more work to do, I am proud of the NDAA—that the NDAA reflects the whole-of-government action called for by the Commission. I applaud the example set by our European partners in particular in approaching cyber in novel and holistic ways, as recent as today with the announcement of the first-ever cyber sanctions issue—issued—passed—that issued through the European Union against six individuals and three entities responsible for the WannaCry, NotPetya, and Operation Cloud Hopper attacks.

This is going to be essential going forward in enforcing international norms, and this is a concrete step toward making sure that there are consequences to actions that violate norms in cyberspace on the international front.

As I noted earlier, we have four witnesses appearing in front of the subcommittee today. In addition to the distinguished gentlemen from Wisconsin and Maine, we are also joined by two additional commissioners.

The Honorable Patrick Murphy, a former member of the House of Representatives from Pennsylvania, is here today. Commissioner Murphy has served with distinction as an Acting Secretary and Under Secretary of the Army, is a former member of the House Armed Services Committee, and today continues his service as distinguished chair of innovation at the United States Military Academy. Commissioner Murphy was the first veteran of the war in Iraq to be elected to Congress.

Finally, we have Commissioner Frank Cilluffo, who, in addition to his service with the Solarium Commission, serves as the director of Auburn University McCrary Institute for Cyber and Critical Infrastructure Security. From 2001 to 2003, Commissioner Cilluffo served as special assistant to President Bush on Homeland Security, and then led the Center for Cyber and Homeland Security at George Washington University.

So I welcome all of our witnesses here today. I thank them for their extraordinary work on the Cyber Solarium Commission. Your input and your insights were absolutely invaluable.

Before we hear from our witnesses, I do want now—want to turn to Ranking Member Stefanik for her opening comments.

[The prepared statement of Mr. Langevin can be found in the Appendix on page 29.]

STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, RANKING MEMBER, SUBCOMMITTEE ON INTELLIGENCE AND EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. Thank you, Chairman Langevin.

Welcome to our witnesses, Senator King, Congressman Gallagher, Congressman Murphy, and Mr. Cilluffo. It is great to have you before the subcommittee today. I thank you not only for your

leadership and service to the Cyber Solarium Commission, but your long and distinguished records of public service to this country.

And although you are not testifying today, I also want to thank Chairman Langevin for his service on the Commission as well, as all of the other commissioners who are not participating today.

It is truly remarkable how much ground the Cyber Solarium was able to cover in such a brief period of time. In 11 short months, the Commission developed over 50 legislative proposals, 22 of which were included in the House-passed version of the National Defense Authorization Act. This impressive commitment reflects the hard work of the commissioners and the staff, and also recognition that we must address these issues immediately.

As is often the case, our Nation's strategy, policy, and laws trail the advent of new technology. This is especially true of many emerging disciplines, but none quite as consequential as cyberspace. The debilitating cyber attack on Estonia in 2007, the devastating Office of Personnel Management data breach in 2014, and the cyber attack on the city of Atlanta in 2018, all should have served as wake-up calls for the need of a comprehensive strategy to bolster our cyber defenses, to deter hostile action in cyberspace, and to build more resilient public and private cyber infrastructure.

The threat actors in cyberspace are as diverse as the tools and tradecraft they employ to infiltrate and attack our networks. And while we must maintain a flexible and adaptable approach to meet the evolving threat, we must also communicate an unequivocal position that demonstrates our willingness to defend the United States in cyberspace and impose costs on our adversaries if and when deterrence fails.

I firmly believe we must simultaneously strengthen our cyber defenses and demonstrate our unwavering resolve to challenge our adversaries in cyberspace. I appreciate the Commission's recognition of this as well. Deterrence alone is not sufficient, especially with the challenges of timely attribution and the notional fog of war in cyberspace. The United States must proactively take steps to increase the resilience of our networks and our Nation's critical infrastructure. This task is not one that the Federal Government can take on alone. Any effort to bolster our cybersecurity must be done in partnership with the private sector, our cities and States, and our critical infrastructure operators.

The Commission's recommendations that were included in the NDAA address this reality. Accountability, information sharing, collaboration, and more timely response and mitigation to cyber incidents are all critical attributes that we must reinforce and strengthen.

While the Commission is coming to an end, the work is not done. We have a long road ahead to see through conference and fully implement these changes. I look forward to ensuring the Cyber Solarium's recommendations are translated into concrete policy action.

We have a lot to talk about today, so thank you to our witnesses, and I yield back.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 32.]

Mr. LANGEVIN. I want to thank the ranking member for those comments.

And before we turn to our witnesses, I would be remiss if I didn't acknowledge the extraordinary work of the staff of the Cyberspace Solarium Commission, starting with Mark Montgomery and the entire team that he assembled that serve the Commission so well. And I also want to, of course, mention on my own staff, my legislative director, Nick Leiserson, as well as on the committee staff, Josh Stiefel, for their subsequent work in seeing that the findings were put into action and getting them into the NDAA, but extraordinary effort all the way around. I can't say enough about the work of the entire staff, again, led by Mark Montgomery. We thank them for their contributions and their service.

So, with that, we will turn to our witnesses now.

Senator King, we will begin with you. The floor is now yours for any comments you may have.

STATEMENT OF HON. ANGUS KING, CHAIRMAN, CYBERSPACE SOLARIUM COMMISSION

Senator KING. Well, thank you, Mr. Chairman. And thanks to the ranking member for those eloquent statements. You stated the case. I can save part of my remarks. I do have written remarks, which I would like to submit for the record if—subject to your approval, Mr. Chairman.

Mr. LANGEVIN. Without objection, so ordered.

Senator KING. And I will have some informal remarks now.

First, I want to thank this committee and thank the full committee for the work that you have already done on this critically important subject, the work that went into the National Defense Authorization Act that, of course, has now passed both Houses.

Both bills from the Senate and the House have a number of our recommendations. They are not in 100 percent overlap, so there will be some work to do in conference, but we certainly have made a substantial start in really putting these recommendations—implementing the recommendations, because if it is just a report that sits on a shelf, it is not going to serve the public interests.

Just a bit about the Commission. You talked about it, Mr. Chairman. There were 14 members. There were four Members of Congress, four members from the executive branch, and six from the private sector. Our work was entirely nonpartisan. There wasn't a moment of partisan discussion in the 30-plus meetings that we had. In fact, I couldn't tell you the partisan affiliations of pretty much anyone that was in the room, except, of course, the ones—the Members of Congress. And that was the spirit with which we approached this incredibly important problem.

I don't really need to outline for this committee how serious this is. This is one of the, if not the most serious international relations problem that we face. The ranking member listed the attacks that we have already endured, and there will certainly be more to come.

We are the most wired country in the world and, therefore, we are the most vulnerable country in the world. And as we have learned in the pandemic, something which strikes at our essential economy and government poses a grave danger to this country.

So let me just give you a brief outline of how the work of the Solarium sort of breaks down. There are really three pieces. One is reorganization, one is resilience, and one is response.

Reorganization means trying to develop a coherent structure in the United States Government so that we can respond to cyber threats and cyber attacks. The problem, as is often the case, is that the authority for cyber is scattered throughout the government. It is in the FBI [Federal Bureau of Investigation]. It is in Cyber Command. It is in CIA [Central Intelligence Agency], DHS [Department of Homeland Security]. It is in all areas of the government. So one of our primary focus was on bringing some coherent organizational strategy to that silo problem which the chairman mentioned.

The principal recommendation there is one that you have already adopted in your committee, which is the creation of a national cyber director to oversee and coordinate all of these various functions throughout the Federal Government.

The second piece is resilience, which is building up our cyber defenses, and it goes from simple cyber hygiene to being just more secure in how we deal with the cloud, how we certify home routers and all of those kinds of things in order to be more resilient to make it less likely that an adversary will succeed.

The third piece is response. How do we respond to a cyber attack and, more importantly, how do we notify potential adversaries that we will respond? And we will be talking about that. And all of these four—three pieces come into what is called a layered cyber deterrence.

The intention is to shake behavior—we will be talking about that—in the international field of norms and standards. The second is to deny benefits. That is the resilience that I was talking about. And the third piece is impose costs.

The truth is that we haven't done a very good job of imposing costs. We have become a cheap date in cyber. We can be attacked, as we were with the OPM [Office of Personnel Management] breach the ranking member mentioned, or other attacks on our democracy, and there is no real consequences. There are no real results. There is no cost paid by our adversary.

We have got to make adversaries go through a cost calculation saying, well, if we do this, they might do this—something else to us, and it may not be cyber. It may be sanctions. It may be other kinds of a response. But we have to establish that there will be a response. Otherwise, because cyber is a relatively cheap form of aggression, it will continue to happen.

So that is the overall focus of our Commission. And I have to say, working with the two members from your subcommittee, Jim Langevin and Mike Gallagher, has been one of the great pleasures of my life. We have had a fantastic experience working together with the other 12 members of the Commission, really wrestling with some difficult issues, working hard, concentrating, and coming up with what we feel is a solid piece of work that will really help our country move forward in this critically important area.

So I thank the subcommittee for your attention and look forward to the hearing.

[The joint prepared statement of Senator King, Representative Gallagher, Mr. Murphy, and Mr. Cillufo can be found in the Appendix on page 34.]

Mr. LANGEVIN. Very good. Thank you, Senator King, for those remarks, and, again, for your extraordinary leadership in co-chairing

the Cyber Solarium Commission and your commitment to public service. The citizens of Maine have chosen wisely in having you as their Senator.

With that, let me now turn to our colleague on the House Armed Services Committee, the co-chair of the Cyberspace Solarium Commission, Chairman Mike Gallagher—Co-Chairman Mike Gallagher.

STATEMENT OF HON. MIKE GALLAGHER, CHAIRMAN, CYBERSPACE SOLARIUM COMMISSION

Mr. GALLAGHER. Thank you, Chairman Langevin.

Let me state at the outset that this is the most nervous I have ever been sitting in this room with all of you, but thank you, Chairman Langevin, for your leadership, and, particularly, you know, there was a 2-week stretch when NDAA was happening where I was not—I was out of commission because my wife had a baby, and Jim stepped up and really led the way in terms of making a forceful argument for a lot of our recommendations and getting them included in the NDAA, and really Project Solarium or the Cyberspace Solarium Commission represent the culmination of a lot of work that Jim has been doing for decades. And so it was an honor to work with you.

Ranking Member Stefanik, thank you for your input into the report and all of your contributions in this space and your leadership.

I too have an official written statement that I would like to submit for the record, if that is okay.

Mr. LANGEVIN. Sure. Without objection, so ordered.

[The information referred to was not available at the time of printing.]

Mr. GALLAGHER. And in an attempt to be brief, I will just say a few things.

When I first approached then Speaker Paul Ryan and asked him to consider me for this Commission, I got about 10 seconds into my spiel, and I had printed out my journal article I wrote on the original Project Solarium, I was really proud of myself, when he cut me off and said, Mike, no one else has asked me to be on it, so if that holds, you will have the spot on the Commission.

And I just bring that up to say I came into this not with a particular expertise on cybersecurity, but a desire to, if nothing else, to demystify a lot of what we talk about in cybersecurity, because while we all have an interest in the space, it is my experience that this can easily devolve into a complex discussion of technology and acronyms. And so I hope you will see reflected in the final report an attempt to speak in plain language, not only to each other and to the executive branch, but to the American people about the threats we face in cyberspace.

And I also came with a desire to demystify a lot of what happened with the original Project Solarium. And by that I mean I think it is—we have this tendency to look back on the early days of the Cold War and think, well, we just had a bunch of like-minded people that were able to come together and agree on everything and join hands and sing kumbaya, and that is how we beat the Soviets and laid the foundation for successful containment.

I don't believe that is the case. We had very vicious disagreements at that time. We went through multiple variants of contain-

ment, even within the Truman administration before we got to Eisenhower. But there was this persistent willingness to challenge each other in good faith to think through the unthinkable, think through the consequences of a nuclear exchange with the Soviets in order to ascertain what we needed to do to avoid that exchange.

And I just want to highlight that, because I think, among the many recommendations in this report, one that I think is absolutely critical is a similar effort today that is needed to think through the unthinkable in cyberspace, think through the consequences of what a massive cyber attack on the United States would look like, what a so-called cyber 9/11 would look like, and that is why you see a lot of recommendations in here on why Congress should mandate the executive branch do continuity of the economy planning. So we think through how we can get the economy back up and moving when we are faced with such a significant cyber attack.

And so I just wanted to highlight that, because I really think it gets to what was the genius at the heart of the original exercise, which really reflected Eisenhower's style of making decisions. He had this beautiful phrase where, you know, we always remember he said, you know, in times of war, the plans are nothing, but the planning is everything, and that is reflected.

But he also said to his subordinates frequently when they are sitting around the National Security Council, there can be no nonconcurrence through silence. In other words, you had to speak up. You couldn't claim after the disaster that you actually had the right answer the whole time but you failed to share it with your colleagues. And, similarly, we have tried not to suppress disagreement in this report but to surface it and, if nothing else, provoke a more thoughtful debate among our colleagues.

So I thank you for your attention, I thank you for your engagement, and I thank you for your pushback on our findings. And I yield the rest of my time.

Mr. LANGEVIN. Thank you, Chairman Gallagher.

The chair now recognizes Commissioner Patrick Murphy for his opening comments.

STATEMENT OF HON. PATRICK MURPHY, COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Mr. MURPHY. Thank you, Mr. Chairman, and thank you, Representative Ranking Member Stefanik. I do have written opening testimony that is brief. If it is okay, I would like to submit it for the record.

Mr. LANGEVIN. So ordered, without objection.

[The information referred to was not available at the time of printing.]

Mr. MURPHY. Terrific. And to my other commissioners, thank you so much.

You know, today is a great day to be back in the House Armed Services Committee, where I used to serve, and I am honored to testify today along with my fellow commissioners on the recommendations from the Cyber Solarium Commission's report. Our report has been a lot of blood, sweat, and tears over a year in a bipartisan, bicameral, public-private sector approach.

And before I was in political public service, I did serve in the United States Army and am a veteran of the Iraq war, and I now chair innovation at the United States Military Academy at West Point.

But when I was appointed to this special bipartisan commission, I was naturally interested in how the United States could preserve and employ the military instrument of power to impose costs on our adversaries and defeat the ghosts in our networks. And I want to concentrate my comments today on this important aspect of our Commission's work, because at the end of the day, it is our United States military that is responsible for keeping our families safe here at home.

I am firmly in support of our Commission's choice to expand upon the concept of defend forward as described in the 2018 Department of Defense Cyber Strategy, to incorporate both military and nonmilitary instruments of power as part of our Commission's strategy of defend forward and layered cyber deterrence.

I believe that this strategy, if endorsed and appropriately resourced by our United States Congress, will ensure that the United States is prepared to impose costs on our adversaries to better deter and, if necessary, fight and win conflicts. It is no secret that our adversaries are using cyberspace to steal national security, intellectual property, and hold U.S. military systems and functions at risk. The latter, in particular, threatens to undermine our deterrence across all of our instruments of warfare.

The conventional and nuclear technologically advanced military capabilities that form the bedrock of America's military advantage also create cyber vulnerabilities that our adversaries could exploit to their own benefit. And so whether it is nuclear, conventional, or cyber, the United States must be confident that its military capabilities will work as intended.

Moreover, across a spectrum of engagement from competition to crisis and conflict, the United States must ensure that it has sufficient cyber forces to accomplish our strategic objectives in and through cyberspace. This demands sufficient capability, capacity, and streamlined decision-making processes enabling rapid and effective cyber response options to impose meaningful costs against adversaries and to respond to adversary action.

You know, while our Commission's final report—it boasts over 80 recommendations, but I would like to draw this committee's attention, this committee in particular's attention, to ensure that you give serious consideration to the following 3 items as it involves defending our Nation.

First, Congress should direct the Department of Defense to conduct a force structure assessment of the Cyber Mission Force to ensure that the United States has the appropriate force structure and capabilities in light of mission requirements and expectations that are growing in both scope and scale. Additionally, this assessment must also include ensuring sufficient resources for entities within our intelligence community that do play critical combat support agency functions for our U.S. Cyber Command, particularly the NSA [National Security Agency].

Second, currently, the CMF, the Cyber Mission Force, has 133 teams comprised of 6,200 incredible individuals. However, these re-

quirements were determined over 7 years ago in 2013, before the United States fully appreciated the scope and the scale of the threat in cyberspace, which has increased mission requirements on the CMF. A force structure assessment of the CMF is the first step to make sure that we get it right to ensure that the CMF has appropriately sized forces and sufficiently capable—is sufficiently capable to achieve its objectives.

And last, as it relates to defense, Congress needs to direct the Department of Defense to conduct a cybersecurity vulnerability assessment of all these segments of the nuclear command and control system, continually assess weapons systems' cyber vulnerabilities.

Now let me go to the economy.

I thought our co-chairman, Senator Angus King, said it great and appropriately when he said we are the most wired and vulnerable country in the world. And whether it is my time in the Pentagon, as a soldier overseas, or in the Congress, we understand that the greatness of America is that we do have the number one economy in the world, and we have the number one military in the world, and it is up to us to make sure we keep it that way.

And as it goes to our economy, I want to make sure that we comment and address the continuity of the economy. I believe the United States must prepare for the cyber day after. The government needs a continuing plan to ensure that critical data and technology remains available after a devastating network attack.

You know, during the height of the Cold War, the U.S. Government had a plan for the day after. The government did what it needs to ensure that after a massive nuclear strike, how do we ensure that our government and how do we get the private sector operating, especially when it comes to critical infrastructure, getting it back online, and even how to put hard currency back into circulation and begin regenerating our economy.

Similar to the necessary plans to manage a pandemic, we currently have no such reconstitution plans for such a cyber event. I strongly believe this Congress should direct the executive branch to develop and maintain this plan in consultation with the private sector to ensure the continuous operation of critical infrastructure of the economy in the event of a significant cyber disruption.

Like COOP [continuity of operations] and COG [continuity of government] before it, this will be a critical piece of our national planning. And in similar vein, you know, Congress should codify a cyber state of distress tied to a cyber response and recovery fund to ensure that the CISA [Cybersecurity and Infrastructure Security Agency] and appropriate Federal agencies have sufficient resources and capacity to respond to significant cyber incidents before they turn into major disasters.

You know, while the NDAA functions to provide the DOD [Department of Defense] with an annual health and wellness checkup, Congress must not ignore the underlying national security threats that could damage our infrastructure that is owned and operated by the private sector, because these digital foundations drive the American economy. They spur technological innovation and they support our United States military. The status quo in cyberspace and this lack of a COOP plan is unacceptable, and we need your

help to protect the key elements and enablers that make our military and our country it serves the best in the world.

Thanks, Mr. Chairman and the ranking member, for this opportunity to testify before you today, and we look forward to your questions.

Mr. LANGEVIN. Thank you, Commissioner Murphy, for those comments.

And now the chair recognizes Commissioner Frank Cilluffo, Frank, for any comments that you would like to make.

You are still muted.

STATEMENT OF FRANK CILLUFFO, COMMISSIONER, CYBERSPACE SOLARIUM COMMISSION

Mr. CILLUFFO. Thank you, Chairman.

Mr. LANGEVIN. Gotcha.

Mr. CILLUFFO. Thank you for the privilege, Chairman Langevin, to join you today, Ranking Member Stefanik, distinguished representatives, and my fellow commissioners. It really is a privilege to be able to spend a little bit of time with you and share some of our thoughts on the recommendations of our Commission's report.

The strategy that we have laid out, as Senator King said, is the modern credible deterrent that the United States urgently needs in cyberspace. The current status quo in which China, Russia, Iran, and North Korea conduct malicious cyber campaigns against the country is, simply put, unacceptable.

As my colleagues addressed, it is imperative we move fast, starting with a national cyber strategy and a national cyber director who will focus government efforts on cybersecurity. I also second the call that Patrick was espousing to establish continuity of the economy planning. There can be no more important efforts than the ones to make our Nation resilient to cyber attacks.

But I thought I would highlight a couple of other recommendations that are equally as important.

First, to foot stomp what Patrick had mentioned in terms of the Cyber Mission Force, we really do need to conduct that force structure assessment, which is dated in terms of what the gap and the need is today from when that was initially established. And the scope of the threat obviously grows exponentially. And since the bulk of capabilities within DOD to counter malicious adversary campaigns and impose costs are within the CMF, we simply have to ensure that they are resourced and have the authorities to fulfill its job.

I think, as Ms. Stefanik rightly put, we must continue to lead and innovate by integrating cyber into our warfighting strategies and doctrine. We need to ensure that we can bring in both the offensive capabilities and the defensive capabilities to lead.

Second, as Patrick also mentioned, conventional and nuclear weapons systems. They need to work when—when needed and as intended. And I just want to double tap the recommendation in terms of conducting a cybersecurity vulnerability assessment of all segments of not only our NC3, our nuclear command and control systems, but continually assess our conventional weapons system cyber vulnerabilities as well, and we need to do this in a systems-

to-systems approach. You can't look at it in isolation. You need to look at it in its totality.

And I also highly support the recommendations that Congress should require defense industrial base [DIB] participation in threat intelligence-sharing programs and threat hunting on the DIB networks.

And as I said before, to preserve and employ the military instrument of power, we must also maintain resilience in our economy and critical infrastructure. And, again, I just want to foot stomp the continuity of economy recommendation. I hope Congress can act upon that.

Third, the public and private sectors, along with key international partners, must collaborate to build resilience and reshape the cyber ecosystem in a manner that enhances security. This means partnering with the private sector and especially those that are ideally positioned to scale their impact on the ecosystem, such as IT [information technology] companies, ISPs [internet service providers], and cloud service providers, and to better secure the services and products that they offer.

The Commission recommended a number of important actions that Congress should take now to that effect. One, Congress should establish and fund a national cybersecurity certification and labeling authority for information and communications technology funnels, and a bureau of cyber statistics to provide a foundation for decision makers to base policies and programs on empirically based evidence. This statistical information also serves as a platform to facilitate market-based solutions and mechanisms, such as cybersecurity insurance.

I also want to thank the committee for including demark standards in the NDAA. This can go a long way in securing email from phishing and malware attacks. And while we obviously need to be focused on advanced persistent threats, often the first way into one system is through phishing expeditions and the like.

And, lastly, we need to ensure that our supply chains are trusted, and Congress should direct the U.S. Government to develop and implement an industrial base and manufacturing strategy, again, for information technologies and communications technologies.

Finally, I would like to focus on a topic that is critical to mission success. We must, must invest in our Nation's cybersecurity workforce. The shortfall between supply and demand in this area is staggering. And it is all the more concerning because the threat continues to expand exponentially, and the gap gets greater, not lesser.

And we need to—as a matter of national and economic security, we need to redouble our efforts to pull in more veterans and get serious about recruiting and retaining more women, people of color, and neurodiverse individuals.

Leveraging different perspectives and diversifying a cybersecurity workforce is not only the right thing to do; it is the smart thing to do. The time to act is now.

Mr. Chairman, I hope I didn't go over my time, but thank you for the opportunity to testify before you today. I look forward to questions. And I really do appreciate your leadership, not only

through the Solarium Commission, but for many, many years on cyber-related issues. So thank you, sir.

Mr. LANGEVIN. Thank you very much, Commissioner Cilluffo, and for your longstanding contributions to the issue of cybersecurity in your own right.

So, with that, I thank all of our witnesses for their testimony today. We are now going to move to our questions.

Before I do that, though, I was remiss in not recognizing a couple of other people that were very involved in certainly helping us to get the recommendations through the Armed Services Committee and into our mark and to the floor. I want to recognize Chairman Smith and Ranking Member Thornberry for their support, as well as Ranking Member Stefanik and staff director Paul Arcangeli and many others.

Let me also recognize my team, Allison Browning, my—you know, my colleagues, military fellows, along with Caroline Goodson and Matt Lake, my other military fellow. And I know that Eric Snelgrove as well on the minority side was very, very helpful.

So, with that, let me now turn to questions. And if it is conducive, Senator King, if I could start with you. If I could ask, which defense-centric recommendations strike you as the most urgent, whether directed at the executive branch or the legislative branch?

You are muted. You just need to unmute.

Senator KING. If I seem a little out of breath, it is because I just voted. I had to go upstairs for a vote, but I was able to listen to Frank's testimony, so I appreciate it.

I think, Jim, our probably the most significant recommendation that relates indirectly to defense but is—overall is the national cyber director. The reality is that, right now, we have enormously capable people throughout the Federal Government, but there is no central point of oversight. There is no central point of coordination. There is no central point of defining strategy. And I really think that that is—that is one of the critical recommendations. It is one that is already in your committee bill, which I think is really important.

I think, secondly—and Patrick Murphy mentioned this—the force structure assessment. We haven't really looked at the force structure of—in the Defense Department on cyber since 2013, and I think we all know that there have been dramatic changes since then. There have been dramatic changes in the risk, in the complexity, in the adversaries, in the target space. So I think that is probably—I would put that next in line.

And then the development of the cyber workforce, because we can have—we can talk about force structure, but if we don't have the people to fill those positions with the skills, then we are just not going to make it. For example, a cyber workforce, there is a—we have a scholarship program now that is very effective, but it has graduated, I think, 2,000 people in the last 4 or 5 years. We need to—or 3,600, I guess. We need to graduate 2,000 a year. I mean, we have a tremendous need for these skilled people.

So I would say national cyber director, assess the cyber force, and develop workforce would be my first three priorities in the—in that—in the military area.

Mr. LANGEVIN. Yeah. Very good. Very insightful. I completely concur. Thank you for those observations. And we need to grow the size of the cyber pie, not just competing for a bigger slice of it from a government standpoint. We need to—it helps both government and private sector to grow the size of the cyber workforce pie. And I concur with the other recommendations you highlighted.

How about Chairman Gallagher, same question to you, what do you see as the most urgent and important of the 82 recommendations, if you would like to comment?

Mr. GALLAGHER. Well, I agree with Senator King that I think, over time, we will realize that the force structure assessment of the Cyber Mission Force will end up having perhaps the biggest impact on DOD over the next decade if we come back with a finding that suggests that we do not have enough personnel dedicated to the issue.

But I do think perhaps more urgent, and it is an area where I know there is still some debate, is to get the authorities right that would allow us to do threat hunting on defense industrial base networks. I think one of our biggest findings in the report was that, while we are getting a better awareness of our own systems, we still, down to the level of some of our DOD contractors, subcontractors, all the small companies that, you know, work with the big defense primes, don't have the level of visibility on the threat picture and the security of their networks that we need.

And so we have a lot of recommendations in chapter 6 towards that end. And I just would argue that we need to figure that piece out, because we just can't be in the process of reacting to cyber intrusions after the fact. We have to identify those threats at a quicker timeline than that at which our adversaries can break out on networks.

So I just would highlight some of what my colleagues have talked about in terms of threat hunting, not only on DOD systems, but on the whole defense industrial base network.

Mr. LANGEVIN. Very good. Thank you for that.

Let me turn to Commissioner Murphy now. Commissioner Murphy, based on your time within the Department of the Army as a soldier, as an officer, and a civilian leader, what are your views on the Solarium's recommendation on evaluating different models for their Reserve Component? Are you optimistic that the Army, as an institution, can accommodate a different model for their Reserves than existed, say, for the last several decades?

Mr. MURPHY. I do, Mr. Chairman, and I appreciate that question. Can I just address something? I think this is the first time in American history we had someone testifying and at the same time voting in the U.S. Senate when Senator King did that about 15 minutes ago.

But to your question, Mr. Chairman, absolutely. We all know that the largest fighting force we have in America is our U.S. Army. We have got a million soldiers strong, 300,000 civilians. But of those a million soldiers, unlike the other services, the majority of our soldiers are actually in a Reserve Component, in the National Guard, in the Army Reserves. And that is why it is critical that when we say we have in the CMF 133 teams, you know, Chairman Milley and I, when we were running the Army, we made

it a point that we didn't talk about just the 10 Active Duty divisions. We were one Army, and we made sure that we fought as one Army. We trained as one Army. And that includes with cyber.

So, yes, I think our Army, now being led very well by my battle buddy from Fort Bragg, Secretary Ryan McCarthy, and also General McConville, they get that, and they are trying to really do what they can to partnership with the HASC [House Armed Services Committee] and the Congress to make sure that they had that proper balance between the Reserve and Active Component as it relates to cyber, as it relates to CMF. But we need to make sure that as we address this assessment, which we critically need, because, remember, Mr. Chairman, in my statement, 7 years ago is when we did the last assessment. That was before we even had defend forward. That is before we even had layered deterrent.

So now that we have a bigger footprint digitally and we are still vulnerable—and I said, as Senator King mentioned, we are the most vulnerable country in the world because we are so wired. And when we look at the pandemic of coronavirus and what it has done to our economy, imagine the destruction which cyber would do. And that is why, to your point, we need to make sure that we have this assessment and make sure that assessment absolutely positively incorporates the Reserve Component of our military forces.

Mr. LANGEVIN. Well said. Well said. Thank you.

Thank you all for your—the answer to those questions. They are all very insightful answers, and I thank you again for your work on the Commission.

With that, now I want to turn to Ranking Member Stefanik for any questions she may have.

Ms. STEFANIK. Thank you, Chairman Langevin.

I wanted to ask Senator King, both in my opening statement and many of our witnesses have touched upon this, and that is the importance of establishing deterrence in cyberspace that was featured very prominently in the report, but the Commission also notes that true deterrence must be adapted from how it is applied in other domains.

What actions can we take to better deter our adversaries, including state actors like Russia, China, Iran, and North Korea, from conducting cyber attacks on American interests?

Senator KING. Well, I think there are a series of steps, and one that hasn't really been mentioned very strongly so far is the international community. We are in the infancy of the law of cyber war, if you will, and we need to be more active participants in setting the standards and the guardrails and the norms for activity in cyberspace so that when we do act, whether it is the imposition of sanctions or other responses, we are not acting alone or unilaterally.

Winston Churchill said the only thing worse than fighting with your allies is fighting without allies. And that is one of our major advantages on the world stage with regard to our principal near-peer adversaries of Russia and China. I was in Asia about a year ago, and the—someone said, America has allies; China has clients. And I think that is—so that is step one, is to develop an international set of norms that will themselves be at least some level of deterrent.

Secondly, we have to have a clear declaratory policy. I emphasize the word "declaratory," because if you don't tell your adversary that you will respond, then it is not a deterrent. And so I think we need to have a much clearer statement of our doctrine, of our strategy, so that adversaries know that they will, in fact, pay a price.

The problem has been you can argue that we have done a good job of deterring catastrophic cyber attacks. Of course, there is no way to measure something that doesn't happen, but we haven't deterred lower—below the threshold of the use of force cyber attacks, whether it is the OPM breach that you mentioned, or the attacks on our election, our election infrastructure, or the kind of intellectual property theft. We haven't done a very good job of deterring that. So I think the important thing is to establish, (a), the means, the credibility, the credible response; and, secondly, to declare it, to make it clear that you will not attack the United States and not have a significant cost imposed upon you.

So I think international norms and a clear declaratory strategy. It is not exactly, as you note, I think, as you understand, it is not exactly analogous to the nuclear deterrent. It is a different and more subtle kind of issue. But I do believe that unless we make it clear to our adversaries that they have a—they have to calculate that there will be costs imposed, and it may—it doesn't have to be cyber for cyber. It may be sanctions or other kinds of responses. Until they make that calculation, they are going to keep coming after us.

So that would be my response to that very good question. Thank you.

Ms. STEFANIK. Thank you, Senator King.

And my next and final question I am going to address to Congressman or Chairman Gallagher. As you know, oftentimes it is not the DOD or even the Federal Government that is the target of our adversaries in cyberspace. It is often our cities, our States, universities, or private-sector businesses. And many of those entities are ill-suited and, frankly, ill-prepared to protect against cyber threats from nation-states.

How do we address this capability gap, and what are some of the Commission's recommendations that address this really important issue where we tend to have siloing within our Federal agencies?

Mr. GALLAGHER. That is a great question. I would connect it to your previous question, actually. Actually, I think this is the primary difference between the logic of strategic nuclear deterrence and the logic of deterrence as we see it in cyberspace, which is that so much of what we are trying to protect and so many of the actors that we are trying to get to buy into that logic are not card-carrying members of the Federal Government and certainly don't wear uniforms.

And so we had a private-sector commissioner, Tom Fanning, who runs a major energy company, and he would remind us constantly that 85 percent of the critical infrastructure in this country is owned by the private sector.

I think what we also see, to get to the heart of your question, is the good-faith effort to thread the needle in this report between the recognition that the Federal Government has to compel the organizations you identify, be they universities or companies or major

banks on Wall Street, against the unwillingness to saddle them with a bunch of counterproductive and onerous regulations that might stifle innovation and entrepreneurship in this country, which, as Senator King and I say at the outset, is our best path to beating China over the long term.

So the approach we took, whether it is through recommendations like mandating penetration testing for major publicly traded companies or requiring companies that are part of the defense industrial base to participate in threat intelligence sharing or establishing a joint planning office within CISA in order to more proactively engage with the private sector so they are actually integrated into our defensive planning process, we get their input on the front end, is a mix, I would say, of carrots and sticks.

We want the C-suite executives to take cybersecurity seriously, and we are prepared to sort of nudge them in that direction. But we also want them to view the Federal Government as a valuable partner, a partner that understands that, in many ways, the private sector is the main effort in cyberspace and the Federal Government is the supporting effort.

Ms. STEFANIK. Thank you. I yield back.

Mr. LANGEVIN. Very good. Thank you, Ranking Member Stefanik.

Mr. Larsen is now recognized for 5 minutes.

Mr. LARSEN. Thank you—thank you.

My first question is for Representative Gallagher, and this gets to the business of the private sector side of things, because we have the Cybersecurity Maturity Model Certification [CMMC] process now working its way through the Pentagon and being utilized, mainly focused on smaller businesses within the defense industrial base.

Did you look at how that could be or should be integrated with what your recommendations are for private-sector cyber hygiene?

Mr. GALLAGHER. I think our view is that it needs to be more expansive than that, and that—I think it needs to take a prior step of even understanding who is included in the phrase "defense industrial base." We have actually gone through this process before, not in a cyber context, where the Pentagon has actually tried to have what I would call total defense manufacturing visibility. Who are all the companies that are part of this ecosystem? And for whatever reason, we haven't gotten there. It is now even more complex in cyberspace.

So I view our recommendations as perhaps building upon the efforts you reference. I know that those—there are a lot of companies who may not want to participate in that, but I just would say, if you are working with the Pentagon, if you are working on systems that are critical to our national defense, and if we know that you are a target for foreign actors, be they state-sponsored hackers from China or cyber criminals, you are going to have to demonstrate a higher level of cybersecurity than those companies have right now.

Mr. LARSEN. Yeah. Yeah.

For Commissioner Murphy, good to see you again, Commissioner. Recommendations recommend that the U.S. strengthen existing bilateral and multilateral relationships. Can you talk specifically how the U.S. could partner with NATO [North Atlantic Treaty Organi-

zation] to enable and help the member countries strengthen their systems against cyber attacks?

Mr. MURPHY. Absolutely. And, Congressman Larsen, it is great to be with you again, and I hope your home State of Washington is doing great.

Mr. LARSEN. Thank you.

Mr. MURPHY. On your earlier question, really quick, on the private side sector, I know with the CMMC, what we need to do also is that data. Data is king, as you know. And that data and that—really that what we are calling the CSET, the Bureau of Cyber Statistics and Emerging Threats, that is critical, because we need that to make sure that we have a more robust insurance program, et cetera. So I just wanted to dovetail on that.

But to your question directly, no doubt what makes America the shining city on the hill is our diplomatic power. You look at the symbol, the American eagle, 1 talon, 13 arrows signifying the 13 colonies and our military might, the other talon with the olive branch showing our diplomatic power and using smart power.

And so, with that, and with our very specific recommendations that we were tasked to do is asking for a new Assistant Secretary of State. And this one is very, very important, because we need to make sure that we strengthen the norms, we make sure that we use that diplomatic power to let other nations, like China, like Russia, like Iran, know that this is not acceptable, and establishing those norms and making sure that we bring everybody to the table. And I think that is critically important, and we do that by also advocating, frankly, in the White House for the NCD, the national cyber director.

You know when we worked together in the HASC that I am a big believer in leadership and one throat to choke, and by having one person, one quarterback within the Executive Office of the President, that national cyber director will help make sure we are streamlining within our government and also in the private sector, what we need to do to protect our military, to protect our economy and our companies, and also to make sure we are keeping our families and our economy safe.

Mr. LARSEN. Yes. Thanks. Final question will be for Commissioner Cilluffo, because you shouldn't be exempt from having to answer questions while you are here.

Senator King mentioned paying the price. I think it is an attribution. So can you talk a little bit more deeply about what the Commission considered with regards to a policy of attribution? And, second, would attribution apply only to those countries that are specifically listed in the National Security Strategy or would it be any country that is participating in cyber intrusions, which sometimes are not those countries that we consider adversaries?

Mr. CILLUFFO. Thank you, sir, for the excellent question. I mean, for starters, attribution has improved dramatically over the years. We are not fully where we want to be, but I think we are in a much better place. And I think it is worth noting—and this transcends all of the various questions we have seen here—is that cyber is its own domain, but it transcends all the other domains, whether air, land, sea, space, and there are other means of collection that can be brought to bear to enhance our attribution, wheth-

er it is through technical means or through human sources. So the bottom line is our attribution is improving.

You have probably noted a big uptick in at least Five Eyes countries coming together and doing joint and shared attribution. I think this actually is having some very positive net effect in terms of some of our adversaries and actually putting them on notice, as Senator King was discussing earlier. So we need to be able to have some declaratory sort of impact.

And I might note our transatlantic partners with NATO, you have also seen an uptick in joint attribution.

Bottom line is, just the facts, ma'am. We have got to be going where the facts arise. Obviously, there are other potential diplomatic questions when discussing allies, but I think that in terms of informing our USG [United States Government] entities and some of our dot-com entities, we have got a responsibility to do that as the U.S. Government.

So longwinded way of saying I think you are going to see us moving out from our Five Eyes to our NATO partners to allies that don't exist in any of those organizations, such as South Korea, Japan, Israel, and a handful of others, and then build—India, and building out from there. So I think we have made some progress, we have got to continue to do more, and we have got to hold our adversaries to account. There have to be consequences. There has to be impact.

And I think it is worth noting that we do suggest we lean forward in a lot of these issues. We do support the defend forward concept, persistent engagement concept, but not only through the lens of the military, that is a crucial element of it, but all instruments of statecraft.

Mr. LANGEVIN. Very good. Thank you, Mr. Larsen.

Before we go to Mr. Bacon, I will comment and say that Mr. Cilluffo's answer is absolutely right that we are getting better at attribution. What we do need to do, though, is shorten the timeline between incident and our response. I applaud the Europeans who are—the sanctions that they put on the entities that were responsible for several high-profile attacks or intrusions, but those things happened, you know, several months ago. There is such a long lag between action and consequence. If we can, I think both United States, Europeans, our partners, need to work more quickly to close that gap between action, between incident and response. So we punish the bad actors, and they realize it is relevant to the action.

With that, Mr. Bacon is now recognized for 5 minutes.

Mr. BACON. Thank you there, Mr. Chairman. And I want to thank the Commission for their hard work, a very thoughtful discussion. Great product. I appreciate it.

I am not sure who to target the questions to, so I will just—whoever feels best to answer them, just jump in there. I am curious to hear more about the national cyber director, and the reason is our cyber attack is under Cyber Command primarily. Cyber intelligence is primarily under NSA, but what is most worrisome is the cyber defense. It is really no—there is no single authority.

So is this national cyber director and the team that were put in the executive branch or that you are proposing, is it primarily focused on the defense end or does it involve all three: attack, intel-

ligence, defense? And if it is all three, how will that impact the chain of command for a cyber attack? Is it that command goes through the Cyber commander, Secretary of Defense, and the President? So I am just sort of curious to hear more. Thank you.

Senator KING. Mr. Chairman, perhaps I can take that. That is a really good question. The purpose of the national cyber director is planning and coordination, not operations. So the chain of command between the—between Cyber Command, Secretary of Defense, and the President would not be interrupted. That is not the purpose of this new office in the Executive Office of the President. We want this person to be accountable for the coordination, but does not—would not have an operational role.

Also, a piece of it is planning, as we have been talking about, and coordinating planning throughout, whether it is in CISA in Homeland Security or in other—in NIST [National Institute of Standards and Technology] or wherever it is in the Federal Government. But I think the specific answer to your question is we are not talking about operations for this position but coordination, planning, and budget coordination. This person would have an oversight over the budgets of the various agencies, not a veto but a recommendation and a certification through the OMB [Office of Management and Budget] process.

Again, the whole idea is to bring some level of—I guess I would call it just sensible organization because, right now, there is nobody in charge. But to answer your specific question, it is still Cyber Command, Secretary of Defense, President of the United States.

Mr. BACON. Thank you very much, Senator. I appreciate that.

I surely see a need on the defense side. There is very diffused responsibilities on defense, and it just seems to me that there is a definite need at least on that part of our cyber operations.

Change in topics. I have a little experience with cyber, being in the Air Force for a long time. It seems, if I could generalize, Russia was more focused on military cyber, IO [information operations]; China a lot more on the economic intelligence. Is that generalizations or is that still considered, by and large, still the case?

Mr. GALLAGHER. Well, I think that is largely right, though neither, you know, Russia would ignore the economic domain, nor would China ignore the military domain.

I think if you read the report, in particular the threat analysis portion of the report, it is clear that we agree with the fundamental finding of the National Security Strategy and the National Defense Strategy that China is the pacing threat. China is the pacing threat in cyber in terms of the sheer resources they are devoting to this issue. I think we are—we are concerned about Russia. We talk about Russia. We are concerned about non-state actors. But China really comes out as a threat that organizes a lot of our response.

I am not disagreeing with your analysis, but at least a lot of what I realized in the course of participating in this Commission was that we are insufficiently concerned with the actions of the Chinese Communist Party in cyber.

Mr. BACON. I appreciate that. And my generalizations were going back, not necessarily current. So just curious if it was still the case.

I think the areas that concern me most is the energy sector and the financial sector, you know, whether it is Wall Street. I really think China or Russia would really create havoc with focused attacks on those areas, and we have obviously got to raise our game if we want to defend those two critical parts of our country.

Mr. GALLAGHER. Maybe I can connect it to your first question. I think, you know, under the doctrine of civil-military fusion, China is not making these clear siloed distinctions between military operations and sort of economic warfare. And I do think that is an area where we hope the national cyber director can step up and lead that defensive effort.

One of our biggest findings in the report was that a lot of the work that this committee has done in recent years and the fiscal year 2019 NDAA to make cyber surveillance and reconnaissance a traditional military activity and then to have NSPM–13 [National Security Presidential Memorandum–13] layered on top of that has really been a positive development and helped us on the offensive side. We need similar attention paid to the defensive side, so that someone in the Federal Government is the single belly button we can push and is proactively reaching out to the banks and the financial community to say, hey, here is what we are thinking. What input do you have for us?

Mr. BACON. Chairman Gallagher, I agree. I yield. Thank you.

Mr. LANGEVIN. Very good. Thank you very much, Mr. Bacon.

Next on my list I have Congressman Khanna, but I don't know that he is still there.

Are there any members that have not been recognized that would like to be recognized?

Ms. STEFANIK. We are all good in the room, Jim.

Mr. LANGEVIN. Okay. I guess I have one more question on continuity of the economy. And would anybody like to comment on—and I agree that the comments that were made earlier about continuity of the economy are very important. Commissioner Murphy addressed a lot of these. But what role do you see, say, the Department of Treasury, Department of Commerce, and then independent agencies like the Federal Reserve in a continuity of economy plan proposal, and any thoughts on how that should work?

Senator KING. Jim, let me start off on that—or I should say Congressman. Sorry.

I think one thing the pandemic has taught us is that the unthinkable can happen. If you had told us all a year ago we would be wearing masks and it would be—we would have large part of our economy having severe difficulty, all the things that are happening, it would have sounded like science fiction. The unthinkable can happen, and that is really what we are talking about here.

And I think one of the problems that our Commission tried to attack head on was the fact that has been alluded to today, and the prior questioner mentioned this, in terms of the financial sector, the energy sector. The target is mostly in the private sector. So the continuity of the economy, the planning has to engage the private sector. We have to determine what are the crucial elements? What are the crucial sectors that need to be functioning, no matter what? And how do we ensure their protection?

I think this is one of our most important recommendations. This is one that is in the Senate bill. I don't think it is in the House bill, and hopefully we are going be able to pull it through in the conference committee. But we have really got to be thinking about—you know, an ounce of prevention is a pound of cure. I mean, we have got to be thinking about how to react when the unthinkable happens. And if every—if everybody is pointing at one another and there is no plan on the shelf, we are going to be—it is going to be infinitely worse and take infinitely longer to recover.

So I think this is one of our most important recommendations. And, overall, I think one of the most important insights of the Commission was the extent to which we had to really forge a new relationship. We have to think in a new way about how we relate, how the government and the private sector relate in terms of sharing intelligence, sharing attack data, cooperating, talking to allies. I mean, it is really a very comprehensive approach to this. And I think that is one of the significant insights that we bring to the table in the report.

Thank you.

Mr. CILLUFFO. Mr. Chairman, can I add a thought on that? When we talk about the continuity of the economy, it did, as Senator King said, it became loud and clear just how important that is in a post-COVID environment, both directly and indirectly. And one of the things we did really zero in on, if you think about an x- and a y-axis, you have our critical infrastructures, and some are even more so critical than others, and we mentioned a couple of them already here today: energy, financial services, telecommunications, and, obviously, the defense industrial base.

But then also on a y-axis we have got these critical functions. So agnostic to the particular sector, whether it is the cloud or whether it is timing and signaling from a GPS [Global Positioning System] perspective or a PNT-assured—positioning, navigating, timing, and signaling kind of perspective—this is how we have got to start racking and stacking some of these issues.

And I might note, for the Armed Services Committee as a whole, the challenge around mission assurance or the ability for DOD to rely upon civilian entities and critical infrastructures to project power, deploy forces, this is a tough—we have got to put—this is a tough circle to put in a square sort of peg. So I think this is where the interaction between DOD and CISA at DHS and FBI, as well from an investigatory standpoint, becomes so important, and I think that just makes the case for a national cyber director that much more important. So we at least have the visibility across the various playbooks that can come together to be able to make sure that the whole is greater than the sum of its parts.

And this was a point that came up in various questions as well. I mean, at the end of the day, what I think is so important is also on the intelligence side. The new national cyber director that was stood up at NSA is going to play a very important role in enabling CISA, in—so CISA can better reach out to our State, local, Tribal, territorial partners and, of course, the private sector, and same thing in terms of FBI.

So this, again, may not sound sexy, but it is the org—it is the spaghetti org [organizational] chart right now that needs to be brought—tamed a little bit and brought under control.

Mr. MURPHY. Mr. Chairman, can I just put a stamp on what Frank just said real quick, sir——

Mr. LANGEVIN. Sure.

Mr. MURPHY [continuing]. If that is okay with you? One minute. Two things. One, we are going to get caught with our pants down if we don't focus on continuity of the economy, period. And that is why, you know, in my opening statement, I talked about making sure that we have Congress codifying a cyber state of distress that is tied to that cyber response and recovery fund, so, you know, that we need to direct the executive branch and make sure that we do have that continuity of the economy planning that is in consultation with the private sector. We absolutely need to do that.

I would also say to you, when we talk about the NCD, national cyber director, why that is critically important. As Frank just said about, when he was talking about DHS and CISA and making sure State and local, we also need to ensure that our allies—that is why we were calling for that Assistant Secretary of State—that our allies aren't a launching pad to hurt us here or hurt our private sector clients or our military but, secondly, so that it can more quickly do attribution. Thank you.

Mr. LANGEVIN. Very good. Thank you, Commissioner Murphy and to all of our commissioners, for those answers on the topic.

That concludes my questions. I will turn now to Ranking Member Stefanik for any final questions she may have.

Ms. STEFANIK. I am all set, Jim. Thank you to our witnesses.

Mr. LANGEVIN. Okay. All right. Are there any members in the room that I can't see that have not been recognized and would like to ask a question?

Ms. STEFANIK. No. We are all set.

Mr. LANGEVIN. Okay. Well, with that, let me conclude by thanking all the members of the Commission. You did an extraordinary job here today but an even more extraordinary job in the—on the Commission, both Senator King and Congressman Gallagher, our two co-chairs, and Commissioner Murphy, Commissioner Cilluffo, and the rest of the commissioners. Thank you all for your extraordinary work. You have made a major contribution to better protecting the country in cyberspace with your combined efforts, and it is an honor and a privilege to be one of the four Members of Congress joining you on the Commission. It was one of the highlights of my 20 years in Congress to be a part of this effort, and I just—I found it so meaningful and, again, time well spent.

And I like the fact from the very beginning that we determined that we were not going to allow just this to be a report that would sit on a shelf somewhere, but we wanted actionable findings, recommendations that we could implement and, again, achieve meaningful change.

So with that, I thank you all for your participation today, your service to the country.

With that, the hearing now stands adjourned.

[Whereupon, at 2:14 p.m., the subcommittee was adjourned.]

A P P E N D I X

JULY 30, 2020

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

JULY 30, 2020

Opening Statement
Chairman James R. Langevin
Intelligence and Emerging Threats and Capabilities Subcommittee
Review of the Recommendations of the Cyberspace Solarium Commission
July 30, 2020

The Subcommittee will come to order. I would like to welcome the members who are joining today's hearing remotely. Those Members are reminded that they must be visible on screen within the software platform for the purposes of identity verification when joining the proceeding, establishing and maintaining a quorum, participating in the proceeding, and voting. Members participating remotely must continue to use the software platform's video function while attending the proceedings unless they experience connectivity issues or other technical problems that render the member unable to fully participate on camera. If a Member who is participating remotely experiences technical difficulties, please contact the committee's staff for assistance and they will help you get reconnected.

When recognized, video of remotely attending Members' participation will be broadcast in the room and via the television/internet feeds. Members participating remotely are asked to mute their microphone when they are not speaking.

Members participating remotely will be recognized normally for asking questions, but if they want to speak at another time they must seek recognition verbally. In all cases, members are reminded to unmute their microphone prior to speaking. Members should be aware that there is a slight lag of a few seconds between the time you start speaking and the camera shot switching to you.

Members who are participating remotely are reminded to keep the software platform's video function on for the entirety of the time they attend the proceeding. Those Members may leave and rejoin the proceeding. If Members depart for a short period for reasons other than joining a different proceeding, they should leave the video function on. If Members will be absent for a significant period, or depart to join a different proceeding, they should exit the software platform entirely and then re-join it if they return.

Members are also advised that I have designated a committee staff member to, if necessary, mute unrecognized Members' microphones to cancel any inadvertent background noise that may disrupt the proceeding. Members may use the software platform's chat feature to communicate with staff regarding technical or logistical support issues only. Finally, remotely participating Members should see a 5-minute countdown clock on the software platform's display, but, if necessary, I will remind Members when their time is up.

With the logistics clarified, I want to welcome everyone to today's hearing on the findings of the Cyberspace Solarium Commission, a Congressionally mandated commission charged with developing a consensus on a strategic

approach to defending the United States in cyberspace against cyber attacks of significant consequence.

Inspired by Project Solarium, a task force assembled by President Eisenhower in the early 1950s, the Solarium Commission brought together representatives from academia and the private sector with representatives of the Executive and Legislative Branches.

In the spirit of transparency, I want to make clear that I had the privilege of being selected by Speaker Pelosi to serve as one of four elected commissioners, and one of two from the House of Representatives, along with our distinguished Subcommittee colleague Mike Gallagher, who is appearing as a witness before us today. Mr. Gallagher along with Senator King, also with us today, serve as Co-chairs of the Commission, and I am proud to call them both colleagues and friends.

This Subcommittee, more than most, has heard from numerous individuals on the centrality of cyberspace to our modem lives. The novelty of the Solarium's work and its findings is in examining how to secure cyberspace with an emphasis on a whole-of-government approach.

Congress is methodical in its views of jurisdiction, and we are often too focused on viewing our oversight responsibilities exclusively through the lens of committee jurisdictions. What the Solarium has presented in its final report, completed on March 11th of this year, is a blueprint for legislative and executive actions that force the country to break apart the institutional stovepipes.

In this respect, I see the findings of the Solarium Commission as being similar to those of the 9/11 Commission, in that both bodies recognized government siloes that had been artificially constructed and harmed the national approach to addressing cross-cutting issues. Whereas the 9/11 Commission applied this to the problem of terrorism, Solarium applies it to cyberspace.

The Commission's recommendations have resulted in more than twenty provisions in this year's National Defense Authorization Act, passed just last week by the House of Representatives. In that one bill, this Chamber was able to address matters as diverse as Reserve support for military cyber operations, to the cyber insurance marketplace, to the establishment of a Senate-confirmed National Cyber Director.

While we obviously have more work to do, I am proud that the NDAA reflects the whole-of-government action called for by the Commission. I applaud the example set by our European partners in approaching cyber in novel and holistic ways as recently as today with the announcement of the first-ever sanctions issued through the European Union against six individuals and three entities responsible for the "WannaCry", "NotPetya", and "Operation Cloud Hopper" attacks.

As I noted earlier, we have four witnesses appearing in front of the Subcommittee today. In addition to the distinguished gentlemen from Wisconsin and Maine, we are joined by two additional commissioners.

The Honorable Patrick Murphy, a former member of the House Representatives from Pennsylvania, is here today. Commissioner Murphy has

served with distinction as Acting Secretary and Under Secretary of the Army, and today continues his service as the Distinguished Chair of Innovation at the United States Military Academy. Commissioner Murphy was the first veteran of the war in Iraq to be elected to Congress.

Finally, we have Commissioner Frank Cilluffo, who in addition to his service with the Solarium, serves as the Director of Auburn University's McCrary Institute for Cyber and Critical Infrastructure Security. From 2001 to 2003, Commissioner Cilluffo served as Special Assistant to President Bush on Homeland Security and then led the Center for Cyber and Homeland Security at George Washington University.

Before we hear from our witnesses, I will turn to Ranking Member Stefanik for her opening comments.

Opening Statement of Ranking Member Elise Stefanik
7/30/2020

Thank you, Chairman Langevin.

Welcome to our witnesses. Senator King, Congressman Gallagher, Congressman Murphy, and Mr. Cilluffo – it is great to have you before the subcommittee today. I thank you, not only for your leadership and service to the Cyber Solarium Commission, but your long and distinguished records of public service to this country. And although not testifying today, I'd also like to thank Chairman Langevin for his service on the Commission as well as all of the other commissioners not participating today.

I think it's truly remarkable how much ground the Cyber Solarium was able to cover in such a brief period of time. In eleven short months, the commission developed over fifty legislative proposals, twenty-two of which were included in the House-passed version of the National Defense Authorization Act. This impressive commitment reflects the hard work of the commissioners and the staff, and also recognition that we must address these issues immediately.

As is often the case, our nation's strategy, policy, and laws trail the advent of new technology. This is true of many emerging disciplines, but none as consequential as cyberspace. The debilitating cyber-attack on Estonia in 2007, the devastating Office of Personnel Management data breach in 2014, and the cyber-attack on the city of Atlanta in 2018 - all should have served as wake-up calls for the need of a comprehensive strategy to bolster our cyber defenses, to deter hostile action in cyberspace, and to build more resilient public and private cyber infrastructure.

The threat actors in cyberspace are as diverse as the tools and tradecraft they employ to infiltrate and attack our networks. And while we must maintain a flexible and adaptable approach to meet the evolving threat, we must also communicate an unequivocal position that demonstrates our willingness to defend the United States in cyberspace and impose costs on our adversaries, if, and when deterrence fails. I firmly believe we must simultaneously strengthen our cyber defenses and demonstrate our unwavering resolve to challenge our adversaries in cyberspace.

I appreciate the commission's recognition of this as well. Deterrence alone is not sufficient, especially with the challenges of timely attribution and the notional "fog of war" in cyberspace. The United States must proactively take steps to increase the resilience of our networks and our nation's critical infrastructure. This task is not one that the federal government can take on alone. Any effort to bolster our cybersecurity must be done in partnership with the private sector, our cities and states, and our critical infrastructure operators. The commission's recommendations that were included in the NDAA address this reality; accountability, information sharing, collaboration, and more timely response and

mitigation to cyber incidents are all critical attributes that we must reinforce and strengthen.

While the Commission's remit is coming to an end, the work is not done. We have a long road ahead to see these through conference and fully implement these changes. I look forward to ensuring the Cyber Solarium commission's recommendations are translated into concrete action.

We have a lot to talk about, so thank you again to each of our witnesses. I yield back.

Testimony of:
The Honorable Angus King,
The Honorable Mike Gallagher,
The Honorable Patrick Murphy,
Mr. Frank Cilluffo

Commissioners of the
Cyberspace Solarium Commission

Before the United States House of Representatives
Committee on Armed Services
Subcommittee on Intelligence and Emerging Threats and Capabilities

"Review of the Recommendations of the Cyberspace Solarium Commission"

July 30, 2020

INTRODUCTION - INTENT OF THE COMMISSION

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

In addressing the NDAA's tasking, the Commission looked at the challenges the nation faces in cyberspace. 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 CHALLENGE

For the last twenty years, adversaries have used cyberspace to attack American power and interests. The more connected and prosperous our society has become, the more vulnerable we are to rival great powers, rogue states, extremists, and criminals. These attacks on America occur beneath the threshold of armed conflict and create significant challenges for the private sector and the public at large.

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

Securing the nation in the 21st century requires an interconnected system 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 over a hundred million Americans.

Russia targets the integrity and legitimacy of elections in multiple countries while actively probing critical infrastructure. In spring 2014, Russian-linked groups launched a campaign to disrupt Ukrainian elections that included attempts at altering vote tallies, disrupting election results through distributed-denial-of-service (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.

Iran and North Korea attack the 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 advanced persistent threat groups (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, including temporarily disrupting 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 malicious code on the dark web. In 2019, ransomware incidents grew by over 300% 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 at their most vulnerable state. Remote access and the expansion of the

work-from-home economy continues to increase the threat vectors for criminal actors as the world changes to meet the needs of a global pandemic.

STRATEGIC APPROACH

The strategy put forth by the 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 and nonstate actors 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**. The public and private sectors, along with key international partners, must collaborate to build resilience and reshape the cyber ecosystem in a manner that increases its security, while imposing costs against malicious actors and preventing attacks of significant consequence.

Cyber deterrence is not nuclear deterrence. The fact is, no action will stop every hack. Rather, the goal is to reduce the severity and frequency of attacks by making it more costly to successfully attack American interests 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. It requires international engagement and collaboration with the private sector.

Layered cyber deterrence emphasizes working with the private sector to efficiently coordinate how the nation responds with speed and agility to emerging threats. The Federal government alone cannot 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. These three deterrent layers are supported by six policy pillars that organize the 82 recommendations that collectively represent the means to implement our strategy.

RECOMMENDATIONS AND FOCUS OF OUR EFFORT

First, the Commission found that the Federal government lacks consistent and institutionalized leadership, as well as a cohesive, clear strategic vision on cybersecurity. As a result, the Commission recommends that Congress establish a **National Cyber Director** (NCD) in the Executive Office of the President to centralize and coordinate the cybersecurity mission at the national level. The NCD 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 NCD be staffed with approximately 75 to 100 full-time employees, 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. Additionally, the NCD office would support the President by formulating, recommending, integrating, and implementing policies and strategies to improve the nation's ability to operate in cyberspace. The position would provide clear leadership in the White House and signal cybersecurity as an enduring priority in U.S. national security strategy. Additionally, this position would serve as a mechanism to improve effective congressional oversight of this inherently interdisciplinary policy challenge.

Second, 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 the United States has the appropriate force structure and capabilities in cyberspace. Despite having reached full operational capability in 2018, our Commission found that a gap remains between the current CMF and the scale and scope of adversary threats, as well as mission requirements. The CMF is where the bulk of the capabilities exist within the DoD to counter malicious adversary campaigns and impose costs. Currently, the CMF has 133 teams comprising a total of about 6,200 individuals. However, these requirements were determined in 2013, before the United States fully appreciated the scope and scale of the current threat in cyberspace, and before the DoD developed the strategy of defend forward, which has placed additional mission requirements on the CMF. A force structure assessment of the CMF, as well as an assessment of the resource implications for the various intelligence community agencies that serve combat support agency roles, will work to ensure the CMF has sufficient forces, capabilities, and streamlined decision-making processes and authorities to achieve its objectives.

Third, given the improvements in adversary cyber capabilities, the Commission was concerned with ensuring the United States can still 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 that our weapon systems–which form the bedrock of our military advantage and the foundation for deterrence–will work when needed, and as intended. Given

that so much of our military capabilities rest on cyber infrastructure, a priority of our Commission was ensuring 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. 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.** In the Fiscal Year 2016 NDAA, Congress directed DoD to assess the cyber vulnerabilities of each major weapon system. However, gaps remain that must be remediated. For example, there is no permanent process to periodically assess the cybersecurity of fielded systems. Additionally, the current requirement is to assess the vulnerabilities of *individual* weapons platforms. While this is important, it is also crucial to evaluate how a cyber intrusion or attack on one system could affect the entire mission—in other words, to assess vulnerabilities at a systemic level.

Fourth, 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 the Commission recommends Congress request the DoD in 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. 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.

Fifth, 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. The Commission recognizes that the strategic employment of information is intertwined with conducting cyberspace operations to influence adversary decision-making.

Sixth, 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.

Seventh, the government must continue to improve the resourcing, authorities, and organization of the Cybersecurity and Infrastructure Security Agency (CISA) in its role as the primary Federal agency responsible for critical infrastructure protection, security, and resilience.

The Commission recommends **empowering CISA** with tools to strengthen public-private partnership. Of particular value would be the authorities needed to aid in responding to attempted attacks on critical infrastructure from a variety of actors, ranging from nation-states to criminals. Currently, the U.S. government's authorities in this context are limited exclusively to certain criminal contexts, where evidence of a compromise exists, and do not address instances in which critical infrastructure systems are vulnerable to a cyberattack. To address this gap, Congress should grant **CISA subpoena authority** to enable CISA to more efficiently and effectively notify private and public sector entities put at risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States, while ensuring appropriate liability protections for cooperating private-sector network owners.

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

Ninth, the United States must take immediate steps to ensure our critical infrastructure sectors can withstand and quickly respond to and recover from a significant cyber incident. Resilience against such attacks is critical in reducing benefits that our adversaries can expect from their operations–whether disruption, intellectual property theft, or espionage. As a whole, the government should more thoroughly plan for what we know to be an eventuality, as we currently do in the military domain. Congress should direct the executive branch to develop a **Continuity of the Economy** Plan. This plan should include the Federal government, state, local, tribal, and territorial (SLTT) entities and private stakeholders who can collectively identify the resources and authorities needed to rapidly restart our economy after a major disruption. In addition, the Commission recommends passing a law to endow the Secretary of the Department of Homeland Security with the authority to declare a **Cyber State of Distress** tied to a **Cyber Response and Recovery Fund**, giving the government greater flexibility to scale up and augment its own capacity to aid the private sector when a significant cyber incident occurs. These changes will ensure the infrastructure that supports our most critical national functions can continue to operate amidst disruption or crisis.

Tenth, 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 partners and allies to enforce those norms. This high-level leadership is required to

coordinate efforts to shape behavior in cyberspace and ensure that values like openness, interoperability, reliability, and security remain an integral part of the future of the internet.

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.

INTERSECTION BETWEEN PANDEMIC AND CYBER CRISES

The COVID-19 pandemic has served as a wakeup call for the United States as it both illustrates the challenge of ensuring resilience and continuity in a connected world, and it demonstrates the challenge in responding to non-traditional national security events. It is an example of a crisis that spreads rapidly through the system, stressing everything from emergency services and supply chains to basic human needs. The pandemic has produced cascading effects and high levels of uncertainty. This situation undermines normal policy-making processes and forces decision makers to craft hasty and ad hoc emergency responses in the absence of fulsome preparation and mitigation measures taken well ahead of time. Complex emergencies, like the pandemic, that rely on coordinated action beyond traditional agency responses and processes illustrate what the Commission saw as an acute threat to the security of the United States.

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

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

established, exercised relationships and plans, highlighting the importance of **Continuity of the Economy** planning.

CONCLUSION

The United States and its allies and partners have experienced a number of cyberattacks that clearly indicate the need for improved critical infrastructure resilience. Some, like the Dyn DDoS attack in 2016 disabled large portions of our internet, grinding businesses to a halt for several hours. Others, like WannaCry and NotPetya, locked critical institutions out of their systems, placing lives in hospitals at risk and disrupting critical services. Today, the nation faces another wakeup call in the form of the coronavirus crisis, which has provided the clearest depiction yet of a massive disruption of our economy.

The recommendations put forward by the Commission are an important first step to denying adversaries the ability to hold the United States at risk in cyberspace and will be critical to our efforts to re-establish deterrence in cyberspace. We believe that deterrence is an enduring American strategy, but it must be adapted to address how adversaries leverage new technology and connectivity to attack the United States. Cyber operations have become a weapon of choice for adversaries seeking to hold the U.S. economy and national security at risk. Near peer adversaries such as China and Russia are attempting to reassert their influence regionally and globally, using cyber and influence operations to undermine U.S. security interests. The concept of deterrence must evolve to address this new strategic landscape.

Reducing the scope and severity of these adversary cyber operations and campaigns requires adopting the Commission's strategy of layered cyber deterrence to improve our ability to defend our critical infrastructure. To this end, we believe that Congress and the Executive Branch must prioritize a selection of the Commission's recommendations that include: strengthening the government with a National Cyber Director, empowering CISA, creating a new Joint Cyber Planning Office and improving intelligence support to the private sector; while also building resilience with Continuity of the Economy Planning.

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? And what policies and legislation are required to implement that strategy? The Commission has completed its Congressionally assigned task to develop a new strategic approach, and corresponding legislative proposals. We now need your leadership as you move into conference the 2021 NDAA with your Senate counterparts, in order to enact the critical legislative proposals that will empower and resource the government and the private sector to act with speed and agility to secure our cyber future.

Senator Angus King
Chairman, Cyberspace Solarium Commission

The Commission's Co-Chair, Senator Angus S. King Jr., (I-ME) was appointed to the Commission by Senate Minority Leader Chuck Schumer (D-NY).

Senator King was sworn in as Maine's first Independent United States Senator, filling the same seat once held by storied Maine leaders Edmund Muskie, George Mitchell, and Olympia Snowe. Now in his second term, Senator King is a member of the Armed Services Committee, the Select Committee on Intelligence, the Committee on Energy and Natural Resources, and the Committee on Rules and Administration.

In his time in the Senate, Senator King has worked to strengthen America's national security, conducted critical oversight of the nation's Intelligence Community, supported common-sense budget priorities that promote prosperity, fought the national opioid and heroin epidemic, coordinated efforts to revitalize Maine's forest economy, advocated for policies that contribute to cleaner, cheaper energy and mitigate climate change, chaired hearings on the corrosive effect of unchecked money in politics, fought to improve access to health care, worked to strengthen the government's support of veterans, and promoted increased access to critical community resources like rural broadband.

Senator King has already achieved significant legislative victories. In 2013, for example, when students across America faced the financial threat of a significant increase in their student loan interest rates, Senator King spearheaded the effort to draft and pass through both the Senate and House compromise legislation that not only averted rate hikes, but that also put the program on long-term stable financial footing. That hard-fought bipartisan solution, the Student Loan Certainty Act of 2013, has been projected to have saved millions of students across the country more than $50 billion in interest payments over the past five years.

In fact, it is in small working groups like this that Senator King has concentrated much of his work. He co-founded the Former Governors Caucus, which brings together the Senate's former Governors to chart pragmatic approaches to solutions, and is an active member of the Senate Arctic Caucus, which focuses on Maine and America's growing interest in the Arctic as well as the newly-formed bipartisan climate solutions caucus. Senator King also tries to informally bridge the partisan divide in Washington by frequently bringing his colleagues on both sides of the aisle to his home for barbeque dinners, where the purpose is simply getting to know one another. The bonds that are formed through these relationships often lay the foundation for successful legislation.

Senator King also served as the 72nd Governor of Maine, and during his two terms in the Blaine House, he concentrated on economic development and job creation. Then-Governor King also achieved significant reforms in education, mental health services, land conservation, environmental protection, and the delivery of state services. He was re-elected in 1998 by one of the largest margins in Maine's history.

Representative Mike Gallagher
Chairman, Cyberspace Solarium Commission

Representative Michael "Mike" J. Gallagher was appointed to the Commission by then Speaker of the House Paul Ryan (R-WI).

Mike Gallagher was first elected in 2016 to represent Wisconsin's 8th District in the U.S. House of Representatives. Mike is a 7th generation Wisconsin native, born and raised in Green Bay. Mike joined the United States Marine Corps the day he graduated from college and served for seven years on active duty as a Counterintelligence/Human Intelligence Officer and Regional Affairs Officer for the Middle East/North Africa, eventually earning the rank of Captain. He deployed twice to Al Anbar Province, Iraq as a commander of intelligence teams, served on General Petraeus's Central Command Assessment Team in the Middle East, and worked for three years in the intelligence community, including tours at the National Counterterrorism Center and the Drug Enforcement Agency.

Mike also served as the lead Republican staffer for Middle East, North Africa and Counterterrorism on the Senate Foreign Relations Committee. Prior to taking office, Mike worked in the private sector at a global energy and supply chain management company in Green Bay.

After earning his bachelor's degree from Princeton University, Mike went on to earn a master's degree in Security Studies from Georgetown University, a second in Strategic Intelligence from National Intelligence University, and his PhD in International Relations from Georgetown.

Mike currently serves on the House Armed Services, and Transportation and Infrastructure Committees.

Patrick Murphy
Commissioner, Cyberspace Solarium Commission

The Honorable Patrick J. Murphy, was appointed to the Commission by then Minority Leader of the House Nancy Pelosi (D-CA).

Patrick Murphy was America's first Iraq War veteran elected to the U.S. Congress, and later served as the Acting Secretary and 32nd Under Secretary of the Army.

Secretary Murphy is currently the Distinguished Chair of Innovation at the United States Military Academy at West Point, a Senior Fellow at the Association of the U.S. Army, a member of the Board of Directors at BAE Systems Inc., a media executive, and the Executive Chairman of WorkMerk, an employee engagement company focused on the future of work.

As the Acting Secretary and Under Secretary, he led the management and operation of the Army—a Fortune 10-sized organization and the Nation's second largest employer of over 1.3 million with a budget of $148 billion. His focus on transforming a more innovative and responsive workforce led to an expansion of the Soldier for Life initiative, which saved $340M in FY16, and reaching recruitment goals for the first time in five years with over 130K millennials hired.

Secretary Murphy also facilitated unprecedented public-private partnerships generating over $250M in savings, from Major League Baseball to 20th Century Fox. His aggressive and authentic use of social media to tell the Army story helped lead to an 18% growth across all platforms.

Founder of an award-winning (CLIO, Sherwood) television & film production company, Taking the Hill, specializing in military & veteran projects helping tell the story of over 22 million American Veterans. Projects include the critically acclaimed Stephen Spielberg film 'Thank You For Your Service' (Dreamworks/Universal, 2017), Unconquered (Epix, 2018), Almost Sunrise (PBS, 2017), & previously as host/executive producer for 'Taking The Hill' (MSNBC 2011–2015) and 'The Triumph Games' (CBS Sports, 2015–2016). He authored the book Taking the Hill: From Philly to Baghdad to the United States Congress (Henry Holt, 2008).

He is a graduate of King's College Army ROTC Program and the Widener University Commonwealth School of Law, where he currently serves as a Trustee. He has two young children, Maggie and Jack, and resides in Pennsylvania.

Frank Cilluffo
Commissioner, Cyberspace Solarium Commission

Mr. Frank J. Cilluffo was appointed to the Commission by then Speaker of the House Paul Ryan (R-WI).

Frank Cilluffo is the director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security.

Cilluffo is routinely called upon to advise senior officials in the executive branch, U.S. Armed Services, and state and local governments on an array of matters related to national and homeland security strategy and policy. In addition to briefing Congressional committees, he has testified before Congress on dozens of occasions, serving as a subject matter expert on policies related to cyber threats and cybersecurity, counterterrorism, security and deterrence, weapons proliferation, organized crime, intelligence and threat assessments, emergency management, and transportation security. Similarly, he works with U.S. allies and organizations such as NATO and Europol. He has presented at a number of bilateral and multilateral summits on cybersecurity and countering terrorism, including the U.N. Security Council.

Following the Sept. 11, 2001 terrorist attacks, Cilluffo was appointed by President George W. Bush to serve as a Special Assistant to the President on Homeland Security. There, he was involved in a wide range of homeland security and counterterrorism strategies, policy initiatives and served as a principal advisor to Tom Ridge, and directed the president's Homeland Security Advisory Council.

Cilluffo then joined George Washington University in 2003, establishing the Center for Cyber and Homeland Security as a prominent nonpartisan "think and do tank" dedicated to building bridges between theory and practice to advance U.S. security. He served as an associate vice president where he led a number of national security and cybersecurity policy and research initiatives. He directed the Center for Cyber and Homeland Security and, with the School of Business, launched the university's World Executive MBA in Cybersecurity program. Prior to his White House appointment, Cilluffo spent eight years in senior policy positions with the Center for Strategic and International Studies, a Washington-based think tank. There, he chaired or directed numerous committees and task forces on homeland defense, counterterrorism and transnational organized crime, as well as information warfare and information assurance.

He has published extensively in academic, law, business and policy journals, as well as magazines and newspapers worldwide. His work has been published through ABC News, Foreign Policy, The Journal of International Security Affairs, The National Interest, Parameters, Politico, Studies in Conflict and Terrorism, USA Today, The Washington Quarterly, The Washington Post, and the Wall Street Journal. He has served as an on-air consultant for CBS News and as a reviewer for a number of publications and foundations. He is also a member of the Department of Homeland Security's Advisory Council.

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

JULY 30, 2020

QUESTIONS SUBMITTED BY MS. HOULAHAN

Ms. HOULAHAN. The Commission's recommendation #1.5 regards recruiting and retaining a strong cyber workforce. I really appreciate what you've put forward. A different congressionally mandated group, the National Commission on Artificial Intelligence recommended the establishment of a U.S. Digital Service Academy that would be a dedicated effort to train the next generation of tech talent. Is this a recommendation you would agree with?

Mr. GALLAGHER and Mr. CILLUFFO. The government workforce is short more than 33,000 cybersecurity workers in a workforce of nearly 100,000. Simply expanding government recruitment efforts is not sufficient to provide the cybersecurity workforce needed to protect national security. Rather, the nation's cybersecurity workforce development ecosystem must grow as a whole. Currently, innovative programs are taking the first steps toward addressing this need by building partnerships between educators, government, and industry, but we need to do more. The Cyberspace Solarium Commission studied many federal government hiring programs, private sector initiatives, and educational efforts, and recommended that it should invest in existing programs such as the CyberCorps: Scholarship for Service (SFS), which is a program ripe for expansion, as well as the FBI Cyber STEM program and CISA's Cybersecurity Education Training Assistance Program on a national scale.

The SFS is a joint program between OPM, the NSF, and DHS that helps students finance their education in cyber-related topics in exchange for a term of service working for a federal or state, local, or tribal government upon graduation.[1] The program works much like the Reserve Officer Training Corps (ROTC) program on many U.S. campuses, only better—it awards grants to participating universities, which then award scholarships to students while also using a portion of the funding to build out the university's cyber-focused programming. As a result, the program strengthens educational offerings on cyber topics at the same time that it recruits and develops students who are prepared for federal cyber service. Currently, there are 85 participating universities and community colleges offering SFS scholarships. The program requires that students may pursue degrees that are a "coherent formal program that is focused on cybersecurity," and it has supported students working toward a bachelor's, master's, or research-based doctorate degree focused on cybersecurity.[2] The recent expansion of the SFS program through the Community College Cyber Pilot Program extends eligibility to students pursuing an associate's degree or specialized program certifications in the field of cybersecurity as well, provided that the students already have a bachelor's degree or are military veterans.[3]

The program has graduated about 275 students per year in recent years,[4] and since its creation in 2000, it has placed 3,600 CyberCorps graduates in public-sector cybersecurity jobs in more than 140 different government organizations.[5] These graduates have brought cyber expertise to the government across a variety of cybersecurity areas, including cyber policy and strategy, security architecture, and cyber operations planning. Because a limited percentage of students can fulfill their service obligation in state, local, or tribal governments as well as in the federal govern-

---

[1] "CyberCorps: Scholarship for Service," Office of Personnel Management, accessed July 7, 2020, https://www.sfs.opm.gov/default.aspx.

[2] "CyberCorps: Scholarship for Service, Overview," Office of Personnel Management, accessed August 4, 2020, https://www.sfs.opm.gov/ProspectiveStud.aspx; "CyberCorps: Scholarship for Service, Students: Participating Institutions," Office of Personnel Management, accessed August 4, 2020, https://www.sfs.opm.gov/ContactsPI.aspx.

[3] "Community College Cyber Pilot Program (C3P)," National Science Foundation, Division of Graduate Education, https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505573.

[4] More specifically, CyberCorps SFS is projected to graduate 380 students in 2020. It graduated 307 students in 2019, 324 in 2018, 290 in 2017, 245 in 2016, and 211 in 2015. Data provided by NSF.

[5] OPM, "CyberCorps: Scholarship for Service: History/Overview." At the time of access, the data cited was available at https://www.sfs.opm.gov/Overview-History.aspx; it now can be found at https://web.archive.org/web/20200608183458/https://www.sfs.opm.gov/Overview-History.aspx and https://www.nass.org/sites/default/files/2019%20Summer/presentations/presentation-sfs-summer19.pdf.

ment, the program also provides the opportunity for a limited percentage of graduates to work in public education. This helps address the national dearth of teachers able to provide cybersecurity instruction.[6]

Although the program has an impressive track record, the Commission believes that—given the country's inability to fill tens of thousands of cybersecurity jobs in both the government and private sector—the number of SFS participants should be much higher (Report Recommendation 1.5). Accordingly, taking practical steps toward increasing the number of students also requires increasing the number of participating institutions and expanding university- and federal-level outreach about the program. The Commission recommends a goal of graduating 2,000 CyberCorps students per year. To reach that target, the Commission advocates for SFS's budget to be increased 20 percent above inflation annually over a 10-year period to support scholarships to additional students and the programmatic efforts needed for expansion. To help jumpstart that budget growth, the Commission recommends increasing funding for the CyberCorps SFS program by $20 million in FY2021.

As your question stated, another Congressionally-mandated group, the National Commission on Artificial Intelligence recommended the establishment of a U.S. Digital Service Academy that would be a dedicated effort to train the next generation of tech talent. A brick and mortar effort similar to the service academies. We believe this idea has exceptional merit and should be studied and, if all expectations are met, funded. This USDSA would service as a "service academy" partner to the "ROTC" like efforts of the CyberCorps SFS program The U.S. military benefits from both—the ROTC graduates are on the whole significantly cheaper, but the service academy graduates come with a better grounding in government (service) processes and efforts. An unusual twist is that we would need to consider whether USDSA would have the same flexibilities as CyberCorps SFS—graduate degrees, associate degrees, and limited year scholarships—many SFS are two and three year scholarship students, who are not selected until they have demonstrated some college success. A USDSA study should review and identify the unique attributes that the USDSA would bring to the effort. Moreover, it is important to weave this program into the existing policy proposals and efforts ongoing at various agencies, including DHS, which has proposed a Cyber Workforce Institute. The nation needs one cohesive strategy with streamlined implementation and funding to ensure that agencies pull in the same direction, instead of at cross purposes.

With the high number of annual openings required to be filled, it is likely that the U.S. government needs both an expanded CyberCorps SFS and a brick and mortar cyber institute.—A study to work out the details on all these proposals would provide needed strategic direction as would efforts to determine how to grow the CyberCorps SFS to 2000 plus graduates a year as recommended by the Cyberspace Solarium Commission.

Ms. HOULAHAN. Did you look into current contracting procedures, and do you believe the Department is missing out on innovative cyber solutions due to current contracting policies?

Mr. GALLAGHER and Mr. CILLUFFO. Government contracting is an extremely difficult and complex area, and while it was not our primary focus, we did attempt to make some recommendations which would enhance and streamline government contracting for the cyber domain.

The Commission recommends the executive branch direct the Federal Acquisition Regulation Council (FARC) and the Office of Management and Budget to update its cybersecurity regulations in the Federal Acquisition Regulation (FAR) and cybersecurity guidance under Federal Information Security Management Act at least every five years, to account for changing cybersecurity standards, and explore ways to integrate and fully account for existing models and frameworks, such as the Cybersecurity Maturity Model Certification, in the FAR. In addition, the FARC should be directed to update the FAR to require that federal civilian agency contractors adhere to the contractor-exclusive Binding Operational Directive issued by DHS.[7]

The Commission also recommends the executive branch update to Federal Procurement Regulation and Guidelines, including the FAR, to require National Cybersecurity Certification and Labeling Authority certifications and labeling for certain information technology products and services procured by the federal government to

[6] In fact, legislation has been proposed for inclusion in S.4049, the National Defense Authorization Act for Fiscal Year 2021, explicitly permitting up to 10 percent of SFS graduates to fulfill their service obligation in education roles in higher education institutions that participate in the SFS program.

[7] The Binding Operational Directives (BODs) identify requirements for federal agencies in the executive branch. Each BOD prescribes a set of actions that agency chief information security officers or their equivalents must take to manage their enterprise networks.

enable the broader adoption of Certification and Labeling across the nation. The executive branch should be required to report to Congress on its decision to require National Cybersecurity Certification and Labeling Authority certifications and labeling within the FAR, the extent of these requirements, or an explanation if no action was taken. This recommendation is necessary because the U.S. government is institutionally and legally limited in its ability to attest and certify that products adhere to security standards, and third-party efforts to fill this gap lack sufficient scale, funding, and maturity to enact meaningful change in the marketplace.[8]

Federally procured information technology fully accounts for identified good security practices for building secure software and systems, such as those offered by NIST's Secure Software Development Framework[9] and the ISO/IEC 27000 standards family.[10] When developing requirements, the council should take into account lessons learned with NIST Special Publication 800.171, comments from DOD's Cybersecurity Maturity Model Certification, rulings or comments of the Federal Acquisition Security Council, and the ISO/IEC 27000 standards.

Providers of information technology submit software transparency and software bills of materials for the systems they provide in support of government missions in line with the certifications and labels developed by the National Cybersecurity Certification and Labeling Authority (recommendation 4.1).[11]

Upon the development of cybersecurity insurance policy certifications (recommendation 4.4), U.S. government contractors maintain a certified level of cybersecurity insurance and explore whether the Cybersecurity Maturity Model Certification should be updated to require cybersecurity insurance.

Additionally, to enhance the flexibility and agility of U.S. Cyber Command in a dynamic operating environment, Congress should direct in the FY2021 NDAA that the Department of Defense submit a budget justification display that includes a Major Force Program (MFP) category for the training, manning, and equipping of U.S. Cyber Command. According to 10 U.S. Code § 238, DOD is required to submit to Congress a budget justification display that includes an MFP category for the Cyber Mission Force. However, this law was enacted in 2014, before U.S. Cyber Command was elevated to a unified combatant command. Therefore, there is a need for a new budget justification display that establishes an MFP category for U.S. Cyber Command. A new MFP funding category for U.S. Cyber Command would provide it with acquisition authorities over goods and services unique to the command's needs. It should also provide a process to expeditiously resolve Combatant Command/Service funding disputes, consistent with the intent of DOD Directive 5100.03.[12] This would be analogous to the MFP funding category for U.S. Special Operations Command, which was created to support comparable needs for operational adaptability.

○

[8] Several nongovernmental initiatives, such as Digital Standard and the Cyber Independent Testing Laboratory, are aimed at testing and providing security information for consumer IT and IoT devices. NIST, under Section 401 of the Cybersecurity Enhancement Act of 2014, is tasked with coordinating the development and dissemination of standards and best practices for cybersecurity.

[9] Donna Dodson, Murgiah Soppaya, and Karen Scarfone, "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework" (National Institute of Standards and Technology, 2019), https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf.

[10] International Organization for Standardization, "ISO/IEC 27001 Information Security Management" International Organization for Standardization, https://www.iso.org/isoiec-27001-information-security.html.

[11] "NTIA Software Component Transparency," National Telecommunications and Information Administration, September 5, 2019, https://www.ntia.doc.gov/SoftwareTransparency.

[12] U.S. Department of Defense Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands" (February 9, 2011; incorporating Change 1, September 7, 2017), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510003p.pdf.