Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON THE FINDINGS AND RECOMMENDATIONS OF THE CYBERSPACE SOLARIUM COMMISSION

Tuesday, August 4, 2020

Washington, D.C.

ALDERSON COURT REPORTING
1111 14TH STREET NW
SUITE 1050
WASHINGTON, D.C. 20005
(202) 289-2260
www.aldersonreporting.com

OPENING STATEMENT OF HON. MIKE ROUNDS, U.S. SENATOR FROM SOUTH DAKOTA

Senator Rounds: Well, good afternoon.

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

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

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

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

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

I'd also like to recognize former SASC Policy Director Mark Montgomery, who serves -- or who served as Executive Director of the Commission.

Section 1652 of the Fiscal Year 2019 NDAA established the Cyberspace Solarium Commission to study alternative strategies for defending the United States against malicious cyberactivity and advancing its national interests in cyberspace. Among the strategies to be evaluated were cyber deterrents, persistent engagement, and compliance with international norms. The Commission has produced an impressive report that advocates a combination of all three: deterrence by denial and rapid attribution, deliberate shaping of international norms through aggressive diplomacy, and continued persistent engagement of malicious cyber adversaries.

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

These recommendations are valuable contributions to the debate on what policies, programs, and organizational

constructs will best advance the Nation's cybersecurity. I am proud that we were able to incorporate 11 of these recommendations into the committee mark of the NDAA, with several additional recommendations which were, unfortunately, outside of our jurisdiction, but were incorporated later on the floor discussion.

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

Since its establishment, this subcommittee has focused on improving coordination among the many relevant entities within the Department of Defense to assure synchronized efforts in implementing and executing their cyberspace missions. I believe that the Principal Cyber Advisor within

the Office of the Secretary of Defense has been particularly effective at performing that particular oversight and coordination role, and advising the Secretary of Defense. This has been accomplished without the establishment of a large bureaucracy, and without creation of yet another cyber stovepipe within the DOD.

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

Second, I hope to better understand the recommendations the Commission provided regarding the Department of Defense's cybertargeting. Did the Commission see Cyber Command's current plans and operations as matching the Commission's recommendations in cyber deterrence and

persistent engagement? Did it find the Department's aspirations for persistent engagement of adversaries to be realistic?

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

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

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

STATEMENT OF HON. JOE MANCHIN, U.S. SENATOR FROM WEST VIRGINIA

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

Thank you, Senator Rounds.

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

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

Thank you, Chris, for being here, too.

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

A commission of this type is intended not just to educate Congress, the executive branch, and the public. The intent is to forge a consensus on what needs to be done to

fix the problems the Commission identifies. However, too often those recommendations are too vague or difficult for Congress to legislate on. The Commission spent a lot of time and effort turning those recommendations into actual draft legislation text. This was an immensely important decision. If you have to turn an idea into bill language, you have to really think it through, and the result has to be compatible with the main purpose of Congress, which is drafting laws.

To be sure, we have had to modify these recommendations, sometimes significantly. But, without those legislative drafts, much of the Commission's work might already be collecting dust on someone's shelf. Instead, a vast majority of the Commission's recommendations were included, in one form or another, in the NDAA bills passed by the House and Senate, including a significant number of recommendations that crossed the jurisdictional lines of multiple committees. This is no mean feat. Getting approval across multiple committees for legislative amendments on the floor of the House and Senate is extremely hard, something that Senator King and Representative Gallagher know very well and were able to do it.

One of the main and most influential Commission recommendations is the creation of a National Cyber Director. This recommendation is not popular with the

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

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

First, the recommendation to require reporting of all critical infrastructure entities to the Department of Homeland Security. While it's important that we do all that we can to effectively respond to cyberthreats in the timeliest manner, we must do so without interrupting established cyberthreat reporting. As Ranking Member of the

Energy and Natural Resources Committee, a prime example are critical energy infrastructure entities. They should still report through their established chains with the Department of Energy, and that intelligence should be made available to the eventual National Cyber Director.

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

Before turning to our witnesses for opening statements,

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

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

Senator Rounds: Thank you, Senator Manchin.

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

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

Senator King: Thank you, Mr. Chairman.

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

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

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

The Commission, as you mentioned, Mr. Chairman, was set up almost 2 years ago in the National Defense Authorization Act, and our mission was to develop a comprehensive cyberstrategy for the country, and recommend how it should

be implemented. There were 14 members. And I think part of the success of the Commission rests upon how it was structured. There were 14 members: four members of Congress, and then there were four members from the executive, from the relevant agencies, and six members from the private sector. We had over 30 meetings. We had 90-percent attendance at our meetings. We met in this building, just downstairs, over and over. We had hundreds of documents, witnesses, and an immense amount of literature search and review of all of the ideas that could be brought before us on these subjects.

I'm proud to say that the work of this Commission was entirely nonpartisan. In fact, to this day, other than the four members of Congress whose -- who wear their party labels on their sleeves, I have no idea of the party affiliation of any of the other 10 members of the Commission, and I can honestly say that, in all of those 30 meetings, there was not a single comment, discussion, question that suggested any partisan content or any kind of partisan point of view in our committee's -- in our Commission's discussions. Four-hundred interviews, we came up with 82 recommendations; 57, as Senator Manchin mentioned, were turned into actual legislative language.

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

and response:

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

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

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

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

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

remarks.

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

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

I'd like to introduce both of those documents into the

record, with the permission of the Chair.

Senator Rounds: Without objection.

Senator King: Thank you.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

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

Thank you, Mr. Chair.

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

Senator Rounds: Thank you, Senator King.

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

Mr. Gallagher: I am. Can you hear me?

[Laughter.]

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

All right, let's try that again.

Mr. Gallagher: Okay. Hopefully, that's a little bit better, not too jarring.

Senator Rounds: Much, much better. Thank you.

Welcome.

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

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

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

[Laughter.]

Mr. Gallagher: So, thank you for letting me return to my roots in the Senate.

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

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

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

Secondly, I would like to highlight the necessity for continuity-of-the-economy planning. We need resilience and redundancy in our critical infrastructure. And national resilience necessitates planning. I would submit that the pandemic has shown, not only that our economy is vulnerable to widespread disruption, but to the potential impact that economic disruption has on Americans. And, just as we thought through the unthinkable in the earliest parts of the Cold War, so, too, now we need to think through the unthinkable, in terms of how we would rapidly recover in the

wake of a massive cyberattack so that we have the ability to strike back with speed and agility against whoever chooses to test us.

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

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

simply not getting the job done, and the time to act is now.

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

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

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

Mr. Inglis, please proceed.

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

General Inglis: Thank you, Chairman Rounds, Ranking Member Manchin, and all the distinguished committee members, for the privilege of testifying before you today on the recommendations from the Cyberspace Solarium Commission.

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

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

This committee has done much to improve both the Nation's understanding and the military's preparedness to deal with the challenges of cyberspace, and yet we must do still more, for military cyber power is only one of the many

instruments of power that must be applied to achieve our aims in and through cyberspace. As you well know, cyberspace is inextricably linked to every other domain of human interest, such that, while cyber, comprised of both technology and the humans who make use of it, is an instrument of power in its own right, all other instruments of power increasingly depend upon a properly functioning cyberspace for their efficient and effective operation.

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

Our adversaries have gone to school on us. They routinely seize the initiative of choosing the time, the place, the manner of their transgressions without regard to imagined or commonly accepted boundaries between the pervasively interconnected swaths of cyberspace that are, again, operated by individuals, the private sector, and governments, as a collective whole. Absent a consistent,

proactive, and joined-up effort on our side that gives a premium to preparation, integration, and collaboration, we will fall further behind.

To that end, the United States needs a leader to act as the President's principal advisor on cybersecurity and associated emergency technology issues, and to coordinate the Federal Government response. Our experiencing -- our experience as a Nation in preparing for kinetic attacks has richly informed doctrine and plans on how the military will respond to kinetic attack, to include the supported and supporting roles that other instruments of national power would play under various scenarios. We're not in the same place with respect to cyberattack, where the military instrument may not be the singular, or even the supported, instrument of national power, let alone the need to consider the actions of the private sector, which typically maintains and operates the front line of cyberattacks as they maintain and operate over 85 percent of what we know as cyberspace.

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

authority of those commanders.

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

Finally, I would simply note that cyberspace exists inexorably in the presence of adversaries. The contested nature of cyberspace, where the U.S. is challenged by adversaries who can and do attack us on every front -- in our homes, in our places of business, and within our critical infrastructure -- names -- needs the same essential

coherence in national strategy, defined roles and responsibilities, and in the propensity to collaborate based on leadership that connects and supports the various players to a national strategy.

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

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

Senator Rounds: Thank you very much for your testimony.

And I think -- let me begin. I do appreciate the work that this Commission has done. You've not only started out with a whole series of proposals, but, when we asked you to go back and to flesh out, in particular, the authorities and responsibilities of what a Cyber Director would look like, I have really appreciated the responsiveness to -- from the Commission back to the committee.

It is our intent to use this information to discuss and to, basically, provide information during the markup of the

reconciliation between the House and the Senate versions of the NDAA in conference. And the House committee has laid out what their vision is. And the concern that we had expressed was one that we believe that the Principal Cyber Advisors, as laid out within the Department of Defense, have allowed for technical knowledge and for professional expertise to be available and deliverable to our chief executive officers immediately, and that, with that additional expertise, they could facilitate the use of cyberactivities, offensive and defensively, where needed.

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

Now, the reason why I lay this out for you this is way is, is that, over the last several years, we have followed what has happened at the executive branch with, originally, a very well-intended PPD-20, Presidential Policy Directive Memorandum 20, which was started in the previous administration. Their intent was to find consensus, but, before cyberactivities would be rolled out. Unfortunately, in doing so, it became a consensus, which meant that any one of a number of a different individuals could stop the

movement forward of any cyberactivity. That was changed a couple of years ago with the creation of NSPM-13, National Security Policy Memorandum 13, in which a clear line was laid out for the decisionmaking process on the use of cyber tools and the availability of cyber for our warfighters.

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

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

Senator King?

Senator King: Mr. Chairman, I would say that our

proposal is the anti-silo. The problem is now, as I mentioned, we've got cyberactivities and planning and work going on throughout the Federal Government, and the whole idea is to bring some coherence and coordination to that.

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

Senator Rounds: And that's what I'm hoping, and that's what I -- I just wanted to make it clear so that -- and I'd sure like to have Representative Gallagher concur with that, if he's available, as well.

Mr. Gallagher: I do concur with what Senator King

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

Senator Rounds: Correct.

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

Now, the final thing I'd say is just to confess, my bias when I came into this was to resist the creation of new agencies and, you know, positions. And largely, I think, we have avoided that. But, with this, I've come to believe it's actually the least bureaucratic option. One option would be to create a separate agency entirely. I think that's pretty bureaucratic. But, doing nothing I actually think is the most bureaucratic option, because I think it

will lead to a catastrophic cyber incident that will require in layering on of new agencies and positions in response to that. And so, we really want that National Cyber Director to get to the left of that cyber boom by coordinating and advising the President primarily on the defensive side of the equation.

Senator Rounds: Great. And thank you very much.

And I'm about out of time, but, Mr. Inglis, what would your -- very quickly, what would your thought --

General Inglis: I would say that -- I think I speak confidently -- the Commission would support your sense of the substance and the spirit of the National Cyber Director. The National Security Advisor is busy. He doesn't have the time, or she doesn't have the time, to, on a daily basis, try to figure out what our overall strategy is, vis-a-vis cyber. And, much like this committee has reconciled how we think about the military instrument of cyberpower, what we asked, I think, 2 years ago, was, of the Nation, What is the context of the application of the military instrument of cyberpower? Is it a traditional military instrument -- traditional military activity, or not? Give us the expectations of what, then, it might do, and then let us go do it. I think the National Cyber Director needs to treat all the instruments of power in the same way: provide context, provide expectations, and allow the depth of

expertise to then do that in a distributed fashion.

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

Senator Rounds: Thank you.

Senator Manchin.

Senator Manchin: Thank you, Mr. Chairman.

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

Senator King: Well, we've --

Senator Manchin: -- counter this?

Senator King: Different agencies have different responsibilities. In addition to the ones that you

mentioned, other -- the other agencies that have cyber responsibilities are FERC --

Senator Manchin: Sure.

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

Senator Manchin: Who do these agencies report to now, Senator? Right now. Who do the heads of these agencies,

when there is a cyberattack --

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

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

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

Senator Manchin: I gotcha.

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

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

General Inglis: Well, first, if I might go a half-step back and answer another question that you asked --

Senator Manchin: Okay.

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

To your question about whether the Commission believes it is appropriate or inappropriate to attack the critical infrastructure of other nations, I think that our views on that are perhaps more nuanced than a yes or a no. We would start by, first, saying that we believe, as the United States has long attested, we will follow international law, and we will adhere to the global standards of normal behavior that we attested to in 2015 through the auspices of the State Department, that we wouldn't, in peacetime, attack the critical infrastructure of other nations. That being said, in wartime, it is a political decision of the leadership of this Nation to determine, with necessity and

proportionality, how we should array the various instruments of national power that we bring to bear. And so, we shouldn't be in a place where we never say never, we just need to follow the rules of proportionality and necessity and the international laws that govern such things.

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

Senator Manchin: Right.

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

Senator Manchin: I gotcha.

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

Senator Manchin: Yeah.

General Inglis: -- methods, some of which include cyberpower. But, the use of diplomacy, the use of legal methods, the use of, perhaps, public shaming, all of those need to be brought to bear to stop that and to hold them at

risk in ways that follow international law, that use necessity and proportionality.

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

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

Mr. Gallagher: There were --

Senator Manchin: Congressman Gallagher?

Mr. Gallagher: Yeah, there were six specific recommendations that I talked about that were -- are in the House version of the NDAA, but not in the Senate version of the NDAA. And I brought that up just to urge the Senate to consider the House equities when we're in that discussion. And I believe there is some ongoing debate about our continuity-of-the-economy proposals. And I understand, for various jurisdictional issues in the House and the Senate, there are some other recommendations that made it into neither report. But, we feel fairly good about just the -- sort of the baseline of what made it into either the House

or the Senate, and hope there is a, you know, collaborative approach in the conference committee processes.

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

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

Senator King: No, these are all, we believe, close enough so that --

Senator Manchin: So, they can be considered in to the --

Senator King: Yes.

Senator Manchin: -- conferees.

Senator King: Yes. Yes, sir.

Senator Manchin: You think that will all be -- all 29 will be in play.

Senator King: Yeah. So, they're in the bill. And we hope that they can resolved so that as many as possible -- I mean, you know --

Senator Manchin: Yeah.

Senator King: -- we all know what happens with Commission reports. And we were determined to not have that happen.

Senator Manchin: I gotcha.

Senator King: And that's why we actually drafted legislation rather than just give you ideas. And so, if we can finalize these documents in the -- these amendments in the bill as it comes out of the conference committee, we will have done well more than half of our total recommendations.

Senator Manchin: Thank you all. I appreciate it very much.

Senator Rounds: Thank you.

And -- yeah, just in looking back over the numbers of -- that I've got in front of me, it's been great to see the number of them that were actually put into the -- this subcommittee's mark, and then the other three that were added on the floor. We couldn't do them in subcommittee, because of jurisdictional issues, but -- so, that was good to see, I think, 14 total coming out of the Senate, and then holding a spot for the discussion on the National Cyber

Director position, as well. So, I think the committee has been very successful, and you've done some great work.

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

Examples of such positions that currently exist, that Congress has put into law, top leaders of the Office of Management and Budget, the Director, the Deputy Director, the Deputy for Management, the Controller, the Office of Federal Financial Management, OMB; Administrator, Office of Information and Regulatory Affairs, OMB; Administrator, Office of Federal Procurement Policy, OMB; Director of Office of National Drug Control Policy; top leaders of the

Office of Science and Technology Policy, including the Director and the Associate Directors; Intellectual Property Enforcement Coordinator; Chairman, Council of Economic Advisors; Chair and Members, Council on Environmental Quality; top leaders of the Office of the United States Trade Representative, including the United States Trade Representative, Deputy United States Trade Representatives, Chief Agricultural Negotiator, Chief Innovation and Intellectual Property Negotiator. And I understand that, really, a lot of the language that you've put into this proposal comes from the legislation authorizing and directing the United States Trade Representative, as well. So, there is a format that's been followed here that we can look at to see whether it's successful, or not, in terms of advising the President of the United States.

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

The other thing the committee -- that the committee talked about a little bit was the direction with regard to our activity in cyberspace, whether there should be -- you know, what type of deterrence should be used, whether we should be putting more emphasis on defensive activity,

making it more difficult for our adversaries to get in. And I'd just like to take just a minute, because I -- just to give you the opportunity to share a little bit about your thoughts regarding the operations in cyberspace. You've got air, land, sea, space, and cyberspace. And most certainly, the most inexpensive of any to get into and to create havoc everyplace else is cyberspace. We have to be on top of our game. Can you share with me a little bit your thoughts about the questions, concerns that your Commission found or that you wanted to express and maybe haven't had the opportunity to do so, so far?

Senator King: Thank you, Mr. Chairman.

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

But, I think the -- what I'd like to say about the deterrent issue is that this was a -- there was a great deal of discussion about this, and it grow -- it grew, for me, out of many of the hearings that you and I have sat through

over the last 4 or 5 years, where we haven't had a deterrent policy. We've been purely defensive. And what we are saying is that there's a level -- everybody knows that there would be a response if there was an attack on critical infrastructure. But, the question is, What happens if there's an attack on our election, or what happens if there's wholesale theft of intellectual property? What's the response? And because there hasn't been, and because, as you point out, this is a cheap way to make war, then we've become a cheap date. We've become an easy target. And what the Commission suggests is, there needs to be a new declaratory policy that there will be a response. It may not be cyber. It may not be kinetic. It may be sanctions. It may be any part of the national power toolkit, but that there will be a response.

And another sort of wrinkle of this that's very important is, 85 percent of the target space in cyber is in the private sector. It's not the Army and the Air Force. They will be under attack -- cyberattack. But, the target space is in the private sector. And that's where we have to really develop relationships. This is a whole new way of thinking. One of the things we talk about is the intelligence agencies being able to share with the private sector what they're learning about cyberattacks on SCADA systems at power plants.

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

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

Senator Rounds: Thank you, sir.

I'm going to turn it over to Senator Manchin.

Senator Manchin: Mr. Inglis, one of the Commission's recommendations that was included in the Senate NDAA is to have the Defense Department carefully and comprehensively assess whether the Cyber Mission Force, our military cyberforces, are rightly sized. We included the

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

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

General Inglis: I think that we did look at that, nationally and then within the various components that constitute those who employ cyber workers within the United States Federal bureaucracy. Our sense of United States Cyber Command is, they've done a great job within the authorities that they have of recruiting, training, and developing for careers the people necessary to do the work

that they do. But, as you well know, those forces were set in size in the year 2013. I think we're sitting now with a combined size of that force, the actual, kind of, pointy-end of the force, about 6200, 133 teams, sized in a time and place when our sense of how we use military cyberpower was different, in a time and place when the sense of where that should be used was different. It's time to review that. It's time to take a look at that.

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

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

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

hear.

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

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

Senator Manchin: Thank you.

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

Senator King: Well, first, I wanted to --

Senator Manchin: Okay.

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

The analogy is, the Intelligence Committee, which was created in 1976 for the same reason, there was a realization that intelligence was scattered throughout the Federal Government and throughout the Congress, responsibility, and it made sense to put it into one set of expert hands. And that's the origin of the Intelligence Committee. We think the same thing should be done here, and I'll continue to pursue the idea.

Senator Manchin: With all the expertise you all had on your Commission -- it seemed like you had a wide range of people coming from different walks of life that had

expertise to add -- what was the greatest concern, if we can talk about -- maybe we can't in this type of a setting -- but, the greatest concern you had with our cybersecurity right now, and what our adversaries are trying to do to us on a daily basis, of the vulnerability we might have that you was really concerned about? Or did all of you agree you had one highly concerned sector of our society that was vulnerable?

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

Senator Manchin: Yeah.

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

Senator Manchin: Jesus.

Senator King: Three million times a day. And that gives you the range. Banks, I know, the same -- I don't know if it's the same number, but hundreds of thousands of times a day. So, this is an ongoing threat, not only from State actors, but from malign actors who are doing

ransomware, sometimes they're just garden-variety crooks, but they're also people that want to undermine our society.

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

General Inglis: And, sir, could I speak to that, too, then --

Senator Manchin: Of course.

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

Our view is -- and you won't find this line in the report, but if I was stuck in an elevator with somebody and had 10 seconds to get out, what we propose is that, if you're an adversary in this space, henceforth, you're going to have to beat all of us to beat one of us. That actually derives from using all of the talent, all of the expertise,

all the authorities that we already have in a more coherent, more joined-up fashion, preparing as one, applying those resources as one, such that, when we execute this in a distributed fashion, much like the Department of Defense has, we're giving the freedom to operate, we know that we're operating according to some larger strategy, consistent with some larger purpose, and that we're helping whatever is to the left of us, to the right of us. That's a fundamental problem for us at this moment in time.

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

Senator Manchin: Thank you.

Senator Rounds: Look, I want to take this time to just say thank you to all of our participants. This is critical,

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

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

The second piece that I think we have to recognize -- and I want to thank Senator Manchin for being here today -- we had a number of other members who were here early on, and then had to leave. It's multiple meetings at the same time. But, we shouldn't leave without recognizing how far our cyber teams have come in just the last few years. And the way in which General Nakasone and those teams have really stood up what has been an impressive series of achievements,

both offensively and defensively, and yet they will tell you it's still so much more work to be done. And so, everything we can do to provide them with the tools that they need and the correct public policy that they need in order to do their job, the better off we're going to be. And every other domain, whether you're talking air, land, sea, space, all of them are dependent on our ability to protect them in cyberspace, because it's all connected. And it's the least expensive way for our adversaries to get in and actually do damage in any one of the other domains. And so, we have to pay attention to it.

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

Senator Manchin, any final thoughts?

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

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

My only thing was -- I was wanting to ask the question on -- do you see the private sector starting to harden up a little bit? Are we communicating with them well enough to

let them know they have a responsibility to harden up, also?

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

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

Senator King: No, no, they're very much engaged in their own --

Senator Manchin: Okay.

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

Senator Manchin: Yeah.

Senator King: -- do their part.

Senator Manchin: Yeah.

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

Senator Manchin: Thank you all.

Thank you very much.

Senator Rounds: With that, I would like to say thank

you to our witnesses today: Senator Angus King, The Honorable Michael Gallagher, and Brigadier General John Inglis, Retired. Thank you, to all of you, for your testimony.

And, with that, this subcommittee meeting is adjourned. Thank you.

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