Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON
ENCRYPTION AND CYBER MATTERS

Tuesday, September 13, 2016

Washington, D.C.

ALDERSON COURT REPORTING
1155 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, D.C. 20036
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON

ENCRYPTION AND CYBER MATTERS

Tuesday, September 13, 2016

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:37 a.m. in Room SH-216, Hart Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], Wicker, Fischer, Cotton, Rounds, Ernst, Sullivan, Lee, Cruz, Reed, Nelson, McCaskill, Manchin, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, King, and Heinrich.

OPENING STATEMENT OF HON. JOHN McCAIN, U.S. SENATOR FROM ARIZONA

Chairman McCain: I would -- since a quorum is not present, but we have pending military nominations, I would ask unanimous consent to waive the requirement for two more members in order to conduct a routine business for the 4,158 pending military nominations, which I'm -- none of which are controversial. Is there any objection to that?

[No response.]

Chairman McCain: If not, since -- a quorum is not present, but I ask the committee to consider a list of 4,158 pending military nominations. Of these nominations, 503 nominations are 2 days short of the committee's requirement that nominations be in committee for 7 days before we report them out. No objection has been raised. These nominations -- I recommend the committee waive the 7-day rule in order to permit the confirmation of the nomination of these officers before the Senate goes out for the October recess.

Is there a motion to favorably report these 4,158 military nominations to the Senate?

Senator Reed: So move.

Chairman McCain: Is there a second?

Senator Wicker: Second.

Chairman McCain: All in favor?

[A chorus of ayes.]

Chairman McCain: The motion carries.

And I thank the committee. We wouldn't want to go out for a long period of time with these pending nominations, none of which are in any way controversial.

And I think that there was a cyber attack on Admiral Rogers' automobile, which accounts for him being late this morning.

[Laughter.]

Chairman McCain: We'll have a full investigation --

Voice: He's joking.

[Laughter.]

Chairman McCain: Mr. Secretary, we welcome you and Admiral Rogers. And we'll begin with you, Mr. Secretary.

Mr. Lettre: Chairman McCain, Ranking Member Reed, members of the committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its impact on the Department of Defense.

With your permission, I've submitted a longer written statement, and I would ask that it be made part of today's record.

Chairman McCain: If you'll hold for a moment, Secretary Lettre, in my -- I forgot the opening statements by myself and the Ranking Member --

[Laughter.]

Mr. Lettre: I was wondering about that.

Chairman McCain: -- which is the reason why so many of my colleagues are staying here, in order to hear our words of wisdom.

[Laughter.]

Senator Nelson: We thought you were going to spare us.

[Laughter.]

Chairman McCain: Probably should, given the calendar, but could I just -- I'll go ahead, and we'll hold you, Senator -- Secretary Lettre.

Encryption has become ubiquitous across the counterterrorism fight. ISIL has successfully leveraged messaging applications developed by some of our most innovative companies to create an end-to-end encrypted safe haven where they can operate with near perfect secrecy and at arms' length of law enforcement, the intelligence community, and the military. From Syria to San Bernardino to Paris to Brussels to perhaps even Orlando, ISIL has utilized encrypted communications that, just a few years ago, were limited to a select few of the world's premier military and intelligence services.

As I've stated in the past, this is a complex and difficult problem, with no easy solutions. We must balance our national security needs and the rights of our

citizens. We must also recognize that authoritarian regimes are eager to gain keys to encrypted software so they can further their own abusive policies, such as suppressing dissent and violating basic human rights. Yet, ignoring the issue, as the White House has done, is also not an option.

I look forward to hearing how the use of encryption by terrorist organizations is impacting your ability to detect and prevent future attacks, and how the proliferation of encryption alters the way you do business at the NSA and Cyber Command.

Admiral Rogers, you have frequently spoken with this committee about the so-called "dual hat" under which the Commander of Cyber Command also serves as the Director of the NSA. Last year, you told this committee, quote, "I will strongly recommend, to anyone who asks, that we remain in the 'dual-hat' relationship. This is simply the right thing to do for now, as the White House reiterated in late 2013." You stated that it might not be a permanent solution, but that it is a good solution, given where we are. You were asked again in our hearing earlier this year, and you reaffirmed the need to keep the two organizations tightly aligned.

That's why I'm troubled by recent reports that the Obama administration may be trying to prematurely break

the dual-hat before Obama -- President Obama leaves office. On Friday, it was reported that Secretary of Defense Ash Carter and Director of National Intelligence James Clapper have backed a plan to separate Cyber Command and the NSA. Here we go again. Another major policy matter has apparently been decided, with no consultation whatsoever between the White House or the Department of Defense with this committee. I urged Secretary Carter to provide this committee and the Congress the details of this plan and his reasoning for support it. I will -- hope he will explain what has changed since the last time the administration rejected this idea, in 2013.

And while I'm sure the phrase "predecisional" is written somewhere in our witnesses' briefing papers, I would remind them that this committee does not take well to being stonewalled while their colleagues in the administration leak information to the press. Even if this decision has not been made, our witnesses should still be able to provide substantive analysis on the consequences of separating the dual-hat for our national security and for taxpayers.

Let me be very clear. I do not believe rushing to separate the dual-hat in the final months of an administration is appropriate, given the very serious challenges we face in cyberspace and the failure of this

administration to develop an effective deterrence policy. Therefore, if a decision is prematurely made to separate NSA and Cyber Command, I will object to the confirmation of any individual nominated by the President to replace the Director of the National Security Agency if that person is not also nominated to be the Commander of Cyber Command.

This committee and this Chairman are tired of the way that Congress, in general, and this committee is treated by this administration. These issues present larger concerns about whether the Department is appropriately organized to manage the defensive and offensive requirements of the cyber mission. We know that the Department faces challenges in recruiting and retaining top cyber talent. We know that the Department's cumbersome acquisition system hinders technological advancement and has eroded our technological superiority. And we know that the administration's failure to confront deficiencies in its cyber policy has undermined the Department's ability to effectively defend, deter, and respond to our adversaries in cyberspace. Both Russia and China have leveraged cyber to systematically pillage certain critical defense technologies, create uncertainty in our networks, and demonstrate capability. Make no mistake, they are the first movers in the cyber domain,

and they have put us on the defensive. But, the administration has consistently failed to provide a meaningful response.

The latest media reporting, that Russia may try to undermine our electoral process, underscores this point. Russia is using cyber to undermine American national interest, and now it appears our democracy could be the next target. And the administration's response to a mere warning from the Secretary of Defense -- is that the best the United States can do? Despite this committee's numerous requests for a cyber deterrence framework, the administration has failed to present any meaningful strategy. Instead, it has evidently distracted itself with debates over the dual-hat. Instead of shaping the limits of acceptable behavior in cyberspace, the administration, instead, has allowed Russia and China to write the playbook. As a result, this administration has left the United States vulnerable.

I look forward to hearing more about the cyber operations against ISIL and the challenges, opportunities, and constraints you are facing on the cyber front.

Senator Reed.

STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

Senator Reed: Well, thank you very much, Mr. Chairman.

Let me join you in welcoming Secretary Lettre and Admiral Rogers to -- back to the committee.

Thank you, gentlemen, and the men and women that you lead, for their service and your service.

This is a third committee hearing focused on the encryption issue, which underscores the importance of this issue and its impact on national security. The rapid growth of sophisticated end-to-end encryption applications and extremely secure physical access control to smartphones and computers has an adverse impact on law enforcement agencies at all level of government, and impairs the ability of the intelligence community and the Defense Department's Cyber Command to detect and counter cyber threats to the Nation. At the same time, this security technology helps to protect individuals, corporations, and the government against cybercrime, espionage, terrorism, and aggression.

While FBI Director Comey has tirelessly stressed the danger of law enforcement going dark, respected national security experts, including General Michael Hayden, former Director CIA and NSA, Michael Chertoff, the former Under Secretary -- or Secretary, rather, of Homeland Security,

have advised against compelling industry to ensure that the government can always get access to encrypted data. These experts argue that cyber vulnerabilities are the greatest threat to the public and national security. And this debate underscores the complexity and difficulty of the issue that we all face and we all must deal with very quickly, because it is a growing -- as the Chairman's testimony indicates, it's a growing threat to our national security and our law enforcement.

A major problem for law enforcement at this juncture is gaining access to data on devices that are physically in their control for foreign intelligence collection, where physical access is rarely, if ever, applicable, the challenges to overcome encryption of data in transit, or to gain remote access to devices when they are turned on and communicating. And the latter set of problems is not qualitatively new. And I will ask, when questioning, whether they're more manageable than these law enforcement issues.

In addition to encryption, another important area that I hope we're able to discuss today is the issue that the Chairman brought up. That's the future of Cyber Command. I understand the administration is deliberating on whether it is the proper time to elevate Cyber Command to a unified command, and if, and under what conditions, the

administration should terminate the so-called "dual-hat" arrangement in which the Commander of Cyber Command serves also as the Director of the NSA. An additional issue, a discussion of whether the Director of NSA should be a civilian rather than a general officer. And, while I know that is likely difficult for our witnesses to discuss administrative deliberations in an open hearing, I will welcome any of your thoughts or considerations on these important issues.

Another area that I know is of interest to the committee, but, again, may be difficult to comment on publicly, is several revelations of hacking of major computer systems in this country by outside actors. Again, that is a very critical issue and one that we're very much involved and interested in.

Once again, gentlemen, thank you for your service, and thank you for your appearance here today.

Chairman McCain: Now Secretary Lettre.

STATEMENT OF HON. MARCELL J. LETTRE II, UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE

Mr. Lettre: Chairman McCain, Ranking Member Reed, and members of the committee, thank you for inviting us to discuss the importance of strong encryption, trends on its use, and its impact on the Department of Defense.

With your permission, I have a written statement that is a little longer than my opening statement here, and I'd ask that it be made part of today's record.

In my brief opening statement, I would like to underscore three points:

First, the Department of Defense strongly seeks robust encryption standards and technology vital to protecting our warfighting capabilities and ensuring that key data systems remain secure and impenetrable to our adversaries today and well into the future. The Department's support for the use of strong encryption goes well beyond its obvious military value. For example, commercial encryption technology is not only essential to U.S. economic security and competitiveness, but the Department depends upon our commercial partners and contractors to help protect national security systems, research-and-development data related to our weapon systems, classified and sensitive information, and service members' and Department civilians' personally identifiable information

and health records.

Second, we are concerned about adversaries, particularly terrorist actors, using technology innovation, including ubiquitous encryption, to do harm to Americans. The cybersecurity challenges confronting the Department are compounded by the pace and scope of change, not only in the threat environment, but also in associated technologies. Our adversaries are constantly searching, looking, and adopting new and widely available encryption capabilities, with terrorist groups such as the Islamic State of Iraq in the Levant, ISIL, leveraging such technology to recruit, plan, and conduct operations. Our concern grows as some parts of the communication technology industry move towards encryption systems that providers themselves are incapable of un-encrypting, even when served with lawful government requests to do so for law enforcement or national security needs. This presents a unique policy challenge, one that requires that we carefully review how we manage the tradeoffs inherent in protecting our values, which include individual privacy as well as our support for U.S. companies' ability to innovate and compete the global economy, and also protecting our citizens from those who mean to do us grave harm.

Third, the Department is working with other parts of

the government and the private sector to seek appropriate solutions on these issues now. We need to strengthen our partnership with the private sector, finding ways to protect our systems against our adversaries' cyberattacks and at the same time finding innovative and broadly acceptable ways to address nefarious actors' adoption of new technologies, including encryption, even while we must carefully avoid introducing any unintentional weaknesses in the protection of our security systems or hurting our global economic competitiveness.

Mr. Chairman, the Department is committed to the security and resiliency of our data and networks, and to defending the U.S. at home and abroad. An ongoing dialogue with Congress as well as other departments and agencies and the private sector is absolutely critical as we work together to confront and overcome the security challenges associated with encryption.

I appreciate the committee's interest in these issues, grateful for the dialogue, and I look forward to your questions.

[The prepared statement of Mr. Lettre follows:]

Chairman McCain: Admiral Rogers.

STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN, COMMANDER, UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

Admiral Rogers: Chairman McCain, Ranking Member Reed, and members of the committee, thank you for the opportunity to appear before you today to discuss the current communications environment, including strong encryption and cyber challenges.

When we last met, on the 12th of July in a closed session, I outlined several of those challenges to the committee. And today, I look forward to further discussion so the American people are provided the greatest amount of information possible on these important topics. Of course, some aspects of what we do must remain classified to protect national security, so today I will limit my discussion to those in the public domain.

When I use the term "encryption," I'm referring to a means to protect data from any access except by those who are authorized to have it. Encryption is usually done by combining random data with the data you want to protect. The random data is generated by a mathematical algorithm and uses some secret information only, called a key, in the generation. Without the key, you can't undo the encryption.

NSA supports the use of encryption. It's fundamental

to the protection of everyone's data as it travels across the global network. NSA, through its information assurance mission, for example, sets the encryption standards within the Department of Defense. We understand encryption. We rely on it, ourselves, and set the standards for others in the U.S. Government to use it properly to protect national security systems. At the same time, we acknowledge encryption presents an ever-increasing challenge to the foreign intelligence mission of NSA. The easy availability of strong encryption by those who wish to harm our citizens, our government, and our allies is a threat to our national security. As you well know, the threat environment, both in cyberspace and in the physical world, is constantly evolving, and we must keep pace in order to provide policymakers and warfighters the foreign intelligence they need to help keep us safe.

Terrorists and other adversary tactics, techniques, and procedures continue to evolve. Those who would seek to harm us, whether they be terrorists or criminals, use the same Internet, the same mobile communication devices, the same software and applications, and the same social media platforms that law-abiding citizens around the world use. The trend is clear. The adversaries continue to get better at protecting their communications, including through the use of strong encryption.

I want to take this opportunity to assure you and the American people that the NSA has not stood still in response to this changing threat environment. We are making investments in technologies and capabilities designed to help us address this challenge. And last year, we started a process to better help position ourselves to face these challenges.

It is premised in the idea that, as good as NSA is -- as it is at foreign intelligence and its information assurance mission, the world will continue to change. And the goal is, therefore, to change, as well, to ensure that we will be as effective tomorrow as we are today. The Nation counts on NSA to achieve insights into what is happening in the world around us, what should be of concern to our Nation's security, the safety and well-being of our citizens and of our friends and allies.

We have a challenge before us. We are watching sophisticated adversaries change their communication profiles in ways that enable them to hide information relating to their involvement in things such as criminal behavior, terrorist planning, malicious cyber intrusions, and even cyberattacks. Right now, technology enables them to communicate in a way that is increasingly problematic for NSA and others to acquire critical foreign intelligence needed to protect the Nation or for law

enforcement individuals to defend our Nation from criminal activity.

The question then becomes, So what's the best way to deal with this? Encryption is foundational to the future. The challenge becomes, given that premise, What is the best way for us ensure the protection of information, the privacy and civil liberties of our citizens, and the production of the foreign intelligence necessary to ensure those citizens' protection and safety? All three are incredibly important to us as a Nation.

You've also asked me to talk about cyber deterrence and U.S. Cyber Command's organizational structure. As I have said before, I do not believe that malicious cyber activity by adversaries can only be, or must be, deterred by cyber activity. Our Nation can deter by imposing costs in and through other domains as well as using a whole-of-nation approach. Our instruments -- all instruments of power should be considered when countering cyber threats, intrusions, or attacks.

And with regard to our organizational structure, U.S. Cyber Command is well along in building our Cyber Mission Force, deploying teams to defend the vital networks that undergird DOD operations to support combatant commanders in their missions worldwide, and to bolster DOD's capacity and capabilities to defend the Nation against cyberattacks

of significant consequence.

I, too, ask that my previously submitted written statement be made a part of the record.

And I look forward to your questions, sir.

[The prepared statement of Admiral Rogers follows:]

Chairman McCain: Thank you very much, Admiral. Is it still your professional military advice that maintaining the dual-hat at the -- at this time is in our best national security interest?

Admiral Rogers: Yes.

Chairman McCain: General Dempsey stated that cyber is the one area we lack an advantage over our adversaries. Do you agree -- still agree with that statement, Mr. Secretary?

Mr. Lettre: I do agree that cyber -- that the cyber threat is one of the greatest challenges we face.

Chairman McCain: Admiral?

Admiral Rogers: Yes.

Chairman McCain: Russian activity reporting hacking on our electoral process, I find it interesting that one of the two States there seems to be evidence of it is the State of Arizona. What can you tell us about the Russian activity and reported hacking on our electoral process? And do you think this is acceptable?

Admiral Rogers?

Admiral Rogers: Sir, as this is an ongoing investigation and a public, unclassified forum, I'm not going to be able to provide you specifics as to what our current assessment is. I will say this. This continues to be an issue of great focus, both for the foreign

intelligence community, attempting to generate insights as to what foreign nations are doing in this area, as --

Chairman McCain: This is the first time we've seen attempted interference in an -- in elections in the United States of America, isn't it, Admiral?

Admiral Rogers: Sir, we continue to see activity of concern. Again, I'm not going to characterize this activity "Is it a foreign nation-state, or not?"

Chairman McCain: Mr. Secretary, you have anything to add to that?

Mr. Lettre: Senator, I just would underscore that these are activities that the government is taking quite seriously. The FBI and the Department of Homeland Security has an aggressive investigation underway, so the government can form its conclusion.

Chairman McCain: Do we have a policy as to how to respond to this interference in elections in the United States of America? Do we have a policy as to what our actions be taken?

Mr. Secretary?

Mr. Lettre: In this particular instance, Senator, the government is intending to rely on the results of the investigation being led by the Bureau to --

Chairman McCain: I'm asking if --

Mr. Lettre: -- inform its policy decisions.

Chairman McCain: -- we have a policy, and the answer is no.

Admiral Rogers, there's a Wall Street Journal article yesterday, "New Tricks Make ISIS, Once Easily Tracked, a Sophisticated Opponent." Goes on and talks about how incredibly sophisticated some of their work was in preparation for these attacks -- electronic silences; when they did communicate, called or sent text messages; location; cheap burner phones, et cetera. What are we -- what would you think about this kind of activity, Admiral?

Admiral Rogers: ISIL remains the most adaptive target I've ever worked in 35 years as an intelligence professional, sir.

Chairman McCain: So, it was -- is not a leap of the imagination to think that this kind of activity and planning further attacks on the United States is taking place as we speak?

Admiral Rogers: Yes, sir.

Chairman McCain: Admiral Rogers and Mr. Secretary, do you believe there's a legislative solution that can address some of these challenges we're talking about?

Mr. Lettre: Senator, it -- from my view, the legislative route is not something that we think is the best way to go, at this time. New legal and regulatory approaches are not as potentially productive as a robust

dialogue seeking cooperation and collaboration with the private sector.

Chairman McCain: I agree. And unless there is a policy about what the United States actions will be in the case of a threat, in the case of actual attack, in the case of other aspects of this challenge we're on, then you're going to see legislation. Right now, there is no policy. There is no policy that you can describe to me as to what we would do about an impending attack or what we would do about an attack. And so, there's a vacuum there. So, if you don't act, then I guarantee you the Congress will act.

Admiral Rogers, it was recently reported that Twitter barred Data Miner, a company specializing in searching across millions of Tweets to identify unfolding terrorist attacks and political unrest, from accessing its realtime stream of Tweets because of its work for U.S. intelligence agencies. According to an article in the Wall Street Journal, this service gave the U.S. Intelligence Committee -- community an alert about the Paris terrorist attacks shortly before they began to unfold last November. In March, the company says -- first notified clients about the Brussels attacks 10 minutes ahead. It also appears that Twitter will continue allowing information to be sold for use in the private sector, not just the government.

Help me out, here.

Admiral Rogers: I wish I could, Senator. I am perplexed by their approach in this particular instance.

Chairman McCain: So, we have a situation where -- excuse me -- we have a situation where we have the ability to detect terror attacks using organizations such as Data Miner, and yet, in order for us to anticipate these attacks, we have to have certain information. And Twitter is refusing to allow them to have information which literally could prevent attacks on the United States of America? Is that the situation here, Admiral?

Admiral Rogers: Yes, sir. And at the same time, still willing to provide that information to others for business purposes.

Chairman McCain: For sale.

Admiral Rogers: For sale, for revenue.

Chairman McCain: What do you think we ought to do about people like that, besides expose -- besides exposing them for what they are?

Admiral Rogers: Clearly, I wish I had better understanding -- and perhaps there's insights that I'm just not aware of -- I wish I had better understanding as to the rationale that leads someone to believe that that is the right course of action. I'm just the first to acknowledge, I don't understand it.

Chairman McCain: So, shame on them.

Senator Reed.

Senator Reed: Thank you very much, Mr. Chairman.

And one of the issues -- and it's the last line of questioning, and it's highlighted quite a bit -- is that what used to be the domain of nation-states -- sophisticated research, development, application of products -- are now done commercially all across the globe. I mean, some of these encryption devices were just adapted by ISIL, they weren't developed by ISIL, but they've been very effective. So, we're in a race not just against another nation-state, we're in a race against technical innovation that is widespread and is relatively inexpensive, in terms of the commitment you have to make to develop a product. Is that a fair assessment, Admiral Rogers?

Admiral Rogers: Yes, sir. I often use the phrase, "Cyber is the great equalizer." It doesn't take billions of dollars of investment, it doesn't take tens of thousands of dedicated individuals, and it's -- uses a set of capabilities that are readily available globally to a host of actors.

Senator Reed: And so, I think it's incumbent upon us to approach it not as we've done in the past, you know, a nation-state, to countering their technology, but with a

much more, you know, innovative approach.

So -- and let me ask both you and the Secretary, What is this new innovative approach to counter this new decentralized, disaggregated, relatively inexpensive ability to upset our very expensive and elaborate systems, both platforms and intelligence systems?

Mr. Lettre: Senator, I'd just make a couple of broad points on this.

The most important thing we need to do in the Department of Defense is reach out to any and all partners that can help us find solutions. For example, the Department's senior leadership has invested heavily in conversations with leadership across the U.S. technology sector to really seek a dialogue about how we can come up with innovative solutions to address the dynamics you've raised, which include a quick and agile set of adversaries being able to adapt to new technologies, themselves, and leveraging those technologies to conduct global messaging that advances their interests. We've got to find a way to outpace that. And we believe that we can do so by tapping into the best ingenuity that the American private sector has to offer.

Senator Reed: Admiral?

Admiral Rogers: The other thing we're trying to do, at an operational level, in addition to the power of

partnerships, which I agree with Marcell is very important for us -- the argument I'm trying to make on both the NSA and the Cyber Command side is, "Guys, we're dealing with a whole new ecosystem out there, and we've got to bore into this ecosystem and look at it in just that way. Don't focus on just one particular application as used by one particular target. Think more broadly about the host of actors that are out there, about how that" -- and I apologize, I can't get onto specifics in an open forum, but looking at it more deeply, not just the one particular app, if you will, used by one particular target, that if we look at this more as an ecosystem, we will find vulnerabilities that we can access to generate the insights that the Nation and our allies is counting on.

Senator Reed: But, I think, fundamental to your approach -- and again, it touches on the issues raised by the Chairman -- is that if these large technological players or, you know, civilian potential partners refuse to cooperate, then that is very -- could be detrimental in our security. And we have to find a way either to convince them or otherwise get them to cooperate, because I -- my sense is, without it, that we will not be able to deal with this issue. Is that fair?

Admiral Rogers?

Admiral Rogers: It is, from my perspective.

Partnerships is going to be incredibly foundational to the future, here.

Senator Reed: Just a final point. Raise it. You might comment quickly. That is, you know, there's been some discussion about having sort of a key to these encryption so that -- you know, the proverbial backdoor -- so that government could get in, et cetera. Opponents to that approach suggest that that -- not only government could get in, but other bad actors could get in. So, is that a solution that causes more problems, or is that a real solution?

Mr. Lettre: Senator, from a policy perspective, we're in favor of strong encryption. We benefit from it, ourselves. So, anything that looks like a backdoor is not something we would like to pursue. The important thing, I think, is, on a case-by-case basis, for institutions like the Department of Defense and the Federal Bureau of Investigation and other key stakeholders, to have a really rich dialogue, case by case, with key industry players to see what kinds of solutions can be brought to bear, given the imperative to also balance privacy and civil liberties for our public, as well as to be able to ensure the competitiveness of our economic players.

Senator Reed: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: If I -- Senator Rounds will indulge me one second.

Admiral, I just want to go back to this election in Arizona. Is it possible that Russians could somehow harm the electoral process in my home State of Arizona?

Admiral Rogers: Senator, let me plead ignorance on the specifics of the electoral system in the State of Arizona.

Chairman McCain: Or is it -- is there a possible scenario where they could disrupt the voting results in the upcoming election?

Admiral Rogers: I think there are scenarios where you can see capability applied in particular areas. Again, it's not -- I don't have strong fundamental knowledge across the breadth of the 50 States, since elections are run on a --

Chairman McCain: Yeah.

Admiral Rogers: -- State basis. And one advantage I do see, from a defensive standpoint, is that the structure is so disparate, with some elements being very -- still very manually focused, others being more electronically and interconnected -- because it's not just one nationwide, single, integrated structure, that tends to help us, I think, defensively, here.

Chairman McCain: But, it is a concern.

Admiral Rogers: Oh, yes, sir.

Chairman McCain: Senator Rounds. Thank you, Senator Rounds.

Senator Rounds: Thank you, Mr. Chairman. And thank you, to you and the Ranking Member, for putting this subject before us today.

I have a number of questions concerning how we respond to a cyberattack on civilian infrastructure. And I'm just curious. I know that the Chairman has already raised the question of a policy, but I'd like to go a little bit deeper. And what I'm really curious about is, what is the role of the Department of Defense with regard to an attack on civilian critical infrastructure? Is there a preemptive responsibility that the Department of Defense has to protect civilian infrastructure in a cyberattack, similar to what happens with a kinetic attack?

Mr. Lettre: Senator, from a policy perspective at DOD, we have three main missions. One is to defend the Defense Department and its networks. The second is to support our commanders in providing military options in support of their plans and operations that relate to cyber. And the third is, when called upon by the President and the national command leadership, to support broader efforts that might be brought to bear in the case of an attack on U.S. critical infrastructure.

Senator Rounds: Has that occurred? Has that request

occurred yet?

Mr. Lettre: Well, it -- the request typically would come in, in a specific instance of an attack.

Senator Rounds: So, in the case of an attack on a civilian infrastructure, how long would it take from the time that the attack is initiated until a time that the damage is done? Milliseconds?

Mr. Lettre: It really depends on the circumstances of the attack, but it can be pretty quick, in the case of a cyberattack, yes.

Senator Rounds: So, how in the world would we expect the President of the United States, even if it's not at 3:00 o'clock in the morning, to respond in time to give you permission to protect critical civilian infrastructure if you already don't have a plan in place? Or do you have a plan in place?

Mr. Lettre: Right. And there -- at the policy level, there has been a multiyear effort to develop that overall framework for how to respond to attacks.

Senator Rounds: No --

Mr. Lettre: And then operationally --

Senator Rounds: -- either you've got one --

Mr. Lettre: -- there are systems, as well.

Senator Rounds: -- in place today or you do not. Do you have a plan in place today to respond to an attack on

critical civilian infrastructure?

Mr. Lettre: I believe we do have a plan in place, Senator. In July, for example, the President approved something called the Presidential Policy Directive on Cyberincident Coordination, PPD-41, which lays out a framework for an interagency effort to respond to attacks on our critical infrastructure from a cyber perspective.

Senator Rounds: So, you would not have to respond --

Mr. Lettre: In addition --

Senator Rounds: -- you would not have to wait for a presidential directive to protect critical infrastructure today.

Mr. Lettre: That's right. Now, there are a whole host of operational implications that need to follow from that. Each department and agency has worked through what capabilities it brings to bear and how quickly, operationally, those can be applied. In the case of the Department of Defense, obviously, we look very quickly to the capabilities of U.S. Cyber Command.

Senator Rounds: Admiral Rogers, today --

Admiral Rogers: Sir.

Senator Rounds: -- can we protect critical infrastructure if it is under a cyberattack?

Admiral Rogers: Do I have the capability to protect aspects of critical U.S. infrastructure? Yes, sir.

Senator Rounds: Thank you.

Let me go back. I -- you know, in the news, you've all heard, and we've all heard, about the discussions regarding Secretary Clinton's use of the email systems and so forth. One of the things that concerns me -- and I'd just like you to maybe put this in perspective for me if you could -- one of the ways in which we lose information or in which data that is private, confidential, classified is released, is not necessarily through unfriendly actors getting a hold of or breaking into our encrypted information, but simply human error and individuals within government who have access to classified or confidential information, or information which is classified at a higher category than that. Could you talk to us a little bit about what the responsibility is and whose responsibility it is to actually train or to give information to individuals who are either elected, appointed, or hired by the government to make sure that they understand the differences between the categories, between whether a "C" means that it's in alphabetical order or it is Confidential or any classified setting? Whose responsibility is it within the governmental layout, the structure today, to see that that information is appropriately disseminated and that instructions and remedial instructions are provided if there is a break?

Where does that fit?

Mr. Lettre: Senator, the questions around cyber hygiene, essentially, and how to properly protect yourself against IT intrusions and so forth is one set of policies and practices that typically the CIOs and associated IT security managers have responsibility for educating government employees at all levels. There are also aspects around the handling of classified information that flow from security policies and procedures, and those are typically handled by departments' security subject-matter experts.

Senator Rounds: Department by department?

Mr. Lettre: Typically so, yes, sir.

Senator Rounds: And who oversees that information -- or the delivery of that information?

Mr. Lettre: Well, the --

Senator Rounds: Your agency?

Mr. Lettre: The -- in the case of the Department of Defense, for DOD employees, my office oversees the setting of security policy standards.

Senator Rounds: Mr. Chairman, thank you.

Chairman McCain: Senator Nelson.

Senator Nelson: Admiral, I have often thought of our ability to protect ourselves in cyber as that we are really almost like the standoff in the nuclear, assured

mutual destruction. It gets more complicated with this, because we have nonstate actors. But, could you give us an example, in this open setting -- and, if required, then in a classified setting -- of where we have been attacked and we showed them that the return hit is going to be so hard that it deters them from hitting in the future?

Admiral Rogers: Again, I can't get any details in an open forum, but I would suggest the response to the Sony hack by the North Koreans in November of 2014 is an example of that.

Senator Nelson: And is that in the public domain -- that example?

Admiral Rogers: In the sense that we publicly acknowledged both the event, we publicly acknowledged who did it, and we publicly discussed the steps we were going to take in response to it, and we also highlighted at the time, "And if this activity continues, we are prepared to do more at the time and place of our choosing."

Senator Nelson: And the specifics of that, will that have to be in a classified setting?

Admiral Rogers: No, in the sense that, in this case, we chose to use the economic lever, it goes to one of the comments I made in my opening statement. One of the things I'm always recommending -- I realize I just work the operational piece of much of this -- but, I always

encourage people, "Think more broadly than cyber. When thinking deterrence, think more broadly than cyber." Just because an entity, nation-state, group, individual comes at us in cyber, that doesn't mean that our response has to automatically fall back on, "Well, we have to respond in kind. We have to go back from a cyber perspective." I've tried to make the argument, as have others, we need to play to all of the strengths of our Nation. So, in the Sony case, for example, we collectively, from a policy perspective, made a choice to play to the strength of the economic piece for the United States.

Senator Nelson: Right. And I think that's smart. You've got a menu of things.

Admiral Rogers: Sir.

Senator Nelson: But, when you get right down to tit-for-tat, we could absolutely, with our attacks, shut down a number of things.

Admiral Rogers: We could cause significant challenges to an opponent. I'm not going to get into specifics, but yes.

Senator Nelson: Right. So, do -- with state actors, do we see that that is actually creating a mutually assured destruction?

Admiral Rogers: I would argue, not yet. Because remember, a part of deterrence is both -- some aspects to

deterrence -- convincing someone that the benefit that they will gain doesn't justify the cost, convincing the actor that they just won't succeed, or convincing the actor that, "Even if you were to do this, and even if you were to succeed, what we'll bring back against you in response to this just doesn't merit you doing this. You really ought to think hard and fast before you really do this." And I have said this multiple times publicly before. The challenge we have right now is, I think, for a variety of reasons, some -- not all -- some actors have not yet come to the conclusion that there's a significant price to pay for some pretty aggressive actions on their part in the cyber arena.

Senator Nelson: Well, I'd like to follow with you, in a classified setting --

Admiral Rogers: Sir.

Senator Nelson: -- how we might respond to some of those actors.

Admiral Rogers: Sir.

Senator Nelson: In the private sector, do we have the cooperation that we need to tackle these encryption challenges?

Admiral Rogers: At an operational level, my observation -- because this is much bigger than just Cyber Command or NSA -- my answer would be no, in the sense that

-- my sense, as I look at this problem set, I see multiple parties spending a lot of time talking about what they can't do or what can't be done. And I wish we spent more time thinking about, Well, what could we do, what is in the realm of other possible? Even as I acknowledge I think there's multiple parts to this conversation. What can we do is not necessarily the same thing as what should we do. And those are two very important parts of this conversations that I think we need to have.

Senator Nelson: And the encryption thing does trouble all of us.

Admiral Rogers: Sir.

Senator Nelson: Aside from encryption, what other technology trends are shaping the way that the Department does business?

Admiral Rogers: It -- from a cyber perspective?

Senator Nelson: Yes.

Admiral Rogers: We're very much interested in artificial intelligence, machine learning. How can we do cyber at scale, at speed? Because if we're just going to make this a largely human capital approach to doing business, that is a losing strategy. It will be both incredibly resource-intensive, and it will be very slow. So, I'd say that is a big area of focus for us. In addition, we're constantly reaching out -- DIUX, the

capability that's been created out in Silicon Valley as well as Boston, U.S. Cyber Command has a separate but related -- that teams with DIUX to try to harness partnerships in the private sector.

Overall, I'd say good. But, as the Chairman highlighted, every once in a while, you just run into a situation where you go, "Can't we just step back, sit down, and talk to each other rather than, you know, these arbitrary, 'Hey, you can't do this, you can't do that, we won't do this, we won't do that'?" Even as I acknowledge there are different perspectives out there, I have no issue with that at all. I certainly understand that.

Senator Nelson: Thank you, Mr. Chairman.

Chairman McCain: Senator Lee.

Senator Lee: Thank you, Mr. Chairman.

Thanks, to both of you, for being here. I also appreciate your commitment to protecting the rights that we hold dear as Americans, and our security.

This issue of encryption cuts right to the heart of a lot of things. It cuts right to the heart of the nature of the relationship between the American people and their national government, and to the heart of a number of features in the Constitution, including responsibilities of the Federal Government to safeguard the people and also to safeguard their rights.

I believe it's an issue that Congress and the executive branch have to approach with a great deal of prudence, recognizing that we can't view it exclusively either as a national security issue, on the one hand, or as a privacy issue, on the other hand. We have to view it holistically, understanding that we've got to find a resolution to this that respects all the interests at stake.

Admiral Rogers, I'd like to start with you. On August 17th, the Washington Post reported that a cache of commercial software flaws that had been gathered by NSA officials was mysteriously released, causing concerns both for government security and also for the security and the integrity of those companies who I believe had not been notified by the NSA of the flaws discovered in their systems. So, can you walk through this process with us that the NSA uses to determine --

Admiral Rogers: Vulnerability?

Senator Lee: Yeah. Well, to determine when, whether, to what extent you should notify a private company of a security vulnerability that you've discovered, and whether NSA will continue to withhold such information from those companies when you're holding those and there are some clear concerns about the security of your own systems.

Admiral Rogers: So, there's a vulnerability evaluation

process, interagency, that was started in 2014, that we continue to be a part of, whereas NSA and other entities, not just us, become aware of, you know, zero-day vulnerability, so to speak, those vulnerabilities that we don't think are -- others are aware that haven't been patched or addressed, that we raise those through an interagency process, where we assess what's the impact of disclosing or not disclosing. I have said publicly before, I think, over the last few years, overall -- I think our overall disclosure rate has been 93 percent or so of the total number of vulnerabilities using this process since 2014. And we continue to use that process.

Senator Lee: Okay. Okay. So, you do that on a case-by-case basis --

Admiral Rogers: Yes, sir.

Senator Lee: -- depending on the totality of the circumstances.

Has there been an instance in which a U.S. company has suffered a security breach because of a cyber vulnerability that you were aware of that you -- that NSA had previously identified but --

Admiral Rogers: I can't say totality of knowledge, sir. I don't know totality. I apologize.

Senator Lee: Okay. No, it's understandable.

On Sunday, just this past Sunday, the Wall Street

Journal published a report on the methods of ISIS, the methods that ISIS is using, in which there were some experts who concluded that low-tech communications, including things like face-to-face conversations, handwritten notes, and sometimes the use of burner phones, have proven to be just as much of a problem for Western intelligence officials as the use of high-end encryption by our adversaries.

Mr. Secretary, I was wondering if I could get your sense on this. Are the defense and intelligence communities investing enough into human intelligence and other activities to address low-tech terror methods, like those leading up to the Paris attacks? And if we continue, I -- a related question to that is, If we continue focusing on combating highly sophisticated encryption technology, do we expect to see a corresponding shift into these lower-tech alternatives?

Mr. Lettre: Senator, you're -- you've put your finger on a really important point, which is the need for a really diverse set of intelligence collection capabilities and disciplines. Capabilities that go after the high end, using the best of our technology available, but also capabilities that draw upon individual case officers, area expertise, language expertise, and presence on the ground in a lot of places around the world, where we can, in a

very granular way, pick up what's going on and identify threat actors who, as you noted, may be using relatively unsophisticated mechanisms for planning and plotting attacks against the U.S. homeland and our allies. So, with regard to the aspect of your question around human intelligence, we have been making some investments, over the last several years, to continue to improve the effectiveness and capacity of defense-related human intelligence, working closely with CIA. And I think that that is a very important set of investments to be making.

Admiral Rogers: Senator, could I add one comment?

Senator Lee: Sure.

Admiral Rogers: That would be okay?

I think what that article highlights is the fact that we are watching ISIL use a multi-tiered strategy for how they convey information and insight that runs the entire gamut. And so, I think, for us, as intelligence professionals, we've got to come up with a strategy and a set of capabilities that are capable of working that spectrum. It can't be we just spend all our money focused on one thing. I don't think that's a winning strategy for us, if that makes sense.

Senator Lee: Understood.

I've got a couple of other questions, but my time's expired, so I'll submit those in writing.

Thank you very much.

[The information referred to follows:]

[COMMITTEE INSERT]

Chairman McCain: Senator Heinrich.

Senator Heinrich: Thank you, Mr. Chair.

Admiral Rogers, I want to continue along that line of questioning. And recently there was a worldwide survey, actually, of encryption products, looked at 865 hardware and software commercial encryption products that are available worldwide. And about a third of those were developed in the U.S.; two-thirds were developed overseas. You know, it begs the question, If Congress were to act on this issue, if Congress were to compel some sort of built-in backdoor to those kinds of products, would that in any way effectively limit access to strong encryption projects to our enemies, to foreign terrorist groups? So long as they're widely available on the Internet?

Admiral Rogers: So, I think, clearly, any structure, any approach that we come up with here with respect to encryption has to recognize that there is an international dimension to this, that encryption doesn't recognize these arbitrary boundaries on the globe that we have drawn, in the form of borders of nation-states. I don't know what the answer is, but I certainly acknowledge we have to think more broadly than just one particular market, so to speak.

Senator Heinrich: Given how easy it is to just download an app onto your smartphone to do end-to-end

encryption of texting and other communications, does it -- and getting to, really, Senator Lee's question -- does it beg the question of whether or not we've become overly reliant on signals intelligence, generally? Are we investing enough in human intelligence?

Admiral Rogers: I'll leave that up to the Under Secretary. I'm a --

Senator Heinrich: I know it's dangerous question for someone in your position, but --

Secretary?

Mr. Lettre: Senator, the short answer is, we do need to be investing in a range of capabilities, including the human intelligence capabilities. As to the point about individuals being able to download an app onto their mobile phones and smartphones that can avoid law enforcement or national security coverage, it really just underscores the imperative for a really rich and diverse set of conversations to be going on between government and all players across the technology sector. Each company has a different business model, which may or may not implement end-to-end encryption in a ubiquitous way, and we need to be looking for solutions on a case-by-case basis that allow us to preserve our values, including the ability to conduct law enforcement and national security protective operations in service of the Nation.

Senator Heinrich: You know, one of the issues that was raised earlier is this idea of identifying vulnerabilities that may exist in software, in operating systems, in hardware. Obviously, when there are those vulnerabilities, it means that people who work for the U.S. Government, as well as private citizens, have data potentially exposed to nefarious actors. Has the administration ever considered some sort of reward structure, incentive structure for those sorts of vulnerabilities to be identified and, therefore, identified to companies so that they can plug those holes as they come up?

Admiral Rogers: I can't speak for the administration as a whole, but we have done this twice now within the Department of Defense, you could argue, in the Bug Bounty Program, where we specifically have tried to incentivize the discovery and sharing of vulnerabilities, both to help the Department as well as to help the commercial sector in trying to address them. That's something that we've been doing.

Senator Heinrich: Have you found that to be a -- an effective strategy?

Admiral Rogers: Yes, sir. And, in fact, you'll see us -- in the coming months, we're looking at the next iteration of the program, as well. This is something we

want to continue.

Senator Heinrich: Do you think that's something we should be looking at as a more whole-of-government approach, as well?

Admiral Rogers: I would only say, our experience has been a positive one, and I would fully expect that it would turn to be positive for others. The scale is --

Senator Heinrich: I know with my conversations with the technology sector, that's something that's come up --

Admiral Rogers: Right.

Senator Heinrich: -- consistently over time.

Thank you both.

Chairman McCain: Senator Sullivan.

Senator Sullivan: Thank you, Mr. Chairman.

Thank you, gentlemen, for the testimony today.

Admiral Rogers, I just want to get -- and I know you've been talking about this in a more broad sense, but what do you see as the three top threats that U.S. Cyber Command or the NSA have to plan or defend against? Top three. And it can be a country or it can be an issue. When you're going to bed at night, what are the top three that you're --

Admiral Rogers: So, broadly, as I look out, number one is just the day-to-day defense of the DODIN. I look at DOD. We are a massive Department with a global laydown

and a network infrastructure that was built in a different time and a different place, in which redundancy, resiliency, and defensibility were not core design characteristics. And so, my challenge at the Cyber Command side is, I've got to defend an imperfect infrastructure and give us the time to make the investments to build something better. So, that's challenge number one. I'm always thinking to myself, what are the vulnerabilities out there that I don't recognize yet that someone's exploiting?

Number two would probably be -- I worry about -- most penetrations in networks to date have largely been about extracting information -- extracting, pulling the data -- whether it's to generate intelligence insights, whether it's to generate battlefield insights, whether it's to potentially attempt to manipulate outcomes. What happens when it's no longer just about data extraction, but it's about data manipulation, and now data integrity becomes called into question? As a military commander, if I can't believe the tactical picture that I am seeing, that I'm using to make decisions, that are designed to drive down the risk and help me achieve the mission, if what I'm seeing is a false representation and, in fact, the choices I'm making are increasing the risk and, in fact, are not having positive outcomes -- data integrity, data

manipulation really concerns me. That's a whole different kettle of fish.

And then the third one, probably, What happens when nonstate actors decide that the Internet is not just a forum to coordinate, to raise money, to spread ideology, but instead offers the opportunity to act as a weapon system, to employ capability on a global scale?

Senator Sullivan: So, let me ask about that last one, because I think one of the things that we continually hear, in terms of our cyber strategy and how it -- and how the -- this domain differs in so many other domains -- is that the attacks, when they occur on us, seem to come, in some cases, without much cost. So, we're getting hit from all different angles, and we're not sure where or how, and you can't do a symmetrical smackdown, maybe. But, how do we -- how do we raise the costs for adversaries who are attacking us in this domain? Or how do we signal that we're going to do it? Obviously, a lot of it -- if we're signaling, we have to have credibility. But, how do we raise the cost? Do you think we do need to raise the cost? Do you think, in this domain, that our adversaries or potential adversaries think that they can take action and kind of get away with it because we're not going to respond? Do we need to be more aggressive in signaling how we're going to respond, and then respond?

Admiral Rogers: And I think we need to show adversary we have capability, we have intent, and we have the will to employ it, within a legal framework --

Senator Sullivan: Have we done that, though, much?

Admiral Rogers: We have -- as I've said, we've done it. The Sony piece, I would argue. You could also argue, in the areas of hostilities -- Syria, Iraq, Afghanistan -- we're doing some good things every day that clearly I think the opponent understands that we're applying this capability against them. We've publicly acknowledged that we are doing that. I think, in part, that idea of publicly acknowledging the fact that we were using cyber as a capability to counter ISIL was not just to signal ISIL, but was also to make sure others are aware that the Department of Defense is investing in these capabilities, we are prepared to employ them, within a legal, lawful framework.

Senator Sullivan: Do you think we're sending that signal to state actors in the cyberspace?

Admiral Rogers: I certainly hope so, sir.

Senator Sullivan: Well, do you think we are? I don't know what --

Admiral Rogers: I think it --

Senator Sullivan: You're the -- you're in charge, right? So, "hope" makes me a little worry. What you

think --

Admiral Rogers: It varies by the actor. Honestly. It varies by the actor.

Senator Sullivan: Do the Iranians fear that we could retaliate against them if they take some kind of cyber action?

Admiral Rogers: Yes. My sense is, the Iranians have a sense for a capability. And I'm -- apologize, I can't get into a lot of specifics, but my sense is, they have awareness of capability, and they've seen us use it.

Senator Sullivan: Let me ask this one final question. It seems to me, kind of longer term, one of the biggest strategic advantages we have in this domain is our youth and their capabilities, which far exceed, probably, everybody in this room, given how smart they are in this space and how they've just naturally grown up with it. What are we doing to make sure to try to recruit younger Americans to, you know, be on the right side of the issue, to come serve their country in a really critical area, where they, in many ways, have unique skillsets that a lot of us -- no offense to my colleagues around the dais here -- that a lot of us don't have?

Admiral Rogers: Yes, sir. On the NSA side, I'll just highlight a couple of examples. We have a conscious effort that we've been doing for several years now. We do

high school and junior high school cyber camps that we partner with a variety of institutions across the United States. We have cyber acquisition -- or cyber academic excellence and academic research excellence relationships with over 200 universities on the NSA side across the United States, because we realize much of the workforce that we're looking to gain in the future is going to come from these pools. And so, there's something to be gain, we believe, by interacting early with them, and, more broadly, for the Nation as a whole, helping to encourage the acquisition of these skills, this knowledge, in a way that just wasn't necessarily the case in the past.

Senator Sullivan: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Manchin.

Senator Manchin: Thank you, Mr. Chairman.

And thank both of you all for being here.

Admiral Rogers: Sir.

Senator Manchin: And along the line of questioning there, for those of us who grew up in the not-Internet Age, if you look around at some of us here in the audience and some of us on this -- and now all this coming to fruition, it's quite confusing, quite troubling, quite concerning. With all that being said, you know, we have concern over our food supply, our energy supply. The

average person in America right now is concerned over, whether they have children or grandchildren, cyber bullying, everything that goes on with the Internet. We see the rise of terrorist -- the great equalizer is the Internet for them. They don't have an air force, they don't have a navy. They have nothing more than the will to do us harm or wreak havoc around the world.

With all that being -- going on, the question I would like to ask best is, In a perfect world, without the politics involved, not being -- trying -- being politically correct, what can we, as Senators sitting on this committee or in this body or in Congress, 535 of us, concentrate and do to allow you to streamline this to make this work? It looks to me like you're going to take a covey of volunteers around the country that are smart and bright, to recruit them, but also, if people are out there hacking us continuously, are they able to intercede? Are they able to see what's going on? Are they able to report -- is there some way of communication that the average person say, "Listen, I've seen some activity going on here that I think is going to be detrimental to us, think you ought to know about." You all have a -- an agency -- I mean, a way that you can collect this information? And what can we do to help to streamline this, to correct this, so it doesn't get so convoluted that something falls

through the cracks?

Whoever wants to take that one, you can --

Mr. Lettre: Senator, I'll take a first crack at it. Really, the most important thing, I think, that we can all do -- and this committee and you all, as members, are incredibly powerfully well suited and seated to be able to do this -- is to have that dialogue, catalyze that dialogue with the public, with civic leaders, with industry leaders, about the shared nature of this challenge, both the cybersecurity challenge and the hacking that we all face across -- from the individual to companies and governments, and the acute threat from -- ongoing threat from terrorism, and the need to put our best foot forward, in terms of countering violent extremist messaging, countering their ability to recruit and persuade over the Internet. And so, that --

Senator Manchin: I think --

Mr. Lettre: -- that dialogue with leaders to really impress upon corporate and civic leaders the need to have -- view that as a shared problem and to really look for solutions with us.

Senator Manchin: Well, the question I'm asking, I think, to both of you all, is that -- I mean, if you're looking at us as a -- everybody says lack of money, it's always a money situation, to a certain extent, or is it a

lack of, basically, siloing to where everyone's protecting their own territory? Is there a way that we can break through, that, if you're going to be that agency, there has to be one gathering point and, basically, one dispensing point. And I'm understanding that some of our agencies aren't talking to each other. We have the situation to where we don't have the private sector cooperating -- San Bernardino, Apple, and all that, that comes to mind. This can't happen. If that's the great equalizer, and we have people that have nothing else more than the will to do us harm, we have to have the will to protect greater than the will to do harm.

Admiral, I'm looking for just a way to help.

Admiral Rogers: So, Senator, I don't disagree with many of the statements you're making. This is my takeaway, having done this for a while now. Using the same structures and the same processes and expecting different outcomes probably is not going to get us --

Senator Manchin: We understand that definition.

Admiral Rogers: -- where we want to be. So, I think the challenge, particularly as we're looking in the future, is, Can we take the opportunity to step back and ask ourselves, "Hey, what do we need to be doing differently?"

The other thing, I think, particular as Senators, as

among the leaders of our Nation, these are serious, hard issues, with a wide variety of perspectives, and we have got to get beyond this simplistic vilification of each other to roll up our sleeves and figure out, How are we going to make this work? Realizing that there's multiple perspectives and a lot of different aspects of this that have to come to the fore.

Senator Manchin: You know, I tell -- I speak to children and -- much as I possibly can. I would -- and I tell them, I says, I don't think -- nowhere in the world is there a military might that can challenge us. We have the greatest military in the world. The economy -- our economy is greater than anyone in the world, almost double the closest -- of China. I'm not worried about a military or an economic takeover of the United States of America. I worry every day about the cyber -- breaking down the cybersecurity, how they hack and whack at us and, basically, come at us different ways. And if we're not defending that, if we're not giving you the tools, and if we're playing politics, being Democrat and Republican and who's politically correct -- this is not a time to do that.

I think there's a group of us here that would love to step out and say, "Okay, how do we streamline this? How do we make sure that someone says, 'We do this, or we

don't do this, or we go in this direction'?" That's what we're looking for. And hopefully you know that we're here to help there.

Admiral Rogers: Yes, sir.

Senator Manchin: Thank you.

Chairman McCain: Senator Shaheen.

Senator Shaheen: Thank you, Mr. Chairman.

And thank you both for being here today.

I want to follow up a little bit on Senator Manchin's question, which was really referred back, I think, to Senator McCain and the Twitter example that you used earlier.

So, how do we get some of those private-sector companies to recognize that this a shared challenge and that we've got to work together? Do we need more legislation to address that? And this is really a policy question for you, Secretary. So, is it that, or is it meeting with folks? What do you think we need?

Mr. Lettre: Senator, our view, at this point in the dialogue and debate, is that legislation that forced or required a regulatory solution is not preferred, at this point. And what we have found is that, on a case-by-case basis, when leaders from the executive branch have been able to have a very effective, quiet dialogue with leaders in industry, that the nature of the conversation starts to

shift in a couple of ways. One is, you know, industry and government, for decades, have worked together very proudly on projects that protect the Nation. And so, reminding ourselves of that rich history, I think, starts to put the conversation into a dialogue around solutions rather than being at odds with each other in an antagonistic way. If, on the government side, we're able to communicate the problems we're trying to solve and ask for industry's best expertise and wisdom about the solutions that might be brought to bear that we haven't even thought about yet, often we find that we are able to come up with solutions that meet our law enforcement and national security needs.

The second thing that I think is --

Senator Shaheen: Well, let me just --

Mr. Lettre: -- that we --

Senator Shaheen: -- I'm sorry to interrupt, but has that worked with Twitter, in terms of the willingness of Twitter to allow us to scrub some of the information that they have?

Mr. Lettre: As was mentioned earlier, to the best of my knowledge, Twitter's position hasn't changed on its level of cooperation with the U.S. intelligence community, so far.

Senator Shaheen: And we were not very successful with Apple, either. Is that correct?

Mr. Lettre: That's right, yeah.

Senator Shaheen: So, there are limits. Certainly, there are limits to that kind of a strategy. I appreciate what you're saying. I mean, I would -- I have a -- always rather try and sit down and resolve the situation rather than pass legislation, but right now we've had mixed reviews of the opportunity to work collaboratively with the private sector to address this issue.

Mr. Lettre: Yeah, that's absolutely fair to say. Now, the industry and the private sector is very diverse. Businesses --

Senator Shaheen: Sure.

Mr. Lettre: -- have different business models, which leave them in different positions, as far as their ability or willingness to work closely with government on working our way through some of these law enforcement questions. So, it -- a case-by-case approach, I think, is what is absolutely needed. But, as you pointed out, we are not successful in every case.

Senator Shaheen: I had the opportunity, earlier this year, to visit Estonia, which, as we know, was the first state subject to a massive cyberattack from Russia. Are there lessons to be learned from examples like Estonia who have experienced this, or from other countries or businesses?

Admiral Rogers, are there lessons that we should be taking from what's happened in other places?

Admiral Rogers: So, it's not by chance that I've been to Estonia twice in the past year. Again, I'm not going to get into specifics, but we have talked about creating a relationship to try to build on it. Although one comment I make to my Estonian teammates also is, what works necessarily in your construct may not --

Senator Shaheen: Sure.

Admiral Rogers: -- necessarily scale directly to a nation of 350- -- you know, 335 million and the largest economy in the world. But, there are perhaps some things that we can take away from this. Because you have to admire -- they sat down and decided this was a national imperative for them, and they consciously sat down and asked themselves, So, what do we need to do to get where we want to be? And then, how can the government help to be a primary driver in this? Not the only focus, but how can we harness the power of the government and their structure to help drive that? And that aspect of it is very impressive, to me.

Senator Shaheen: I would agree with that. I was very impressed with what I heard. But, to follow up on what you're saying, do you think we've reached the point where we believe that this is a national imperative for the

United States?

Admiral Rogers: Intellectually, my sense is, most people intuitively realize that, but then translating that into a series of specific actions to drive broader change than we have done, I think that is still the rub, if you will.

Senator Shaheen: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Cruz.

Senator Cruz: Thank you, Mr. Chairman.

Mr. Secretary, Admiral, thank you for your service. Thank you for joining us today on this vital topic before this committee.

Admiral Rogers, during your testimony to this committee in April, you indicated that the Department of Defense was making significant progress towards establishing 133 Cyber Mission Force teams with plans to be fully operational by the end of fiscal year 2018. In my home State of Texas, I'm very proud of the contributions of the Air Force Cyber Command. I'm glad to see that the Air Force is taking advantage of the unique synergies between the academy, industry, and the military which exist in San Antonio. The combined efforts of the Air National Guard and the Active Duty Forces at Lackland have played, and will continue to play, an integral role in modern cyber

warfare. And I thank them for their hard work, and you for your leadership to ensure that they have the right tools they need to train, to fight, and to win.

Admiral Rogers, would you provide an update on the Cyber Mission Force and detail specific shortfalls that merit congressional assistance?

Admiral Rogers: So, the Cyber Mission Force, 6,187 individuals and 133 teams focused on three missions, providing capability to provide combatant commanders, if you will, with offensive capability, providing defensive capability to defend the DODIN, if you will, the DOD network structure, also the third mission set for us, providing capability to help defend critical U.S. infrastructure against significant acts of cyber consequence, if you will. Three primary mission sets, those 133 teams, if you will, break down into those three different missions.

The first goal we had was IOC of the 133 teams by 30 September of 2016. That's 3 weeks from now -- or 2 weeks or so from now. We will be IOC by 30 September 2016 of all teams. And I would compliment the services, because this is one where, quite frankly, I haven't been the nicest individual, at times, about, what don't we understand about -- this is a goal and a standard, and we are going to meet this. So, we're on track to do that.

The next major milestone, if you will, in the fourth generation, is to be at full operational capability by 30 September 2018, because our experience is that it takes about 2 years to get a team, from the time we stand it up til it's fully mission capable, so the teams we're finishing standing up this month in IOC, we expect it'll take us 2 years to get them to full operational capability.

The biggest challenges meet a continue -- we continue to learn insights about tools on the cyber defensive side that we need to continue to deploy more broadly. I'm trying to use a best-of-breed approach to this across the Department, whereas we generate insights from capabilities that the individual services have -- NSA, DISA, other elements -- let's pick the best of breed, and let's apply it more broadly. Let's not waste money, everybody trying to do their own thing, here.

Investment in the persistent training environment, our ability to actually simulate, in garrison, the networks that we're going to defend, the networks that we're going to operate on. That's fundamental to the future for us. We just cannot afford a model, where we do these major exercises, we try to bring everybody together. It's just a cost-intensive approach to doing business. It's a part of our strategy, but it shouldn't be the fundamental

backbone.

Cyber situational awareness is another area where I would argue we have got to be able to visualize this battlespace. And right now, we just don't do that well. I have prioritized it at a lower level. I'm the first to acknowledge that. We've had to identify where can we take risk, so I've tended to prioritize it lower. But, it's an area where I remain concerned from a -- we need to increase the level of investment. We're taking too much risk.

Those are probably the -- I don't want to give you a long answer, because I know you have limited time, Senator -- those would probably be the three biggest areas that I would argue we need to keep focused on, keep investing on.

Senator Cruz: Okay. Thank you, Admiral.

Let me shift to a different topic. An NBC news article this week claims that, despite evidence that Russia is behind a number of cyber intrusions into American networks, that the administration failed to respond because it determined that we need Russia's help in Syria. If true, the Obama administration will have effectively ignored the threats from an adversary, that it is actively trying to influence the election process and will set a terrible precedent for our country, going forward.

Mr. Secretary, are these reports true? And is this, in

fact, what the administration's done?

Mr. Lettre: I'm not aware of the details of that particular NBC story, Senator, but I'm not aware of any linkage of these issues that I've seen in the policy discussions. The incidents that you've described around the apparent hacking related to our electoral systems is under an aggressive FBI investigation so that the U.S. Government can compose its own conclusions about what has occurred there and what are the appropriate actions to take in response. To the discussion that the committee has been having this morning around cyber deterrence, it will be very important to look at the facts around that investigation and the conclusions from it in order to inform policy choices about what kind of acts to take in response.

Senator Cruz: Very well.

Thank you.

Chairman McCain: Senator Blumenthal.

Senator Blumenthal: Thanks, Mr. Chairman.

Thank you for -- both for your service and the excellent contribution that you're making to our national defense.

I want to return to the Chairman's questions about our electoral system. Isn't there a pretty powerful argument that our systems of elections and voting ought to be

declared critical infrastructure?

Mr. Lettre: Senator, that -- that's an important question. I think, when we look at critical infrastructure across the country, we do need to consider the possibility of attacks on infrastructure causing significant consequences to the U.S. And if there were scenarios where we could envision attacks having significant consequences in our electrical -- electoral context, we really do need to consider that.

Senator Blumenthal: Well, certainly we've envisioned those potential consequences.

Admiral, your response to the Chairman's question was, in part, that this electoral system is -- I think you used the word "disparate," by which I took it to mean decentralized; "disparate" meaning divided and localized --

Admiral Rogers: Yes, sir.

Senator Blumenthal: -- which is true. Every State has its own system. But, as you well know, in our presidential elections, the electoral college is the critical decision maker, which results from elective systems within States. And, of course, elections have consequences at the State and local level, as well, and now many are driven or directed by some kind of computer collection of information, so they are vulnerable, maybe

not at the ballot box, but at some point in the chain of collecting and assimilating that information. Isn't that troubling to you? And I don't know the circumstance of Arizona. You're not familiar with the circumstance of Connecticut, but --

Admiral Rogers: Right.

Senator Blumenthal: -- this is a common thread in our elective system. And we've seen, from some of these hacks, that they can have very severe impacts on the -- these systems, and they are largely unprotected right now.

Admiral Rogers: I think it raises a broader question of, What is truly critical in the cyber world? You know, we've tended to think -- I think, my sense -- we've tended to think along very traditional industrial, in many ways, you know, kinds of lines. And one of the things, I think, that the events in the last few years are highlighting to us is that, for example, we need to think about data in a whole different way. And what are the implications from a security and a critical infrastructure --

Chairman McCain: But, Admiral, wouldn't the selection of our leaders -- of our system of government be -- there should be no discussion about that.

Admiral Rogers: So, Senator, my --

Chairman McCain: If you attack that, and succeed in destroying that, you've destroyed democracy.

Admiral Rogers: So --

Chairman McCain: Why are we equivocating, here, about this? I'm sorry to interrupt.

Senator Blumenthal: No, I --

Chairman McCain: -- Senator Blumenthal.

Senator Blumenthal: Mr. Chairman, you took the words, much more eloquently, out of my mouth. I think there is not only a powerful argument, it's virtually incontrovertible.

And I understand that you're approaching it from a more abstract standpoint. And I don't mean to interrupt, because I'm here to listen to you, but I would hope that there would be a move to designate these systems as critical infrastructure. And why don't you -- I know you were remarking on the --

Admiral Rogers: Yes, sir.

Senator Blumenthal: -- nature of data.

Admiral Rogers: So, my only point is, if you look at critical infrastructure, from a data perspective, and you look at -- So, what are the key data-driven decisions that tend to shape us of a -- as a Nation? -- you come to a very different conclusion about an election that -- structure -- for example, that if your perspective was, "Well, critical infrastructure, to us, is primary industry" -- that that's my only point to you, is, this

leads us, I think, to a different set of conclusions as to what is truly critical, here. And an election system is a good example of that.

Senator Blumenthal: Well, my time has expired, but I think that we really need a national consensus that our electoral system, our system of choosing our leaders, as the Chairman has said very well -- our system of choosing leaders at every level, not just the national level, but State government, State legislators -- all of these systems are going to be increasingly involving the collection of -- you refer to it as "data" -- the data are votes. The votes are individual citizens deciding who their leadership is going to be, which is going to determine who sits in the chair you occupy right now. And these chairs here. And who makes these critical decisions. Nothing is more fundamental -- our financial system, our utilities, our system of healthcare, all are critical infrastructure. And I think our system of electing and choosing leaders is no less so.

Thank you very much.

Chairman McCain: Senator Ernst.

Senator Ernst: Thank you, Mr. Chair.

Gentlemen, thank you very much for coming in today and talking about cybersecurity and its impact on our national security.

I'd like to address some situations from the National Guard perspective. I'm a former soldier in the Iowa National Guard, and I have been tracking the increasing cyber capabilities that both the Army and the Air National Guard are bringing to the table, even in my own home State of Iowa. But, unfortunately, it appears that the DOD has not been tracking this as closely as I have.

A report from the GAO last week stated that, quote, "DOD does not have visibility of all National Guard unit cyber capabilities, because the Department has not maintained a database that identifies the National Guard units' cyber-related emergency response capabilities, as required by law," end quote.

This is a little bit alarming to me, because, in the National Guard, we do have some tremendous capabilities, and we're able to poll a number of those private-sector cyber warriors into the Guard. That's their part-time job and full-time job. So, they are very talented, and we want to see that they are being used to the fullest of their capabilities.

Admiral, how close is the DOD to having a database of all of the National Guard cyber capabilities required by law?

Admiral Rogers: Senator, I can't answer to the specifics of the National Guard Bureau. Let me only say

this. I am the son of a guardsman. My father was enlisted as an officer in the Illinois Guard for 25 years. This is the world I knew as a child, growing up. So, the Guard and the Reserve are something personally important to me. In fact, I just, coincidentally, sat down with a team over the last week and were just reviewing, What's the Guard and Reserve plan, the portion of the mission-force piece?

The point I think you make is both important. I'm the first to acknowledge that. And I will take an action from here to pull the string on this, because, I apologize, I just haven't seen that report, and I don't know the specifics. But, it is reflective. We have always maintained that, as we're building the breadth of capability for the Department in cyber, that the structure we have to come up with has to go way beyond just the Active piece, here, that the Guard and Reserve have got to a critical piece of what we do here, which is why, if you look at what the Air Force is doing, six of their 40 or so teams are Guard or Reserve. If you look at the Army, for example, they are bringing online an additional 22 Cyber Protection Teams from the Guard, purely associated with Guard and State missions, not necessarily the Cyber Mission Force, because they realize the importance of this investment. Marine Corps and Navy, there is -- their

approach, slightly different. Again, they don't have a Guard structure. Their approach, slightly different.

So, if I could, let me take for action that one and pull the strong. And then I apologize, I just don't --

Senator Ernst: No, I --

Admiral Rogers: -- have a good answer --

Senator Ernst: -- I certainly appreciate --

Admiral Rogers: -- for you there.

Senator Ernst: -- that. One team, one fight. I think there's a lot of capabilities that we are simply not utilizing or considering when we look at that big picture. So, I do appreciate that a lot.

[The information referred to follows:]

[COMMITTEE INSERT]

Senator Ernst: And are there steps that you think that you can take that would tie together better our Reserve component, our National Guard component? What kind of efforts can you assist with? What we can we assist with?

Admiral Rogers: So, I feel comfortable, overall, with the, quote, "Cyber Mission Force." Where I think the broader challenge for us is, What additional level of investment, as a Department and in a State structure, do we think that is appropriate, over and above that? And that's probably the biggest focus area for me, working with General Lengyel, about -- So, what should the future be? And then, whatever investments we make in the Guard and Reserve, how do we make sure that they are tied in and aligned with the broader Department effort? So, we're working this as one team. Because we just can't afford -- everybody's out there doing their own thing. And that's just not going to get us where we need to be.

Senator Ernst: Right. Absolutely. I agree.

And then, gentlemen, for both of you, please. The Government Accountability Office also found that the yearly cyber exercise, Cyber Guard, failed to focus on emergency or disaster scenarios concurrent to cyber incidents, an area where the National Guard would be very helpful. And what efforts -- and again, you may not be tied as much into National Guard, but what efforts could

you take to improve Cyber Guard for the upcoming year --

Admiral Rogers: So --

Senator Ernst: -- so that we can focus on those --

Admiral Rogers: -- I haven't seen the specifics of the reports, but I will tell you that, not having read it, I'm, quite frankly, a little bit in disbelief, because I would tell you we call it Cyber Guard --

Senator Ernst: Right.

Admiral Rogers: -- for a reason, because it's focus on, How do we exercise, in an annual basis, the integration of the Guard, Reserve, and the Active component with industry? I spend time at that exercise every year. We just did it in June, down in Tidewater. Some members of the committee, in fact, actually came down and observed it.

So, I'm a little bit perplexed by the basic premise, but I haven't -- I apologize, I just haven't seen the specifics.

Senator Ernst: Okay. And I -- my time is running out. But, again, I think that demonstrates where we do need to put a little more emphasis on our Reserve-component forces and tie those in to our Active Duty component, as well, and really take advantage of the talent that exists out there, make sure that we're exercising their capabilities.

Admiral Rogers: Yes, ma'am.

Senator Ernst: So, thank you very much, gentlemen.

Thank you.

Senator Reed [presiding]: On behalf of Chairman McCain, let me recognize Senator McCaskill.

Senator McCaskill: Yes. I want to follow up with Senator Ernst's comments. I just came from a tour around Missouri, and I had the opportunity to see the cyber unit at Jefferson Barracks, the Guard cyber unit at Jefferson Barracks in St. Louis, and also the Cyber Warriors at the 139th Airlift Wing at Rosecrans Air Force Base. Both were remarkable. Both surprised me. I was not aware -- and I'm not sure, candidly, you're aware -- of all these units and what their capabilities are, and what they're doing. And what Senator Ernst just said -- what was remarkable about the Guard unit in St. Louis was who these people were in their day jobs. We're talking about the very top level of cybersecurity at a Fortune 500 company that has huge needs in this area. Huge needs. I mean, this guy knows more, I would bet, than a huge number of the people that you are commanding within the Active military, in terms of both cyber offense and cyber defense.

And I've realized that this is a great opportunity for our Guard to recruit some of the most talented and technically capable people in the private sector, since the vast majority of the networks that we are supporting,

in terms of protection in this country, are, in fact, private networks.

And so, I wanted to bring that up with you and ask your opinion about that integration, and particularly as it relates to the lynchpin with the Department of Homeland Security. Because the beauty of the Guard is, it is busy with domestic security as part of their mission, because of the TAG and the involvement of State governments, whether it's a natural disaster or other kinds of problems. And so, it seems to me that utilizing the Guard as the lynchpin between the Department of Homeland Security and the Department of Defense would make a great deal of sense, Admiral Rogers. And I would like your comment on that.

Admiral Rogers: First of all, I agree with the fundamental premise that the Guard and the Reserve bring a lot of capability. That's one reason why the Cyber Mission Force idea is predicated as the idea -- it's our ability to bring it all together -- not just all Active, not just Guard; it's the ability to bring it together.

In terms of who should be the fundamental lynchpin -- before I get into publicly endorsing a particular strategy or solution, this is just one I want to make sure we think our way through. Because in -- there are challenges if you do it Active-only. There's challenges if you do it

over Guard- or Reserve-only. And I'd also be interested: Hey, what's DHS's perspective in this?

One of the other challenges I've found so far in my time in command, we have to work our way through what -- and this is where the Guard, I think, becomes incredibly critical -- what's the difference between -- we're using DOD capability to work Federal large critical infrastructure versus what is the capability DOD -- by extension, the Guard -- can bring to the fore at a much more localized State and local level? And that's an area that, clearly, the Guard is very optimized for, that the Active piece is not as readily optimized for.

Senator McCaskill: I'm sure one of our problems in this space is retaining Active personnel, because if they become very skilled in this area, the -- there's lots of lucrative opportunities in the private sector. Has there been any thought given to an active recruitment of these folks into the Guard as they move into the private sector for a lot more money and people not being able to tell them where they're going to live 24/7? Is it possible that we are losing an opportunity, in terms of retaining some of the talent that we have, by not directly recruiting them into the Guard?

Admiral Rogers: So, knock on wood, retention on the Active side is exceeding our expectations. That doesn't

mean it won't change tomorrow or next week or next month.

I will say, since the Guard is an Air Force and an Army-specific construct, I know both of those services, in my discussion with my subordinate commanders from them, talk about, how do we make sure, as we're watching the workforce transition out of the Active -- separate, retire -- is there a way to tie in the Guard piece? Senator Cruz mentioned San Antonio, for example. I've seen several instances in the San Antonio area, because they're such a large concentration, where this is working very well. I'm not sure how well it's working in those areas where we don't have this large Guard and Active --

Senator McCaskill: Right.

Admiral Rogers: -- complement of force, if it will. So, I just don't know, off the top of my head.

Senator McCaskill: And this idea has been discussed openly, and I know there is a lot of controversy around it and a lot of pros and cons, but one of these really talented cyber warriors at the Guard unit that I visited with, I was told that one of them almost was removed because of sit-ups. What about the PT requirement? And what value is there to forming an elite cyber squad that is civilian, as opposed to, you know, losing a really talented guy because of sit-ups?

Admiral Rogers: So, my first comment would be,

remember, the Law of Armed Conflict specifically prescribes what civilians and uniforms can do in some particular applications. So, I generally remind people, a lot of it would have to do with, what would the mission be that you gave that entity? Because there are some things in the Law of Armed Conflict that physically could not do. Uniforms have to do it, as opposed to --

Senator McCaskill: Right.

Admiral Rogers: -- application of force and capability.

To date, are there numbers where that is an issue? Clearly. I'm not going to pretend, for one minute. But, we have been able to retain people and still meet the requirements associated with the broader military without decreasing capability. If that changes over time, though -- it's one of the things I have talked about -- we need to be mindful that if circumstances change, we need to look about changing the rules that we currently operate. And if the situation were to change, those would be one of the things I would say, "So, do we need to look at a different force balance or mix? Do we" --

Senator McCaskill: Right.

Admiral Rogers: -- "need to look at a different set of standards or requirements associated with individuals?" I don't think we're at that point now, but if the situation

were to change, I think we would definitely need to do that.

Senator McCaskill: I would certainly urge that flexibility --

Admiral Rogers: Yes, ma'am.

Senator McCaskill: -- because I think this is going to be a growing part of our national security --

Admiral Rogers: Right.

Senator McCaskill: -- piece.

Admiral Rogers: Thank you.

Senator Reed: On behalf of the Chairman, let me recognize Senator King.

Senator King: Thank you, Mr. Chairman.

It seems to me the good news is that we're the most wired society on Earth. It gives us fantastic efficiencies and productivity and advantages, in many ways. But, the bad news is, we're the most wired society on Earth, which means we are the most vulnerable.

Admiral Rogers, you're familiar, I'm sure, with the Ukraine hack of the grid in December 2015. One of the things we learned from that is that there -- that hack was much less serious than it might have been, because of some retro technology --

Admiral Rogers: The antiquated --

Senator King: -- analog switches, old Demetri, who had

to go out and throw a switch somewhere at a relay. Do we have some lessons from that, that we ought to be thinking? And thinking about elections, it's hard to hack a paper ballot.

Admiral Rogers: Sir.

Senator King: Those kinds of things. Is that -- should we be examining that area?

Admiral Rogers: I mean, we certainly are. I mean, one of the lessons, I think, from the Ukraine, for example, is, not only the analog, the physical piece, but also the way that their grid was broken down into components.

Senator King: Right.

Admiral Rogers: It's leading to some things. For example, as a naval officer, we're teaching celestial navigation again --

Senator King: I was going to bring that up.

Admiral Rogers: -- at the Naval Academy.

Senator King: I understand it's the first time in 20 years that --

Admiral Rogers: Right, which we had stopped doing, because we said to ourselves, "Well, we have automated chart processes now. Why would we need to use celestial bodies to -- for navigation to define out" --

Senator King: Because you can't hack a sextant.

Admiral Rogers: Yes, sir. And so, we acknowledge that

there are things that we are going to need to look back, in this current world we're living in, and say to ourselves, "Perhaps some of the assumptions that we've made are not going to prove to be accurate." And we've got to ask ourselves, "What are the second- and third-order implications? What have we got to train differently? What skills do we need to have that we perhaps" --

Senator King: But, we also need to --

Admiral Rogers: -- "for the last 20 years have said we don't need?"

Senator King: As you -- as I think you've said, we need to question the basic assumption that digital is --

Admiral Rogers: Yes, sir.

Senator King: -- always better.

Admiral Rogers: Yes, sir.

Senator King: Senator Risch and I have a bill in before the Energy and Natural Resources Committee to ask the National Labs to work with the utilities to look at the Ukraine situation and see if there are places -- not to de-digitize the --

Admiral Rogers: Sir.

Senator King: -- grid, but places where there could be analog switches or other devices put in to deal with just --

Admiral Rogers: Right.

Senator King: -- just this issue.

Let me turn to encryption for a minute. While this hearing was going on -- and I don't want to sound like this was a big production -- in about, literally, a minute and a half, I downloaded Telegram. And Telegram is an app, as you know, that's encrypted. I thought it was interesting. I looked at what it -- how it works. It's fully encrypted. It's in English, Arabic, Dutch, German, Italian, Korean, Portuguese, and Spanish. It's -- was started by two brothers from Russia. It's based in Berlin. I mean, this is the reality, isn't it, Mr. Lettre, that we're -- we can't stop this. The idea of somehow being able to control encryption is just not realistic.

Mr. Lettre: We can't stop these trends, you're right, Senator. And individuals -- all of us benefit from strong encryption. The Department of Defense does. I personally am in favor of having strong encryption that allows me to protect my personal data. The challenge is -- and yet, we need to find our -- think our way through how we can continue to fulfill our responsibilities to enforce the laws and protect the Nation. And I think what we do find is, there are a number of instances where government leaders have been able to strike a very collaborative and

cooperative dialogue with key sectors in the text sector. Individual players and executives have been able to focus on finding --

Senator King: But, that --

Mr. Lettre: -- solutions.

Senator King: -- that worked pretty well in the '20s, when you were talking about the telephone system, which was only within the country. And you can -- we can deal with Apple or with Microsoft or with Cisco or whoever, but if you've got a cloud-based app that's -- the headquarters is in Berlin, and who knows where the data is -- I mean, we -- as hard it is for us to believe, there are places our power doesn't reach. We can't regulate something that's over in Berlin or Swaziland.

Mr. Lettre: That's a very good point. There will always be places across these sectors and these technology solutions that we just -- we may not be able to find a way forward. They may be -- the solution may be elusive.

Senator King: Well, I'd like --

Mr. Lettre: It does require us to think innovatively --

Senator King: Well --

Mr. Lettre: -- even beyond encryption, about how we can continue to go after national security challenges.

Senator King: That was -- you know, the word "innovation" -- I mean, this is a -- this is the world

history of conflict, is invention, reinvention, reinvention, reinvention.

And I also want to associate myself with Senator Lee's questions. We also need to get back to old-fashioned human intelligence. And I think it's -- SIGINT was easy, in a sense, if you can pick up conversations. Now that that's no longer as easy as it once was, we need to be thinking about, what are the other techniques that we can use? They -- and it may be old-fashioned intelligence. It may also be other high-tech satellite or other things. But, it -- it's -- we can't -- I think innovation is going to be an absolute key to this.

Mr. Lettre: Yes. That's absolutely right, Senator. The -- in particular, as you pointed out, we do need to build innovation across a range of intelligence disciplines and collection capabilities. So, even in the human intelligence arena, we know how effective it can be. We also know that technology trends are changing how we do HUMINT. And we need to be able to adapt and invest in innovation, in how we conduct our human intelligence operations, as well.

Senator King: And my time is up, but I would suggest big data analysis is one of those tools.

Mr. Lettre: Absolutely.

Senator King: Thank you.

Thank you, Mr. Chairman.

Senator Reed: Thank you, Senator King.

On behalf of the Chairman, let me thank you gentlemen for your testimony today and your service.

And, since there are no other colleagues here, I would call the hearing adjourned.

Thank you.

[Whereupon, at 11:20 a.m., the hearing was adjourned.]