Stenographic Transcript
Before the

Subcommittee on Emerging Threats and Capabilities

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON MILITARY CYBER PROGRAMS AND POSTURE IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2016 AND THE FUTURE YEARS DEFENSE PROGRAM

Tuesday, April 14, 2015

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON

MILITARY CYBER PROGRAMS AND POSTURE IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2016 AND THE FUTURE YEARS DEFENSE PROGRAM

Tuesday, April 14, 2015

U.S. Senate
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:35 p.m. in Room SR-222, Russell Senate Office Building, Hon. Deb Fischer, chairman of the subcommittee, presiding.

Committee Members Present: Senators Fischer [presiding], Ayotte, Ernst, Tillis, Nelson, Gillibrand, and Donnelly.

OPENING STATEMENT OF HON. DEB FISCHER, U.S. SENATOR FROM NEBRASKA

Senator Fischer: Good afternoon. The hearing will come to order.

The subcommittee meets today for its annual posture hearing on military cyber programs. And I'd like to welcome all of our witnesses today, and thank each and every one of you for your very honorable service to this country.

Our hearing will be structured in two panels. First, we will hear from Mr. Eric Rosenbach, the Principal Cyber Advisor to the Secretary of Defense, and Lieutenant General Kevin McLaughlin, the Deputy Commander of U.S. Cyber Command. Then, after we do a few rounds of questions, we will ask each of the cyber component commanders to provide their opening remarks and also respond to the committee's questions.

Given the number of witnesses, we ask that everyone keep their remarks to 5 minutes. And your full written testimony will be included in the record.

While the hearing today is the fourth Senate Armed Services hearing on cyber this Congress, it is the first of what I hope will be many engagements for our Subcommittee on Emerging Threats and Capabilities. I thank our witnesses for being here today, and I look forward to their testimony.

With that, I would ask that the full text of my opening

statement be entered into the record without objection.

[The prepared statement of Senator Fischer follows:]

[SUBCOMMITTEE INSERT]

Senator Fischer: And I would like to welcome the Ranking Member of the committee, Senator Nelson from Florida, to offer any remarks he may have.

STATEMENT OF HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator Nelson: Thank you, Madam Chairman.

Welcome. We are obviously at a critical juncture. There's a real cyber threat out there. This Senator certainly has a concern that, despite all of the alarms that have been raised about the cyber threat, we still don't seem to be taking it very seriously.

Not long ago, Admiral McConnell, the Director of National Intelligence and NSA as well as the head of Cyber Command, stated his belief that foreign adversaries could bring down the grid on the East and West Coasts through cyber attack. Recently, I received a briefing from well-informed industry experts that were tasked in a national security staff-sponsored cyber threat exercise. And what they briefed me is that a relatively small group of knowledgeable people could bring down the economy of this country in 3 days. They could wreck the Internet and other critical infrastructure systems in this country in relatively short order. Now, such forecasts are made despite the standup of Cyber Command and assurances about how well it's progressed in its ability to protect the country.

It's still hard for us to get the U.S. Chamber of Commerce to come in behind any legislation involving cyber

security except that which would be entirely voluntary on the part of the business community. And, in light of these real-life cyber attacks, it seems to me that offense in cyber has the sort of advantages that ballistic missiles have enjoyed over missile defenses for over a half a century, and that cyber weapons can have the effects like weapons of mass destruction.

So, I'm concerned that, in the case of cyber, we are not being honest with ourselves, or the American people, that effective defenses are practical and within the reach of our military in the near term. Specifically, I'm concerned that Cyber Command inherited a strategy from NSA signals intelligence from that culture that has significant limitations in the context of military operations.

Our intel agencies always strive, appropriately so, to know everything about an adversary's capabilities. And, in cyber, that means gaining knowledge of the other side's malware and, whenever possible, their intentions for executing attacks. The hope is that NSA and Cyber Command will reliably have such full insight and can take effective action. But, it's unreasonable, in this Senator's view, to rely so heavily on the success of our intelligence operations to anticipate attacks, especially in an area like cyber, where technology enables adversaries to be quite elusive and to be able to go on the offense without us

having a sufficient defense. We must assume that determined adversaries will be resourceful enough to keep secrets from us and to achieve significant surprise. And I don't expect that we're going to have the capability to completely neutralize our adversaries' cyber force, given that computers are cheap and easy to replace, and that the Internet is a vast domain in which to hide and maneuver.

And so, this then brings up the issue of deterrence. Our critical infrastructure is vulnerable, but at least there is deterrence with folks like Russia and China, because they have a lot to lose, as well, knowing that we could respond offensively with a large-scale attack on their economic targets.

So, it's just like the ICBMs of years ago, mutual assured destruction. But, what about the rogue nations or rogue elements -- North Korea, Iran, and so forth? And we've certainly had examples of that already -- the Sony attacks, et cetera.

And so, I want to know from our witnesses if you would agree that deterrence in these circumstances may not be really possible. After Cyber Command's creation, we are finally fielding trained military forces to execute operations. We're about halfway towards our force goals. But, these forces are, to a significant degree, in this Senator's opinion, hollow, in that we are not yet able to

equip them with the tools they need to function effectively. We're in a situation, although understandable -- a flawed assumption is that military cyber operations would be an extension of NSA's SIGINT activities, including utilizing the same tools and infrastructure. And, while NSA has always, obviously, got to be a critical partner for Cyber Command, it's now understood that this Command needs a different set of capabilities.

And so, I want to get into that, Madam Chair, as we get into our discussion.

And if you guys can't answer the questions, then let's go into a classified setting.

Thank you, Madam Chair.

Senator Fischer: Thank you, Senator Nelson.

We do plan to have two panels today. And we'll keep track of questions that you gentlemen are unable to answer in an open setting, and then we will go to a classified setting after that.

But, welcome, again, to the subcommittee. If you have your opening statements ready, we will accept those at this time

Mr. Secretary, if you'd like to begin, please. Welcome.

STATEMENT OF HON. ERIC ROSENBACH, PRINCIPAL CYBER ADVISOR TO THE SECRETARY OF DEFENSE

Mr. Rosenbach: Thank you very much, Madam Chairwoman, Ranking Member Nelson. I really appreciate the opportunity to testify here before the subcommittee to you and other members of the subcommittee.

And I'm also very happy to be with Lieutenant General McLaughlin, the Deputy Commander. He's a very good partner in all this, along with the services, who are working hard.

I think that I don't need to spend a lot of time telling you about the cyber threat landscape, as Senator Nelson just explained. But, over the past several years, we've seen that this is growing, both in sophistication and urgency. When you look at something like the Sony cyber attacks or other things, attacks just against our own DOD networks, we recognize that we need to take this very seriously, both from the state and the nonstate perspective.

Another thing that is really important to highlight, though, is that we're very realistic, from the Department of Defense perspective, that this is a team sport, that we do not actually have the lead for all domestic cyber security, that DHS is the lead for many aspects; we need to partner with the FBI; and, just as you mentioned, Senator Nelson, that the private sector has a very important role in protecting themselves. We do have a key role, though. And

I'll talk a little bit more about that.

I would like to tell you a little bit about the way we think about deterrence, because this is critically important to our thinking. And, in light of the evolving nature of the threat, DOD is committed to a comprehensive, whole-of-government cyber strategy to deter attacks. This strategy depends on the totality of U.S. actions, to include declaratory policy, overall defensive posture, effective response procedures, indication and warning capabilities, and the resilience of U.S. networks and systems.

Within this, we have three specific roles within the U.S. Government, from a deterrence perspective:

First, we need to develop capabilities to deny a potential attack from achieving its desired effect.

Second, the U.S. must increase the cost of executing a cyber attack. In this regard, DOD must be able to provide the President with options to respond to cyber attacks on the U.S., if required, through cyber and other means. So, something that I would like to emphasize is, although it's a cyber attack, we don't think about the response purely through a cyber lens. It would be all the tools of foreign policy and military options.

And finally, we have to ensure that we're resilient, so, if there is an attack, that we can bounce back. This, when it comes down to it, is pure cost-benefit-type analysis

to make sure that the costs are much higher than the benefit to the adversaries who want to attack us. But, again, I have to be very candid that some type of attacks are much easier to deter than others. In the case of nation-states, those are easier to deter. As you mentioned, sir, the Chinese and the Russians, easier to deter -- much easier to deter than the North Koreans or the Iranians, and, some of the lower-level criminal attacks or the theft of intellectual property, the most difficult, as I know you all understand.

In order to bolster this deterrence strategy in the Department, we've made the conscious decision to invest in capabilities, and the Cyber Mission Force in particular, that allow us to improve our deterrence posture. So, we have built robust intelligence. I do think that it's an important part of it, although not the core part. I would agree with Senator Nelson on that. And we know that we need to reduce the anonymity in cyberspace so that adversaries who attack us don't think that they can get away with it, that we know who they are, that they will be identified, and we'll be able to take action. These attribution capabilities have increased significantly in recent years, and we continue to work closely with intelligence and law enforcement to improve this.

I just want to remind you all, there are three

important missions that we have in DOD:

The first, and our most important mission, is for us to defend our own DOD networks. I know that may be surprising. When you think about the Department of Defense, we're very network-reliant and network-centric, the largest enterprise network in the world. All of our military operations depend on our network. And that's why Cyber Command's first job is to defend DOD networks. The Secretary makes that very clear.

Second, we need to defend the Nation against significant cyber attacks. This is a small part of all the cyber attacks against the U.S. This is not a denial-of-service attack, unless it would cross the threshold of armed attack, for most instances. Right? The Department of Defense is not here to defend against all cyber attacks; only that top 2 percent, the most serious.

And then, finally, we want to provide full-spectrum cyber options to the President or the Secretary in cases where that would be advantageous to our national interests.

To carry out these missions, we're building a Cyber Mission Force which is composed of 133 teams. I can tell you more details about that. But, I want to emphasize, too, that there's an important role for the National Guard and Reserves. We want to capitalize on the expertise that folks who are in the private sector but still want to serve the

country have. And we've already worked with the services to allow some force structure on that. And developing this talent in a cadre of cyber experts is very important to the Secretary. Since Secretary Carter has been here, it's one of his top priorities, is ensuring we have new tunnels through which talent can come into the Department and cyber and other ways.

Again, to show that we're thinking very clearly about this, next week we'll release a new strategy for the Department that will guide the way forward for the next several year in cyber. The Secretary has driven this, he's very action-oriented, with projects, milestones, and things that we'll be able to measure our effectiveness on. And I'm more than happy to tell you all some about that today, and a lot more in the future, next week.

Also, I just want to emphasize how important building strong partnerships is -- with the private sector, with our other government agencies, and with allies and partners. The geography of the Internet itself means that we can't do this alone, and we've invested a lot of time, even recently, in Asia, the Gulf, and other places in the Middle East, and, of course, with our traditional allies, the five allies, and in NATO, in this area.

So, in conclusion, I think it's also important to emphasize that the role that Congress plays in this is very

important, both in passing legislation, like the information-sharing legislation, or cyber security legislation that improves the standards of cyber security. Up til now, we've had a very good relationship with the Senate Armed Services Committee and your staff. We want to be very helpful. I look forward to that continuing over the next several years.

With that, I'd request that I could submit my written record for -- or, my written testimony for the record, and turn the podium over to Lieutenant General McLaughlin.

[The prepared statement of Mr. Rosenbach follows:]

Senator Fischer: Thank you, Mr. Secretary. General.

STATEMENT OF LIEUTENANT GENERAL JAMES K. McLAUGHLIN, USAF, DEPUTY COMMANDER, U.S. CYBER COMMAND

General McLaughlin: Madam Chairman and Ranking Member Nelson, thank you very much for having us here today. It's a pleasure to be before you.

It's an honor to also testify with Mr. Rosenbach, our Principal Cyber Advisor to the Secretary of Defense.

And it's an honor to be able to tell you a little bit about what's happening at United States Cyber Command, to represent the hard work of the men and women that are in our Command, and so you could hear a little bit about what their focus is today.

I think that, both in your opening comments and in Mr. Rosenbach's, a discussion of threat is sort of paramount. And I think what I'd, maybe, just add to that is, what's different today, on the military side, is commanders. Whereas, before they might have thought of the threat as a nuisance or something where maybe, you know, people were conducting espionage against the United States, realize that, today, the cyber threats are actually something that could actually threaten their ability to command and control their forces and put at increased risk to their ability to accomplish their mission, and that -- the Sony attacks are a great example, and it's not lost on them that, today, destructive attacks could occur against, you know, their own

cyber terrain, making it difficult or impossible for them to accomplish their mission. So, the threat, in that context, is not just important to U.S. Cyber Command, but it's important to the Department, you know, writ large.

The -- so, the real -- the issue is, What are we doing about it? And so, the creation of U.S. Cyber Command, again, as Senator Nelson kind of went through a little bit of our history, we've been around just a little bit over 4 years. We are about halfway into the fielding of our Cyber Mission Force, which are the 133 teams, which are a significant way of bringing capacity and capability to bear in our ability to defend the United States and to accomplish Department of Defense missions in cyberspace.

Admiral Rogers, as -- in addition to the three missions that Mr. Rosenbach laid out that U.S. Cyber Command has -- has really laid out a vision that -- where we have four imperatives within our Command aimed at getting after the challenges that have already been laid out today and that I think we'll discuss in more detail.

The first is to defend our Nation's vital interest in cyberspace. We don't do that alone. As was mentioned, our primary lane in the road is to defend our Department of Defense networks and then to bring military capabilities to military commanders. But, we do know that, as part of a broader team with other parts of the government, with the

private sector and with our allies, there is a much broader strategic mission that's really on the plates of Americans and our allies. And that's, How do we deal with the threats, more broadly, to the Nation? And that is a key part of this first imperative.

Second, we have to operationalize this mission set. There was a early part in Senator Nelson's comments about early focus, perhaps, on approaches that might align themselves with the intelligence business. And we know we're dependent on intelligence in this area, but what we have to focus on is bringing an operational mentality to this space. This is not just an IT-focused endeavor. This is an operational domain. And so, we are bringing the same operational mindset and processes that we would see in any of the other domains. That's a critical transition, culturally and from a mindset perspective, to how we think about operations in military cyberspace.

Third, we have to integrate cyberspace operations in support of joint-force-commander objectives. A key part of the capacity and capability that we're going to bring is there to support the operations of other commanders, noncyber-focused commanders. And so, a key focus for us is to make sure we integrate and we bring capacity to all the combatant commanders around the globe, and that they have a place to turn for cyber capability, whether it's defensive

or offensive in nature.

And then, last, accelerate towards full-spectrum capability. We have to have the ability not just to do -- to defend our networks. That's critical. Not just to command and control cyber forces. But, we have to be able to bring full-spectrum capabilities, including offensive capabilities, to bear if we're going to be a full command, able to meet the challenges of our Nation.

All of these forces, as we bring them into being, will also have to be trained and brought to a high level of readiness. And so, you wouldn't expect a fighter wing or a carrier strike group or a brigade combat team to ever go into combat if it hadn't been fully trained and certified as ready to conduct its warfighting mission. And so, a major focus for us will to be to make sure that the forces that we have are also brought up to that same level of readiness and that, when they are asked to go into combat, that -- you know, that the commanders understand that they're certified and they're able to do their job.

It is a real privilege to be here with you today. I would like to thank the committee for its strong support, and the Congress for their support, in this area. This open testimony is important for us to actually -- just to make sure that these important issues are both understood by, you know, the rest of the military as well as the American

people that are watching this. We look forward to working with you as partners, help operationalize the cyber domain, and to make, you know, the challenges that we're faced a little bit less daunting in the future.

Thank you.

[The prepared statement of General McLaughlin follows:]

[SUBCOMMITTEE INSERT]

Senator Fischer: Thank you, General.

We will start with 6-minute rounds. And I will begin, for either of you gentlemen to answer.

In the President's FY16 budget in dealing with cyber investments, he has $5.5 billion in that budget, but yet we only are looking at 8 percent of that going to Cyber Command and the development of the Cyber Mission Forces. Do you think that's sufficient?

Mr. Rosenbach: Ma'am, I'll take that first.

I'd say we need to be careful when we look at the cyber budget, because, although maybe 8 percent -- and I'm not sure about that number -- of the 5.5 billion is going directly to CYBERCOM, there's a lot of money that goes indirectly, through NSA or through DISA or through other places, that ends up supporting them. So, NSA is a combat-support agency. There are lots of things they do to support CYBERCOM.

That said, in the Department and in a fiscally constrained environment, cyber is one of the only three areas where it's either held or grown over the last several years. And the Secretary has made very clear that it's an area that will continue to receive increased growth, and the vast majority of that is for Cyber Command. So, the bottom-line answer is, we even assess that 8 percent is not enough and that there should be some additional growth, and

that's part of the strategy, moving forward.

Senator Fischer: Can you give us any examples of what's needed to more efficiently and effectively provide training?

General McLaughlin: So, ma'am, what we have on the training side -- let me first tell you what we have, and what it is that we still need -- one thing that we do have is, as we were directed to bring on the 133 teams, each of the services -- and you'll be talking with some of those component commanders in a little bit -- were asked to build capacity, really almost overnight, to be able to produce, you know, young enlisted and young officers that could come onto these teams. That part of the training's going great. They went from a standing start, doubled, and then really doubled again their capacity to build those people that are the initial accessions onto these teams.

The place that we still have work to do, and we're pursuing it with vigor, is what we call the persistent training environment. And that is the ability now to take those teams, once the people show up, and -- like we would in -- you know, in any other warfighting domain -- and have the ability for those teams, either subsets of teams or entire teams, to do training against -- routinely -- against, you know, live adversaries, like aggressor forces, to be able to do mission certification or mission rehearsal

events, and to sort of train throughout a continuum from the time they show up until the time they might have to deploy or do their COMINT job.

Senator Fischer: Right.

General McLaughlin: That part --

Senator Fischer: I'll speed you along a little bit on that.

On -- but, when we're looking ahead, can you say, in this setting, what you feel will be needed in the future?

General McLaughlin: Yes, ma'am, I'd -- what's going to be needed in the future is, we need to have a couple of components. We need to have a range environment, so the virtual environment for these forces to do training. It needs to be interconnected throughout the United States. We need to have aggressor -- you know, forces that replicate the adversary so that there's someone to train against. We have to have people that actually manage and sort of write training scenarios and scripts. So, it's all the components that make up the capacity to train our forces.

Senator Fischer: You mentioned, General, earlier, about the readiness and the force structure. How do you measure that? Where do you come up with, say, the number 6200? How do you measure that at all?

General McLaughlin: Well, ma'am, the initial sizing of the Cyber Mission Force, I think, was really put together to

-- with an estimate of the amount of offensive and defensive capacity we thought we needed as a Department.

Senator Fischer: Have you been able to, I guess, verify that number, or are you still in the process of estimating what you need on that for readiness and to be prepared and just moving forward? Where are you on that?

General McLaughlin: Ma'am, I would say that we are primarily focused on taking the forces that have been allocated to us and, on the readiness side, to make sure those forces are trained and ready. I don't -- I wouldn't say that we've done a lot of analysis up to this point to determine: Is -- are 133 teams the right number, or enough? We're mostly trying to take those teams and make sure that they're ready to do their job.

Senator Fischer: So, you can't say, at this point, if that number would be adequate.

General McLaughlin: No, ma'am. But, I also wouldn't be able to say that it's not adequate. You know, our view right now is, we're only halfway fielding the teams. So, I think we would have to get them all the way fielded and have them at full operational capability to be able to do reasonable analysis as to whether or not there's sufficient resource there.

Senator Fischer: When you look at the question of deterrence -- and, Mr. Secretary, I appreciated your

comments on that, that it wouldn't necessarily be a cyber response to a cyber attack -- but, do you think, at this point, our adversaries view an attack on either government agencies or the private sector -- but, let's focus on government agencies -- do you think they're -- they view an attack right now as low risk for a high reward?

Mr. Rosenbach: Ma'am, I'd say it really depends on what type of attack. I would say they probably do view it as low risk, when it comes to the exploitation and trying to steal data. I would say it's considerably a higher risk if they were to conduct a destructive attack against a DOD network, for example. The deterrence level there is much higher, and I think they see that as high risk, which is what we go for.

Senator Fischer: Thank you.

Senator Nelson.

Senator Nelson: Thank you, Madam Chairman.

Obviously, NSA is going to be a critical partner for Cyber Command. And I think it's pretty well, however, understood that Cyber Command needs a different set of capabilities: command and control, operational planning, situational awareness, battle damage assessment, mission execution, network infrastructure, weapons.

Mr. Secretary, do you agree that Cyber Command lacks robust joint computer network infrastructure to execute

military cyber campaigns effectively?

Mr. Rosenbach: Yes, sir, they currently do not have a robust capability.

Senator Nelson: Well, what are the attributes of the needed infrastructure?

Mr. Rosenbach: Sir, I can go into a lot more detail in a closed session. But, I would say, here, that the ways we think about this depend on offense or defense. In defense, I think we have pretty robust capability, and we're in good shape, but could be better. And I think big data analytics could make that even stronger, something we're calling the "unified platform," bringing that together. On offense, Secretary Carter, when he was Dep Sec Def, made the decision and put money against a more Title 10-specific infrastructure that would be for military options, that goes after a platform and access and a payload, to put it in very simplistic terms. But, I can talk to you a lot more about that in a classified session.

Senator Nelson: Okay. Do you agree that Cyber Command lacks a robust command-and-control platform and systems to plan and execute fast-moving and large-scale cyber operations?

Mr. Rosenbach: Yes, sir, I agree with that.

Senator Nelson: You agree that Cyber Command itself does not have the resources or expertise to build this cyber

command-and-control infrastructure and weapon systems.

Mr. Rosenbach: At this point, sir, I think that the question of resources is one where we have added resources in those areas. And, because we're trying to be very smart about attacking a very difficult technical problem, we're doing it in a measured way to be good stewards of government money. These are very hard technical problems. And, rather than invest a large amount of money before we're sure, we're kind of taking that incremental approach, but are working towards it. And, I think, when we see success, the Secretary, in particular, will be willing to invest more in it.

Senator Nelson: Well, if you don't have the resources, do you think that the military services will have to do this?

Mr. Rosenbach: Sir, there's no doubt the services play a huge role in this. And I say this very honestly, that what they've done, thus far, has been great, and they will continue to play a key role in --

Senator Nelson: I'm sure. But, we're trying to help you, here. So, are the Army, Navy, and Air Force prepared to step up and budget for these joint requirements?

Mr. Rosenbach: It depends on the service, but, in large part, the services are stepping up, although, in a tough environment like we have right now, it's very hard for

them to allocate existing resources to cyber. And so, one of the things that we're looking at is whether there should be new resources for the services.

Senator Nelson: So, you're not even to the point of allocating the task to each of the services.

Mr. Rosenbach: It depends on what the task is, sir. But, here's why we haven't specifically allocated tasks to each of the services. There is as big decision to make about the model that we want for CYBERCOM. And, essentially, it comes down to this. Is CYBERCOM going to be more like SOCOM, with those types of authorities and that type of model, or is it going to be something closer to now that is much more reliant on service-generated man/train/equip and the capabilities, in particular? That's a decision we're thinking very consciously about, but have not yet made.

Senator Nelson: And that's the lack of a policy decision that has been made. And so, does Cyber Command have the resources and the expertise to at least produce operational requirements?

Mr. Rosenbach: I think it depends. And, honestly, I'd prefer that you ask General McLaughlin for his perspective on that so that I'm not answering too much for the Command on that.

Senator Nelson: Well, let me ask you. If you're

lacking in this area, which you've already said, basically, that you don't have the budget for it, how is the Secretary -- what should the Secretary of Defense do to provide the needed support?

Mr. Rosenbach: I guarantee you this, sir, that Secretary Carter really cares about cyber. He's taking it very seriously. And if we see that there's a need for additional resources, he would be the first one to put them there.

The other thing I would say is, it's nothing against CYBERCOM, but it's a young command. It's nascent and it's still growing. And it does take a very highly developed human-capital base to make acquisition decisions, to run programs, things that, traditionally, the services have done. And that's why we're thinking so carefully through this.

Senator Nelson: In your planning, do you plan to hit nonmilitary targets?

Mr. Rosenbach: Sir, I can tell -- I can touch a lot more detail in a closed session. But -- yes, but in a very, very precise and confined way that would always adhere to the Law of War and all the things we think about for collateral damage and other targeting. And I'm sure General McLaughlin could add more to that; in particular, in a classified environment.

Senator Nelson: Such as, if, for example, that you wanted to take out the enemy's air defenses, you could go in and knock out the power stations, the civilian power stations.

Mr. Rosenbach: Sir, you know, I think talking in a classified environment would be better for specifics. And then I can go into great detail about things like that.

Senator Fischer: Thank you, Senator Nelson.

Senator Ernst.

Senator Ernst: Thank you, Madam Chair.

Thank you, gentlemen, for being here today.

This past weekend, I had a very exciting drill, in that we, in the Iowa National Guard, spent some time discussing our 2016 Vigilant Guard exercise. This is exercise play which will involved Federal agencies, of course the Iowa Army and Air Guard, as well as State agencies, local agencies. It's a series of -- the play will include a series of weather and natural disasters, but also including cyber attack and security issues. And it is something that we have recognized at all levels in the government in Iowa, that this is a very real possibility.

So, I appreciate you stepping up. I know that the Command is new, but I look forward to those challenges and opportunities that we have in developing that. And I am excited about the 17 series cyber branch bringing on

officers and new soldiers into that area. I will tell you, in the Guard, we have a great number of members that would quite adequately fill into those types of activities.

Admiral Rogers, I believe, on March 4th before the House Armed Services Committee, he did state that there -- in quote, "There's no DOD solution to our cyber security dilemmas. The global movement of threat activity in and through cyberspace blurs the U.S. Government's traditional understanding of how to address domestic and foreign military, criminal, and intelligence activities.

And, with that being said, the fiscal year '14 NDAA directed the President to develop an integrated policy to deter adversaries in cyberspace and to provide that cyber deterrence policy to Congress within 270 days. And that deadline has come and gone, and we have not seen that policy. Considering that we see a continuously evolving threat to our cybersecurity, this failure to present a deterrence policy places our country at risk. And again, we're seeing that at all levels, in all places of the United States.

And, to Senator Nelson's point, we talked a lot about budgeting, but it's very difficult to budget when you don't know what the administration's policy is. When you talk about SOCOM-type activities versus other types of activities, we don't know, we don't have a policy.

And so, I would just ask, Mr. Secretary, is there something that we're not aware of that is stopping the President from providing this policy? Are there some hurdles that we need to overcome? What do we need to do to get that policy?

Mr. Rosenbach: Yes, ma'am. First of all, I'd just like to say I've met with the Iowa TAG several times to talk about cyber issues. Very smart guy. And I also -- my mom would kill me if I didn't say I spent my summers in Lake Okoboji, so I know about Iowa.

[Laughter.]

Mr. Rosenbach: But, that's -- yes, ma'am, but that's not to butter you up and to not admit that we're not late on the --

[Laughter.]

Mr. Rosenbach: -- the deterrence report that you mentioned.

The interagency and the White House has led an effort. That report is almost entirely finished. We've put a lot of thought into it. And, just because I'm in the Pentagon, I'm not able to say exactly when it would come to you. But, I want to emphasize that that's more of a report. The overall deterrence policy is something in -- a cyber operations policy that the National Security Council has put forward and does play into our thinking, in a large degree.

So, I wouldn't want anyone to think that there's not a lot of deep thinking about deterrence in the U.S. Government, but particularly in DOD.

Senator Ernst: Okay. Well, I appreciate that. And, yes, you did butter me up. Okoboji is lovely. So, you're welcome back anytime.

Yes, and General Orr is very intent on making sure that we have a very realistic exercise play, this upcoming year. And so, we are excited about this opportunity.

So, as we continue to develop the cyber deterrence policy, what are some of the challenges that you are facing right now? Senator Nelson has brought up a number of challenges that are out there, SOCOM versus other types of activities. What are those challenges? And do you see anything that we, as legislators, can assist you with in that aspect?

Mr. Rosenbach: Thank you, ma'am. I'll sort of answer quick and then let General McLaughlin say it.

The biggest challenge, quite frankly, when we think about deterrence, is making sure that we deter enough that the attack doesn't come, but we don't escalate things to the point that we bring more attacks upon ourselves. So, it's really important to remember that the U.S. is a glasshouse when it comes to cyber, and we need to be really careful how much we do things like think about going on offense, because

that almost inevitably will lead to more attacks on us. So, that's why we think about using other tools in the toolbox, like economic sanctions or other aspects of military show of force, from my perspective.

But, I think General McLaughlin has thoughts on this, too.

General McLaughlin: The key thing on the -- from the Cyber Command perspective, ma'am, on the deterrence piece, is really making sure we deliver the capabilities that are part of deterrence. It's defendable networks -- make sure that we get those networks fielded so that the adversary doesn't think he just has an easy target and doesn't tempt them to use their capability. Today, I think we are -- we could be an easy target, because we haven't fielded that defendable terrain. Getting our teams not only fielded, but, as was mentioned -- Mr. Rosenbach mentioned things like the unified platform or Title 10 tools and infrastructure -- we think of those sort of as enablers.

And so, we need to get the enablers crisply defined and fielded so that you have people plus the capability, whether you consider them the weapons or the infrastructure. It's the kit that our teams -- that these component commanders behind me, that their teams need to actually be able to have a robust capability. I think, from -- on the deterrence piece, that's what we really bring to the table at Cyber

Command, will be the military forces that can be an element of deterrence, certainly not the -- certainly not everything that's required to deter.

Senator Ernst: Thank you. My time is expired.

Thank you, General. Thank you, Secretary.

Thank you, Madam Chair.

Senator Fischer: Thank you, Senator.

And Senator Tillis.

Senator Tillis: Thank you, Madam Chair.

Thank you, gentlemen, for being here today.

One quick question is, How does any of the funding you receive -- how is it threatened by sequestration?

Mr. Rosenbach: Sir, I'm going to give you one specific example and then turn to General McLaughlin so he can give you more detail.

During sequestration in the past, it put a big hole in the training pipeline for these Cyber Mission Forces. And what we saw is, because we had to turn off schoolhouses, there was as big impact on the rate of development for the overall Cyber Mission Force. And it really has hurt us in a way that makes me nervous. And, if that were to happen again, we'd be even further behind in developing the capability --

Senator Tillis: And, Secretary --

Mr. Rosenbach: -- the capabilities like that.

Senator Tillis: Mr. Secretary, that, as the human capital you need to execute the mission, can you give me a rough idea, in terms of a percentage of the pipeline that you would have liked to have had versus was affected by sequestration -- a rough idea of what that is?

Mr. Rosenbach: I think, honestly, General McLaughlin can give you more details on that, and even more on the impact.

Senator Tillis: Okay.

General McLaughlin: So, sir, we're roughly 50 percent through the fielding of those 133 teams, and we are -- we're supposed to have all of them at initial capability by the end of fiscal year '16. So, we literally have a quarter of the additional teams that are in the build just for -- in this, in the next fiscal year. So, sequestration will make -- will put a big dent on the ability of the services to produce the people that we need to fill out those teams.

Senator Tillis: What about the -- some of the longer-term investments that you have to make while we're in this budget mode of living paycheck to paycheck? What sorts of long-term strategic investments are out there that you would like to make that are impossible to make on 12-month investment horizons?

Mr. Rosenbach: Sir, Secretary Carter recently has emphasized that sequestration is one of those things where

it's actually a waste of money, for the reason that you note, is, we're not able to do long-term planning, so you make poor investment decisions based on a shorter time horizon.

For some of the big rocks, as CYBERCOM calls them -- so, the persistent training environment, a unified platform -- those are things that are a more significant investment that we think much harder about whether or not we would allocate resources to when we're unsure of how much will actually be there.

Senator Tillis: You all were mentioning that your top priority is the 2 percent of, I think, DOD or defense-related cyber attacks that you see. Is that -- did I hear that correctly?

Mr. Rosenbach: Yes, sir. It's not exactly 2 percent. Only to show -- for the biggest threats to the Nation are the ones in that defend-the-Nation mission that we try to prevent or deter.

Senator Tillis: What about the sort of macro threat? If I were -- I worked in the private sector and did ethical hack testing and tried to find ways to penetrate businesses -- large businesses and -- you know, if I were on the cyber battlefield, I wouldn't necessarily go after the ones where I know it's going to hurt most if I get caught. To lead up to your capacity to do that, I'd go after the downstream

supplier base for DOD. I'd go after municipalities and government institutions to disrupt a broader population so that you have a whole lot of things that you have to look at before I would get to a level -- I mean, are we looking at threats in that way? And do we have resources marshaled in that way? Because that transcends into the private sector and the U.S. Government supply base, which is large and diverse.

Mr. Rosenbach: Yes, sir, that's a great question. There are two ways, in particular, that we've been watching this as it relates to DOD. So, the first is, we know that a lot of the defense contractors have been penetrated and intellectual property pulled out. And so, we're trying to use new contracting mechanisms. And the SASC has been very helpful in this in passing some aspects of the law to make it better so that the private sector has sort of upped their game. Then, second, TRANSCOM, we've seen, has been penetrated by some adversaries -- the Chinese, in particular -- who know that, by going to the supply chain, they may be able to hit us at a weaker point than going directly there. And that's something that SASC also did some reports on that were helpful. So, those are the two ways.

And then, in the more general private sector, it's an even more difficult situation, because it's a significant investment for a lot of the private-sector firms.

Senator Tillis: I don't think I'll get to this question, but I would like to speak with you all at some point about, How do we look at the underlying infrastructure through which all these cyber attacks occur? And are we looking at ways to, maybe, look ahead to an architecture that makes it still maintain the privacy considerations, but find better techniques or a better underlying infrastructure for authentication so that it puts you in a better position to defend and potentially attack?

But, I had a final question that has more to do with -- I love what the Commandant of the Marine Corps said at a SASC meeting a couple of months ago. He says he never wants to put an American soldier in a position to where he or she is going into a fair fight. And I think, for most of our men and women in uniform, we've got the strategies to do that. But, it seems to me that, in this realm, we have adversaries out there that, on any given day, although our sophistication may be slightly better, there are certain battlefields where it could just be a fair fight and we could get -- we could be harmed as much as we could do harm. Is that a fair assessment?

Mr. Rosenbach: Sir, I think it's a fair assessment, just given the asynchronous, asymmetric nature of cyber. And General McLaughlin probably has some thoughts on that, too.

General McLaughlin: Well, I think, because of the diverse nature of the threats against us, including threats that operate in ways that we wouldn't operate as a Nation -- it's just not in our character -- I do think you could see the potential where it might not look -- where it might look like it's a fair fight, you know, at least today. And so, I think our goal is -- at least within the DOD side -- is to make it where it's not fair, you know, to bring these capabilities to bear that we're -- that we've been discussing, so that our military forces, in particular, don't have to go into conflict, in the future, thinking about this is going to have be a fair fight.

Senator Tillis: Thank you.

Senator Fischer: Thank you, Senator Tillis.

Senator Gillibrand, I know you just arrived. Would you -- are you ready for your questions? Okay, thank you.

Senator Gillibrand: Thank you, gentlemen, for being here. Appreciate your service and your hard work.

CYBERCOM obviously has a wide array of responsibilities. How do you deal with unexpected threats? And do you have the capabilities to meet those threats? And, in the event of a cyber attack, would you need an additional surge capacity?

General McLaughlin: Ma'am, I think the ability to deal with unexpected threats, and then surge them, requires a --

some attributes that I think that we are building. First is the ability to be flexible, to be able to move resources from one set of challenges to another. We've seen the need for that, just in the recent 12 months. You know, we've seen things, like the Sony attack, we've seen resurgent issues with regard to Russia. So, we've seen issues where our Department has made, including the cyber, adjustments in priority. So, being flexible and agile to respond to things that perhaps you weren't forecasting is something that's built into our model.

But, you raise a great point on the ability to surge. So, we are building a set of forces -- we've talked a little bit about them today -- 133 cyber teams that are going to be the basic capacity and capability for our military forces in Cyber. What we've also added, though, are forces in the total force. So, all the services have constructs for their Reserve forces. And the Army and the Air Force have -- with their Guard forces, are actually going to be brought online and actually provide capacity for the Nation if they needed to be called up. You could surge and bring even more military capacity with the total force. That is part of our construct. It's just really been defined in about the last 12 months, and now both the Reserves and the Guard are building their teams, certified to the same standards that the Active Duty teams will have. And that will be

additional resource if there was a surprise or a need to surge resources to an emergency.

Senator Gillibrand: And what's your vision, with regard to Guard and Reserve components, for CYBERCOM?

General McLaughlin: Our vision, from the Cyber Command perspective, was very clear. We wanted to make sure that all Reserve and Guard forces were able to be trained to the same standard so that, if they were called up to do the Title 10 -- you know, to support in a Title 10 status -- they would be equal and capable.

Senator Gillibrand: So, you're envisioning equivalent training.

General McLaughlin: Yes, ma'am.

Senator Gillibrand: Okay.

General McLaughlin: Absolutely. And that they would be able to also be commanded and controlled in a seamless, the same way that the Active Duty forces would -- you know, would be commanded and controlled.

So, that's the -- that's really the -- from the Cyber Command perspective, what we laid out. Each of the services has taken a slightly different way that they've -- that they are thinking about integrating Reserve and Guard forces into their structure. They all fit within our construct at Cyber Command. And I know each of the -- those component commanders in the second panel would be glad to talk to you

about specifically what's unique about each service, in terms of how they think about their --

Senator Gillibrand: And will that change after fiscal year '16? Would you still be able to -- the people assigned to CYBERCOM would still be able to receive the same training?

General McLaughlin: Yes, ma'am. Our plan is that this -- that's the steady-state --

Senator Gillibrand: Okay.

General McLaughlin: -- mode that we would like to be in.

Senator Gillibrand: And then, representing New York, obviously, we have a lot of emerging threats to our infrastructure, to our financial markets, and to basic national security. And I've met with a lot of the experts in the field there. What are your thoughts on the relationship and the coordination between Homeland Security and DOD, in terms of cybersecurity and role responsibilities? And, more to the point, do you see -- what do you see as the Department of Defense's role in the support of States, DHS, and the FBI?

Mr. Rosenbach: I'll take that one, ma'am.

I think -- it's been interesting for me, because I've been in the Department for almost 4 years now, working on cyber issues. And when I first came, there was a lot of

tension between DOD and DHS, and a little struggle about who would have the lead. It's completely different now. The relationship is very strong. We know that DHS/FBI have the lead for domestic issues. We then will come in behind them and support them, very often. You could ask General McLaughlin, if you want, for example, about the support that DOD and NSA gave during the Sony cyber attacks in a domestic way.

And then, the relationships between the State and local governments usually is through DHS, just like defense support for civil authorities. In all ways, we need a lead Federal agency, and then we can provide support to them or to the States.

Senator Gillibrand: Now, if you are doing this level coordination and training, do you have the resources and support you need to do those missions?

Mr. Rosenbach: Ma'am, you know, the -- because the cyber threat is growing so much, we see that we'll need more resources down the line, and the Department has prioritized Cyber as one of those that will continue to get additional resources.

Senator Gillibrand: Do you need any additional authorities?

Mr. Rosenbach: Right now, there are none that we think we need, but we've always worked real closely with the

Senate Armed Services Committee in the past. And I'm sure, if we identified those, that we would -- we would welcome your support.

Senator Gillibrand: In the issue of recruitment, we've just received a report from all services articulating their plans either to create separate specialties or designators for cyber. It's my understanding that the training necessary to build a cyber warrior can take up to 2 years. How do you envision the development, not only of separate specialties for cyber, but also career tracks for cyber warriors? How do we retain them and get a return on the investment the United States has put into these warriors?

Mr. Rosenbach: I'll let General McLaughlin speak in more detail, but I know that's something you've worked a lot on in the past, and been helpful in getting new authority for us. That has been very good. So, I would like to thank you for that, explicitly, and then let General McLaughlin talk more about the details of the training.

General McLaughlin: Sure. Senator, the -- each -- as you mentioned, each service is thinking through what type of specialties and career tracks it needs in the cyber warfare domain. They've all taken slightly different paths, but each of them are -- have come up with a path so that you can now come in as a new entry or accession, and you can conceive a career in this area. It's not something you

would dabble in or come in and out of.

Senator Gillibrand: That's great.

General McLaughlin: And so, from our perspective, it's not only important that they've done that so that our initial people, as they come in, are qualified, but we actually need, you know, mid-level and senior, you know, people that have deep experience in this. So, the -- so, their work to build the career path is critical for us, and it's something we're watching. We've really just sort of laid out the requirement, and each of the services, you know, strapped on and has, I think, again, taken a slightly different path, but each of them, at the end of the day, are going to have people with that type of -- that depth over a career.

Senator Gillibrand: Thank you.

General McLaughlin: The last thing, you mentioned about just -- I would just add -- keeping them in. So, retention will be a big deal.

Senator Gillibrand: Yup.

General McLaughlin: If you're going to invest 2 years training someone on a set of very, very high-end skills that actually are marketable in the civilian workplace, our job will be to retain them. It's not only to show that they have a valid career, but also if there are incentives or other things that might help offset, you know, the fact that

they could make more elsewhere, you'll see us -- where each of the services is looking at that.

And then also flexible models. You know, how can we be flexible in the workforce of the 21st century to let people, you know, feel like they -- perhaps we could bring in people from the private sector, or we could do other things, not just use the same model we've always used in the Department.

Senator Gillibrand: Thank you.

Senator Fischer: Thank you, Senator.

We will have a 4-minute round for the second round, here, so we can have our second panel up and still get down to the classified briefing. Senator Nelson would like to meet down there yet today.

So, I'm just going to ask a couple of quick questions, here, Mr. Secretary. One on deterrence again, and then on acquisition, if I can.

When we look at the sanctions that were recently authorized by the President and against the cyber attackers, how do you see that contributing towards better deterrence in cyberspace? And specifically, when you look at the other agencies, when you look at State and you look at Treasury and you look at Justice, are the agencies working together? And how's the Department working with him on that?

Mr. Rosenbach: Thank you, ma'am. In the case of the Sony attacks, on the sanctions that went against the DPRK,

we, as an interagency, looked very, very closely at the organizations we could target with those sanctions that would inflict the most cost on them. So, remember what I talked about, the cost-benefit relationship for deterrence; that's why. So, that, of course, was led by Treasury and other experts in the interagency, but we had as much a voice in that as anyone. And I do think that's something that was effective and has impacted the decision calculus of the North Koreans.

Senator Fischer: When we have a show of force in other domains, that can have a stabilizing effect, I believe, on a situation that may be deteriorating out there. How important do you think it is that we be able to do that within the cyber realm?

Mr. Rosenbach: Ma'am, I think, honestly, most countries around the world know that we have capability in cyber and could demonstrate that force. I personally don't think that it would be wise to demonstrate it unless we really needed to, because I'm very worried about how vulnerable we are and that someone would then follow our example and just try to show the U.S. that they could also take down part of the infrastructure to demonstrate that. So, I think a cautious approach, where we're conservative and we try to keep things stable, is quite important.

Senator Fischer: A lot of times, we hear that cyber is

similar -- the -- a cyber deterrence is similar to nuclear deterrence. Many people believe that. I question it in many regards. Feel free to correct me on that, but how do you see it?

Mr. Rosenbach: Without sounding too, maybe, cheeky, I'd say most of the people I hear who say that tend to be from the Cold War era and think that things are very analogous, when, in fact, I don't think they are at all. And I agree with you that the analogy with the nuclear part is not that strong.

Senator Fischer: I was able to spend some time back in Nebraska, the last 2 weeks, and I spent a day out at STRATCOM and had some briefings on cyber. So, it -- it's fascinating what's out there. I appreciate the work you do on that.

With acquisition now. When we look at the latest addition of the better buying power list, cyber security -- they're listing that as a new area of emphasis, and they want to elevate that in the acquisition process. What input do you have on that release from Secretary Kendall? How do you see that shaping up?

Mr. Rosenbach: Yes, ma'am. I work very closely with Under Secretary Kendall. Almost every day, we're in touch. And in my role as the Principal Cyber Advisor, I'm kind of the point guard or the quarterback for things on cyber

inside the Department. And so, of course, he's the lead on that. But, it was something that was coordinated even with the services. And we want to, you know, just strengthen our ability to make some of the defense contractors up their game a little bit in cyber security.

Senator Fischer: And when you look at the acquisition process, I mean it takes forever, right? So, when you're looking at cyber and you're looking at technology, how are you going to speed that up in order to, I mean, truly meet the needs that are there before what you're trying to acquire becomes out of date in 18 months and you haven't even gotten through the process?

Mr. Rosenbach: That's a great question. And I assure you, Secretary Carter's interest in accomplishing exactly that is very passionate, and he's put a lot of pressure on everyone in the Department to do better. Next week, he is going to Silicon Valley and will give a speech. That's one of the topics that he's going to address to try to push us to do better in that area and build more bridges with the private sector. Silicon Valley, just one example.

Senator Fischer: Great. Thank you.

Senator Gillibrand.

Senator Gillibrand: Can you just describe -- it came up in the last hearing, that we're going to be doing some recruiting for Guard and Reserve in Silicon Valley -- can

you describe what that program's going to look like?

Mr. Rosenbach: Ma'am, I can't give too many details, because I don't want to unveil the gift before it comes next week in the speech, but we've been thinking a lot about ways we can get new pipelines or tunnels of talent into the Department from kind of nontraditional places. So, the Guard is another place where, in going and traveling and visiting some of the Guard units, I've recognized there really are people who, for example, work for Microsoft and still work in the Guard in Washington State. That's just one way, but we would also like to try to find other ways in the Department where you don't have to go into one of the services, for example. So, we're thinking a lot about that. Silicon Valley is a natural place. New York and around New York City, another place. There are a couple of places like that, where we're looking at centers of excellence.

Senator Gillibrand: So, once it's public, can you send me a letter describing the program?

Mr. Rosenbach: Yes, ma'am, I will absolutely do that. I promise I'm not trying to be evasive. I'm just trying to --

Senator Gillibrand: No, I know. I just -- I'm interested, so I want to know.

Mr. Rosenbach: I will. We'll send you the full report. And I can brief your staff --

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Gillibrand: To the extent you need any support for that program in this NDAA, let me know and we will write it.

Mr. Rosenbach: Great. Thank you.

Senator Gillibrand: So, any substantive language needs to be added about authorities or funding, this year's NDAA would be the appropriate place to try to put that in.

Mr. Rosenbach: Yes, ma'am, thank you.

Senator Gillibrand: Continuing on, on the issue of sort of the dynamic threat environment, how do you address the fact there's continually morphing requirements and distinct threats that face both the DOD and the U.S. as a whole? How do you plan for it? How do you model for it? How do you stay ahead of it?

Mr. Rosenbach: I'll say, very generally, and then I'd like General McLaughlin's thoughts, is, we try to build a very capable force that is dynamic enough that it can shift. And, with that, I think he can give you the best answer.

General McLaughlin: Yes, ma'am. I think if we spend our time trying to predict exactly what the threat is going to be or how it will manifest itself, we'll end up guessing wrong. So, our job is to field forces that both technically are trained at a very high level, you know, they have a lot of technical skills, and they've been given a flexible set of capabilities so that -- and that we have great

intelligence -- you know, we'll need great intelligence capabilities, as well -- so that, if something occurs, and it will, that we didn't forecast, we don't have to retool our force, you know, create new capabilities. We actually can take the people and the capabilities we've fielded and rapidly put them against some new or emerging threat.

Senator Gillibrand: And I assume you're also training for offensive acts.

General McLaughlin: Yes, ma'am. I would mean that for both our defensive and our offensive teams.

Senator Gillibrand: And you probably need to answer this in the closed setting, but can you describe a little bit where you feel the threats are, whether they're lone-wolf threats or they're state-actor-driven threats, or if it's really a balance of both? If you need to reserve that for closed setting, you can.

General McLaughlin: Yes, ma'am. I think to address it in depth, it would be better in closed hearing, but I will tell you they span the range from the nation-state-level threats to -- you know, to the lone wolf or --

Senator Gillibrand: But, do you see either one more of a growing threat or more of a risk?

General McLaughlin: I think they're all threats, but I would say the place to bring the most capacity are nation-state-level threats.

Senator Gillibrand: State actors, yeah.

General McLaughlin: Yes, ma'am.

Senator Gillibrand: Thank you.

Thank you, Madam Chairwoman.

Senator Fischer: Thank you, Senator.

Thank you, gentlemen. Hopefully, a little after 4:00, we'll meet you down in the SCIF for a classified session. Thank you so much.

And, with that, I would ask that panel two step forward, please. And I apologize, to you folks, that we have a brief time for your presentation.

On our second panel, we have Lieutenant General Cardon, who is the Commander, U.S. Army Cyber Command; Vice Admiral Tighe, Commander, U.S. Fleet Cyber Command; Major General Wilson, Commander, Air Forces Cyber; and Major General Daniel O'Donohue, Commanding General of the U.S. Marine Corps Forces Cyberspace.

So, welcome, gentlemen. I would --

And, I'm sorry, ma'am. It's so good to see you.

Welcome, to all of you. And I would ask that, if you would have very brief opening remarks, Senator Gillibrand and I, then, will ask questions and give you an opportunity to respond to those.

So, Major General O'Donohue, would you like to begin, please?

STATEMENT OF MAJOR GENERAL DANIEL J. O'DONOHUE, USMC, COMMANDING GENERAL, U.S. MARINE CORPS FORCES CYBERSPACE

General O'Donohue: Madam Chairwoman, it's an honor to appear before you today on behalf of your marines and their families. Thank you for continued support to our growing cyber capability.

During this dynamic period of transition, it's especially important that we receive budget capability on time, as well as flexible support for still developing manpower, acquisition, and training initiatives.

As a component of U.S. Cyber Command and in full partnership with our sister services and agencies, Marine Force Cyber is ready to conduct full-spectrum cyberspace operations. Specifically, we provide the joint force specialized cyber teams in a dedicated joint force headquarters. In our component role, our worldwide cyberspace operations are primarily in support of SOCOM. This reinforces a broader relationship, in keeping with the Marine Corps' role as a global crisis-response expeditionary force and readiness. In our service role, the Commandant set a clear priority to fully integrate cyberspace operations into the already multi-domain approach for our marine air/ground task forces and naval expeditionary forces. This involves a reset of our networks based on operational principles and innovative manpower model or

challenging readiness standards and a supporting IT strategy that includes operationally responsive acquisitions. Commanders at every level seek competitive advantage in air, land, sea, and cyberspace, with a combined-arms approach, in concert with maneuver, intel, command and control, kinetic and nonkinetic fires. Commanders should be able to contain and defeat adversaries in cyberspace while simultaneously operating across all other domains with potentially degraded but still resilient command and control.

To that end, we are fielding the cyber forces required by our strategy -- ready, on time, and with increasing interoperability -- in ways we have not imagined. Even before units are fully manned, trained, and equipped, we are achieving operational outcomes as these teams support current operations in stride with their fielding.

We defend against advance threats through active deterrence, hardening of our networks, realistic training, and exercises in high-fidelity cyber ranges. Every marine is increasingly trained as a disciplined and opportunistic cyber warrior.

Currently, we are pursuing a joint service strategy for the multiyear development of a unified network that will facilitate command and control, provide real-time situational awareness, and assist with decision support for commanders. Our network will be optimized for operational

support to forces as they deploy globally in an unstable and unpredictable security environment. The marines provide a ready, forward expeditionary extension of cyber capability for the joint interagency and combined force.

Thank you for the opportunity to appear before you today and the continued support for your dedicated marines. I look forward to answering your questions.

[The prepared statement of General O'Donohue follows:]

Senator Fischer: Thank you, sir.

General Wilson.

STATEMENT OF MAJOR GENERAL BURKE E. WILSON, USAF, COMMANDER, 24TH AIR FORCE, COMMANDER, AIR FORCES CYBER

General Wilson: Madam Chair Fischer and the distinguished members of the panel -- of the subcommittee, thank you for the opportunity to appear before you today alongside my component commanders. It's an honor to represent the outstanding men and women of 24th Air Force and Air Forces Cyber.

I'm extremely proud of the work our airmen, officers, enlisted, and civilians do every day to field and employ cyber capabilities in support of combat and Air Force commanders.

In the interest of time, let me just share a few examples to highlight how our airmen are making positive, lasting impacts to our Nation.

Last year, the Air Force completed the migration of our unclassified networks from many disparate systems into a single architecture. We transitioned 644,000 users over -- across 250 geographic locations to a single network, and reduced over 100 Internet access points to a more streamlined 16 gateways. The end result is a more reliable, affordable, and, most importantly, defensible network, which has been a significant step forward for the Air Force.

The Air Force also championed the fielding of the next generation of technology, known as the Joint Information

Environment, by partnering with the Army in the Defense Information Systems Agency. Together, we are implementing joint regional security stacks in modernizing our networks in order to achieve a single DOD architecture. The combined team achieved a critical milestone last fall, when we fielded the first security stack down at Lackland Air Force Base, in Texas. We fielded several more, and continue to push hard. These efforts will benefit the entire Department by reducing our network attack surface and increasing network capacity and capability. We see this as a very significant step.

Like the other services, we have made significant progress towards fielding and employing our initial Cyber Mission Forces. Today, the Air Force has 15 teams that have achieved initial operating capability, and two teams have achieved and have reached full operating capability. In addition to providing unprecedented support to joint and coalition combat forces in Afghanistan and Syria, these cyber forces are engaged in support to combatant commanders and Air Force commanders around the world, as well as defense of the Nation.

I'm proud to report our Air Reserve component is a full partner in the Cyber Mission Force build in addition to our other day-to-day cyber operations. We've leveraged traditional reservists, Air Reserve technicians and Air

National Guardsmen across the Command to meet our warfighting commitments. Whether it's providing command and control of our cyber forces from one of our operation centers, deploying as part of our combat communications team, installing cyber infrastructure around the world, or any other task, each of our total-force airmen meet the same demanding standards and serve alongside their Active Duty counterparts. In my humble opinion, it's a tremendous example of the total-force integration at work.

Today, the Air Force also -- we've instituted several key initiatives to better recruit, develop, and retain our cyber forces. Most recently, we approved a Strikes for Certifications Program, which provides the opportunity for candidates to enlist at a higher grade when entering the Air Force with described -- or the desired cyber-related certifications. We've also continued our selective reenlistment bonus program to provide additional incentives for enlisted members to continue to serve in the demanding cyber and intelligence specialties. For our officers, we have complemented the cyberspace warfare operations career track, which we established several years ago, with our new Cyber Intermediate Leadership Program, which we believe has been key. Our first board competitively selected 83 majors and senior captains to serve in command and operational positions, many as members of the Cyber Mission Force.

And finally, we continue to host a number of initiatives aimed at improving the outreach to our Nation's younger generation. I'd like to highlight just one, if I could, please. It's called Cyber Patriot. And it's sponsored by the Air Force Association, in partnership with local high schools and middle schools around the country, several industry partners, as well as cyber professionals from the Air Force. Cyber Patriot's goal is to inspire students to pursue careers in cyber security or other STEM career fields. In September, we had over 2100 teams, involving nearly 10,000 students in the United States, Canada, United Kingdom, and our DOD schools around the world. They all began participating in cyber training and competitions. We saw a 40-percent increase in participation, this school year. Cyber Patriot culminated here locally at the National Harbor last month, when 28 teams competed in national finals. Students earned national recognition and scholarships. And, without a doubt, the program is an example of how public/private partnerships can make a real difference. Personally, it's been a rewarding -- very rewarding to see our airmen giving back to our younger generation.

These are just a handful of examples of how Air Forces Cyber and 24th Air Force are all-in and fully committed to the mission. Our cyber force is more capable than ever

before. We continue to have challenges, but we get better every day.

None of this would be possible without your continued support. It's clear resource stability in the years ahead will be vital to our continued success in developing airmen and maturing our capabilities to operate in, through, and from the cyberspace domain. Simply put, our cyber warriors are professionals in every sense of the word, and they deserve our full support.

Along with my fellow commanders, it's an honor to be here today. Thank you again for the opportunity, and I look forward to your questions.

[The prepared statement of General Wilson follows:]

Senator Fischer: Thank you, sir.

Vice Admiral Tighe.

STATEMENT OF VICE ADMIRAL JAN E. TIGHE, USN, COMMANDER, U.S. FLEET CYBER COMMAND, COMMANDER, U.S. 10TH FLEET

Admiral Tighe: Thank you. Madam Chairwoman Fischer and distinguished members of the subcommittee, thank you for your support to our military and for inviting me to appear before you today. I appreciate the opportunity to share with you the Navy's operational view of cyberspace in addition to our initiatives to improve both our cybersecurity posture and operational capabilities as part of the joint cyberspace team in order to address this ever-increasing threat to our Nation and our allies.

Fleet Cyber Command directs the operations to secure, operate, and defend Navy networks within the Department of Defense information network. We operate the Navy network as a warfighting platform which must be aggressively defended from intrusion, exploitation, and attack so that it is both available and trusted for all maritime missions that the Navy is expected to carry out. The Navy network consists of more than 500,000 end-user devices, approximately 75,000 network devices, and nearly 45,000 applications and systems across three security enclaves.

We've transformed the way we operate and defend this network over the past 2 years based on operational lessons learned. Specifically, beginning in summer of 2013, the

Navy fought through an adversary intrusion into our largest unclassified network. Under a named operation, known as Operation Rolling Tide, Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy commanders, U.S. Cyber Command, the National Security Agency, Defense Information Systems Agency, and our fellow service cyber component commanders.

Although an intrusion upon our networks is always troubling, this operation served as a learning opportunity and has matured the way that we operate and defend our networks and simultaneously highlighted our gaps in cybersecurity posture and weaknesses in our defensive operational capabilities. As a result of this operation and other cybersecurity initiatives inside of the Navy, we have already made, proposed, or planned for a nearly $1 billion investment that greatly reduces the risk of successful cyberspace operations against Navy networks. Of course, these investments are built on the premise that our future real budgets will not be drastically reduced by sequestration.

Specifically, if budget uncertainty continues, we will have an increasingly difficult time addressing this very real and present danger to our national security and maritime warfighting capability.

Operationally on a 24-by-7 and 365-day-a-year basis,

Fleet Cyber Command is focused on configuring and operating layered defense and depth capabilities to prevent malicious actors from gaining access to Navy networks, in collaboration and cooperation with our sister services, U.S. Cyber Command, Joint Force Headquarters, DoDIN, DISA, and the National Security Agency. Additionally, we're driving towards expanded cyberspace situational awareness to inform our network maneuvers and reduce our risk. As you know, the Navy and other service components are building the maneuver elements in the Cyber Mission Force for U.S. Cyber Command by manning, training, and certifying teams to the U.S. Cyber Command standards. Navy is currently on track to have personnel for all 40 Navy-sourced Cyber Mission Force teams in 2016, with full operational capability the following year. Additionally, between now and 2018, 298 Cyber Reserve billets will also augment the cyber force manning plan.

In delivering on both U.S. Cyber Command's and the U.S. Navy requirements in cyberspace, I am fortunate to have fantastic partners, like these component commanders, in addition to many other partner organizations across the Navy, Department of Defense, U.S. Government, academia, industry, and our allies who are every bit a member of our team cyber and critical to our collective capability.

Thank you again, and I look forward to your questions.

[The prepared statement of Admiral Tighe follows:]

Senator Fischer: Thank you, Admiral.

General Cardon.

STATEMENT OF LIEUTENANT GENERAL EDWARD C. CARDON, USA, COMMANDER, U.S. ARMY CYBER COMMAND

General Cardon: Madam Chairwoman Fischer, members of the subcommittee, it's an honor to be here on behalf of Army Cyber Command and 2nd Army alongside my fellow joint commanders. I appreciate the work of this committee to protect the American people from emerging threats and to ensure our military has the capabilities needed to defend the Nation.

The Army's gained tremendous momentum, both with institution and operationalizing cyberspace, but much work remains. For the institution, we've created the Cyber Center of Excellence at Fort Gordon, Georgia, and Army Cyber Institute, at the United States Military Academy. In addition, the Army is establishing the necessary service frameworks for building cyber capabilities for the Army and, by extension, the joint force.

Operationally, we've made progress supporting both the Army and combatant commands. With respect to the Cyber Mission Force, we have 25 of the 41 teams on mission now, and expect to have all 41 teams on mission by the end of fiscal year '16, as planned. However, we're employing these teams as they reach initial operating capability. The threat, vulnerabilities, and mission set demand this sense of urgency. We're also building a total Army force to

include 21 additional Army Reserve and Army National Guard cyber protection teams.

We're going to need more people, beyond what is required for the Cyber Mission Force, to build out the support required to fully employ the Cyber Mission Force and to build cyber capabilities for all Army formations. To better manage our people, the Army created a Cyber Branch 17, and we're exploring the creation of a cyber career field for our civilian personnel. For training, we have essentially funded Joint Model for Individual Training. We're working to build the collective training capabilities and associated facilities within a joint construct. For equipping the forces, we're developing and refining the necessary framework to give us the agility needed in programming, resourcing, and acquisition for the infrastructure, platforms, and tools. For more defensible architecture and network, we're partnered with the Army Chief Information Officer, Defense Information Systems Agency, and the Air Force for an extensive network modernization effort. These are critical to the joint information environment and to the security, operation, and defense of our networks.

Our budget priorities include fielding the Cyber Mission Forces, growing our joint force headquarters cyber, developing a skilled cyber workforce, highlighting

capabilities for that Cyber Mission Force, and restationing our headquarters. The Army's FY16 requested cyberspace operations budget is $1.02 billion, and that includes $90 million for our Fort Gordon operational headquarters facility. We've made tremendous progress. With your support, we'll have the necessary program resources to continue this momentum. We cannot delay, for the struggle is on us now.

Thank you, and I'm happy to answer your questions.

[The prepared statement of General Cardon follows:]

Senator Fischer: Thank you, sir.

Thank you all for your service to this country, and thank you for being here today to answer our questions and provide us with some good information.

Admiral Tighe and General Wilson, I know that, both the Navy and the Air Force, you've established task forces to review weapon systems for vulnerabilities. And, as we're looking at those systems, I know that you want to ensure that they haven't been compromised, and also that they are configured to resist a cyber attack in the future. Can you tell us how you're prioritizing those reviews? And when do you expect to have those high-priority systems assessed?

Admiral Tighe: Yes, Madam Chairman, I'll take the first shot.

From the Navy perspective, my command has been operationally involved in demonstrations to help us assess how at risk that the Navy missions may be. Beyond the responsibilities we have for our corporate networks, for our communications, for our C4ISR capabilities, we know that there are potential risks that exist inside of our weapon systems and inside of our control systems in our platforms. And so, our demonstration has helped to inform Navy investment decision-making from a Task Force Cyber Awakening, is the organization that was stood up by the CNO and by the Assistant Secretary of the Navy for Research,

Development, and Acquisition, to take a holistic view across all of the Navy investment portfolios, all of the Navy system commands and programs so that we are accounting for cyber security in the most holistic way in all of those programs.

Senator Fischer: So, you're looking to see if anything's been corrupted within an existing system?

Admiral Tighe: We're looking to make sure that cyber security is accounted for in every program that we are -- you know, at developing and delivering to the Navy, every capability that may depend upon an operating system or something related to network in that regard. And so, Task Force Cyber Awakening has broken into three different subgroups to look -- organizationally, do we have the right authorities to, again, go beyond the authorities that we execute, you know, in behalf -- on behalf of cyber and communication systems and our networks, go into control systems, go into operating systems.

And, as it pertains to dealing with any vulnerabilities that may exist there, what is the right resource investment strategy to mitigate the risk that exists today, especially on our ships that we will have with us for many years to come? How will we mitigate any risk that may exist there? And how will we build the types of teams that we are building, aimed at communications and networks, for those

types of systems, which are different skills, different tool sets, when you get into the realm of the combat systems and the --

Senator Fischer: Right.

Admiral Tighe: -- and the control systems. And so, that's what --

Senator Fischer: When do you expect that to be assessed, then?

Admiral Tighe: We're expecting the Task Force Cyber Awakening to --

Senator Fischer: I know the Navy's further along.

Admiral Tighe: We are. It started in September. We are trying to get to completion on Task Force Cyber Awakening by this summer. But, there will be enduring resource investments, organizational changes, and potentially additional processes put in place, much like the SUBSAFE Program took on making sure water doesn't get into our submarines, thinking in terms of CYBERSAFE for our systems that go beyond the things that we are protecting and defending today.

So, by the summer, we should have a good feel for what are our next steps, whether we will be, you know, totally complete at that point. there's -- there may be more work to be done, certainly more investment to be made, in terms of mitigating the risks that we are carrying.

Senator Fischer: Okay. I just have a half-minute left.

Admiral Tighe: Sorry.

Senator Fischer: If I could have the other gentlemen -- what's happening with the Air Force, and then the Marines and the Army, as well, on this?

General Wilson: Absolutely, ma'am. So, we --

Senator Fischer: You have, like, a half -- three of you, half-minute.

[Laughter.]

General Wilson: Ours is called Cyber Secure Task Force. The Chief and the Secretary just approved that, then it kicked off about a month ago -- 4 to 6 weeks ago. They've given us 12 months. It's a whole-of-Air-Force-effort initiative to look across programs, networks, as well as installations. It's focused on our core missions -- air superiority, space superiority, global strike, command and control, et cetera. I think we've done a nice job in the network side, with some of the Cyber Mission Force standing up. There's a recognition that we may be vulnerable in our program of record. And so, that's really the focus. I mean, we're involved from the 24th Air Force perspective, but it's really a whole-of-service -- CIO, program offices, PEOs, et cetera.

Senator Fischer: Okay. Thank you.

General O'Donohue: The Marines are tracking with the Navy. We're part of Task Force Cyber Awakening. We have programs that we share with the other services. We'll work with them as we go, comprehensively. And then, lastly, we're working with our acquisition community to get this at the root requirement as we get new systems coming in.

Senator Fischer: Thank you, sir.

General.

General Cardon: And, ma'am, the Army, same as the others, specifically for the programs of record, given the scale of the Army's equipment, going forward, making cyber security a key performance parameter on all contracts, and then to work backwards, and then -- over time. And then, finally, I would say this is a competitive space, so we're never really going to be done in this space. This is going to have to be something that we just constantly assess on a regular basis --

Senator Fischer: General, have you budgeted for that?

General O'Donohue: It's not inside my budget. It's -- would be inside the acquisition budgets. The Army's been having a -- quite a debate about how much do we really fix, against which threats? And General Williamson and I are were -- are working together on that, both of them.

Senator Fischer: Thank you, sir.

Senator Gillibrand.

Senator Gillibrand: Thank you, Madam Chairwoman.

I appreciate all your presentations. And I was very excited to hear about a lot of the work you're doing to get the best cyber warriors you can. I think it's very exciting.

So, I want to look a little bit into the issue of the Reserve component, which you all mentioned, how you're addressing it. My understanding for the Air Force, that they plan to staff its Cyber Command requirements, in part, from the National Guard units. With regard to Army, do you also intend to staff part from National Guard units for your CYBERCOM requirements? And, if not, how do you plan to use the Reserve components, specifically?

General Cardon: So, ma'am, we have, in the Army National Guard, 1,035. They work in Cyber Command, in DISA, in my own headquarters, in the Joint Force Headquarters. And, of that, there are 11 Cyber Protection Teams. And one of those is on Active Duty now, up in Maryland.

Senator Gillibrand: And how do you do their training? Do they get a different kind of training or the same kind of training?

General Cardon: We're still -- we just started growing. The one we have, we've received -- 17 have received equivalency training, thus far.

Senator Gillibrand: Oh, that's good.

General Cardon: So, they have to --

Senator Gillibrand: Seventeen individuals?

General Cardon: Correct. They have to be trained to the same standard that's --

Senator Gillibrand: Yeah.

General Cardon: For the others, working with the institution, education systems, the PEC, down in Arkansas, to get that online with the Cyber Center of Excellence, which will give them equivalency training for the training, as well. So, they'll all be trained to the same standard.

Senator Gillibrand: That's excellent.

And, for Air Force, how do you plan to train the -- your Reserve components?

General Wilson: Ma'am, the same -- to the same standard. They go through the same schoolhouse, same curriculum, same standard.

Senator Gillibrand: They'll just do it over time? It'll take them longer, because there are only -- or would you have them in a --

General Wilson: They come right through the same schoolhouse, side by side with Active Duty members, whether they're Guard, Reserve, or --

Senator Gillibrand: So, you might activate them for a certain amount of time to get the training? Like activate you for the 6 months to get the training, or whatever it is?

General Wilson: You're right, spot on, ma'am.

Senator Gillibrand: That makes great sense, actually. That's terrific.

Do you think the services need additional resources for this training, for this additional capacity? And, if you do, I hope you request it.

General Wilson: So, ma'am, for the Air Force, we've already built that into the model.

Senator Gillibrand: Okay.

General Wilson: We've invested in our schoolhouses both at Goodfellow, Keesler, and at Hurlburt, the first two being intermediate -- or initial training for intel and our cyber training, and then, at Hurlburt for our intermediate training. And so, all of those adds have been put in place. We're looking at the training model in the out years to make sure that we're comfortable with the size of the pipeline that we have today. But, that's already been accomplished. Matter of fact, the courses are up and running full steam right now.

Senator Gillibrand: That's great.

And this was mentioned in the previous panel, but retention obviously is something important if you're going to invest up to 2 years training these cyber warriors. Do you have plans on how to retain them, whether it's through, I don't know, compensation or -- I don't know what plan you

would -- or approach you would take.

General Wilson: So, ma'am, in the Air Force, we have several different retention initiatives, both for Active and for Reserve and Guard. We like to say we'll never compete on price. We just are not going to be able to --

Senator Gillibrand: You certainly --

General Wilson: -- compete on price.

Senator Gillibrand: -- can't, yeah.

[Laughter.]

General Wilson: It just isn't going to happen. So, we do look at targeted reenlistment bonuses. We look -- we're considering proficiency pay for certain skill sets, when they achieve certain skills. To be honest, it's the pride of service, it's the fact that there's a pretty interesting mission set, and we empower and give a lot of responsibility for very young folks. We find they have a passion. Not everybody is going to stay in the service. That's just a fact. The first thing we do when they think about getting out of the Active Duty is, we put our arms around them and talk to them about the Guard and Reserve opportunities out there.

Senator Gillibrand: That's great, yeah.

General Wilson: And if that's not the case, that's okay. We consider it an investment for the country, and we'll restock the pipeline.

Senator Gillibrand: Can you update me a little bit on Rome Labs and how that's being developed?

General Wilson: I'm sorry, ma'am, didn't --

Senator Gillibrand: Can you update me on Rome Labs and how that's being developed for the Air Force?

General Wilson: Absolutely. So, ma'am, Rome Labs is key. It's one of our science and technology wheelhouses. It's the epicenter for our S&T work. It's a very tight relationship with regard to the technology that's come out of Rome Labs. We're taking a look at the portfolio and then how to accelerate some of the technologies that are coming out of the labs, and how do we field it, make it operational in a more rapid fashion. And so, that's -- it's key to the partnership there.

Senator Gillibrand: Sure.

And, Lieutenant General, can you talk a little bit about how West Point's doing? I thought their cyber training was very impressive when I was last there. And I met a number of the cadets that were focused on that, and I thought it was really inspiring.

General Cardon: So, this year we'll assess 30 cadets into 17 -- 15 from the Reserve Officer Training Programs, 15 from the Academy. The Academy has adjusted their programs to account for cyber security, so I think that is going to be a tremendous benefit here for the future.

Like with the Navy, they're -- we're also exposing all of the officers to cyber security, because this has to become part of the foundational education that we expect them to have.

If I could just loop back on the retention really quick. On the high-end operators, what we've started doing is using 6-year enlistments. We're having no troubles filling that. The retention, I think, all of us are working through what is the best model to retain them.

Senator Gillibrand: And the other thing that I was impressed by at Fort Drum was that they're off the grid. And I thought that was vital, in terms of cyber defense and cyber missions, that there's an independence, where you can't be subverted or isolated because of energy needs. So, I would recommend to all the services, to the extent we have assets anywhere around the world, that ability to be off the grid is vital, in terms of protecting infrastructure and protecting abilities to respond. So, thinking long-term, defensively.

Admiral Tighe: I think the Navy, as part of Task Force Cyber Awakening and our shore infrastructure folks, recognize that we are dependent on a combination, obviously, of power generation that is internal to the Navy and commercial power providers, and then -- you know, that extends to overseas in all the complexities there. So, our

facilities folks have taken a -- taken on a special project to go study and look at what is -- what does "good" look like, in terms of the resiliency that we need to be resistant to any type of attack on that infrastructure upon which you depend.

Senator Gillibrand: Thank you.

Thank you all. Very grateful.

Senator Fischer: Thank you, Senator.

Thank you all. I would invite you to join us in the SCIF for a classified briefing.

And, with that, I will adjourn the open hearing today.

Thank you.

[Whereupon, at 4:07 p.m., the hearing was adjourned.]