Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON THE CYBER POSTURE OF THE SERVICES

Tuesday, May 23, 2017

Washington, D.C.

ALDERSON COURT REPORTING

1155 CONNECTICUT AVENUE, N.W.

SUITE 200

WASHINGTON, D.C. 20036

(202) 289-2260

www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON

THE CYBER POSTURE OF THE SERVICES

Tuesday, May 23, 2017

U.S. Senate

Subcommittee on Cybersecurity

Committee on Armed Services

Washington, D.C.

The subcommittee met, pursuant to notice, at 2:29 p.m. in Room SR-222, Russell Senate Office Building, Hon. Mike Rounds, chairman of the subcommittee, presiding.

Subcommittee Members Present: Senators Rounds [presiding], Fischer, Nelson, McCaskill, and Gillibrand.

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

Senator Rounds: Good afternoon. The Cybersecurity Subcommittee meets today to receive testimony on the cyber posture of the services.

We are fortunate to be joined this afternoon by an impressive panel of witnesses. Let me begin by just saying thank you very much for your service to our country. Vice Admiral Marshall Lytle, Director, Joint Staff, Command, Control, Communications and Computers, Chief Information Officer; Vice Admiral Michael Gilday, Commander, Fleet Cyber Command; Lieutenant General Paul Nakasone, Commander, Army Cyber Command; Major General Christopher Weggeman, Commander, Air Force Cyber; and Major General Loretta Reynolds, Commander, Marine Forces Cyber Command.

At the conclusion of my remarks and those of Senator Nelson, we will hear briefly from each of our witnesses. I ask our witnesses to limit their opening statements to 5 minutes in order to provide the maximum time for member questions.

We are making historic progress in the construction of our cyber force. There is nothing trivial about the standup of a 6,200-person force within the timelines that each of you must meet. And we are pleased that each of you seems to be on track to meet the October 2018 full operational

capability, or FOC, deadline that the U.S. Cyber Command has established.

Part of that progress is also evident as we start to see the deployment of capability and begin to get a sense of how a cyber force can be integrated with air, land, sea, and space.

I want to congratulate and thank each of you for your leadership in building this first of its kind U.S. military capability.

Despite the many successes, there are a number of challenges each of you are confronting. The purpose of today's hearing is to understand both the good and the bad, to get a sense of the areas where progress is sound and understand those challenges that are impacting you, challenges, quite frankly, that should be expected when undertaking the significant task that has been put before each of you.

We all too often gravitate here in Congress towards exposing and addressing the challenges and unfortunately fail to applaud the successes. I specifically mentioned the progress made in training the force, as that is by no means a trivial task. And I remain impressed by the progress.

However, I remain concerned about what happens next, what happens after the cyber mission force reaches FOC. More specifically, will each of you have the bench strength

necessary to sustain the tools, capabilities, and readiness levels required to be effective in the cyber domain?

When Admiral Rogers testified before the full committee earlier this month, it became apparent that our ability to maintain training readiness will be impacted by numerous variables, both within and external to your control. It was mentioned during that hearing that out of the 127 Air Force cyber officers who completed their first tour on the Cyber Mission Force, none went back to the Cyber Mission Force. While reasonable people can disagree about whether the jobs they went to involved an aspect of cyber in one capacity or another, given the low density and high demand of the Cyber Mission Force, we must be especially vigilant in managing the few resources which we have.

I am concerned that we will not generate and maintain the expertise we need unless we can build upon experience and develop the proficiencies required to stay ahead in cyberspace. Maintaining that expertise will require, among other things, the need to train personnel on new and perhaps rapidly evolving technology. My concerns with retention are exacerbated by the apparent lack of cohesive strategy for ensuring that the pipeline of new people will be sufficient to maintain readiness and keep those teams whole.

I look forward to hearing from each of you how we can assure that you are able to recruit the people you need,

train them to the level of capability required, and retain them in professionally viable cyber career fields. Do we need to rethink entirely what it means to be a cyber operator? Do they need to wear uniforms or meet the same physical requirements of other fields?

While the initial demands for the cyber force were personnel and training heavy, we are getting to the point where unless we begin to see dramatic changes in the budget, the forces we have trained will lack the tools required to be effective. Thus far, billions of dollars have gone toward service-level network infrastructure but far too little has been requested for the mission forces themselves. I am concerned that unless this changes immediately, we are heading down the path to a hollow cyber force.

We have been told not to expect much of a change in the fiscal year 2018 request which, if true, is something this committee will need to scrutinize in the coming weeks. Every service is constrained and each service has its own resourcing challenges. As we examine how those constraints and challenges impact the services' ability to resource cyber requirements, I believe it appropriate that we at least ask if the current man, train, and equip model is sufficient or if a new model should be considered, whether it be a hybrid of the existing structure or a cyber-specific service.

Senator Nelson?

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

Senator Nelson: Mr. Chairman, to that I would say amen.

In the interest of time, I will insert my opening comments in the record, and I am going to go kick off another committee and I will be right back.

[The prepared statement of Senator Nelson follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Very good. Thank you, Senator.

Why do we not just begin with opening statements, Vice Admiral Lytle?

STATEMENT OF VICE ADMIRAL MARSHALL B. LYTLE III, USCG, DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND COMPUTERS/CYBER AND CHIEF INFORMATION OFFICER, JOINT STAFF, J-6

Admiral Lytle: Good afternoon, Chairman Rounds. Thank you for inviting us to talk about the Joint Force's efforts in cyberspace. Vice Admiral Gilday, Lieutenant General Nakasone, Major General Weggeman, Major General Reynolds, and I share your keen interest in this topic.

I will focus my remarks on three primary missions in cyberspace and describe the current approach to strengthen cyber warfighting capabilities of the Joint Force.

The Joint Force executes the Department of Defense's three primary cyber missions in support of the national defense strategy: defend the DODIN, defend the Nation, and provide integrated cyber capabilities in support of the combatant commands.

Joint Force's first mission is to defend the Department's networks, systems, and information. The Joint Force must be able to secure its networks against attack and recover quickly if security measures fail. If our DOD systems are not usable, our greater defense capability will be diminished.

Second, the Joint Force must be prepared to defend the United States and its interests against cyber attacks of

significant consequence when directed by the President. This mission may be performed for significant cyber events that include loss of life, significant damage to property, severe adverse United States foreign policy consequences, or serious economic impact on the United States.

Third, when directed by the President or the Secretary of Defense, the Joint Force must provide integrated cyber capabilities to support military operations and contingency plans. These activities are conducted by U.S. Cyber Command according to priorities set within the globally integrated combatant command plans and in direct coordination with other U.S. Government agencies. These activities may include actions to disrupt adversary networks or infrastructure and prevent use of force against U.S. interests.

These primary missions are underpinned by three main cyberspace capability elements used to enable combatant commands' ability to execute their operational plans. These elements are defensible cyber terrain, cyber defenses, and the cyber forces. Together, these elements factor heavily into our ability to prevail against determined and capable nation-state actors.

Information about offensive forces and capabilities is classified, but please understand that these offensive components are important and are coupled with our defensive

capabilities for maximum effect.

The first element of the Department's cyberspace capabilities is defensible cyber terrain. Cyberspace is a manmade domain and requires common standards to achieve defensible, effective, and efficient operations. The Joint Information Environment Initiative provides these common standards for the protection of all network systems. Over the past years, the Department made significant gains in hardening our systems focused under the Department of Defense Cybersecurity Scorecard effort, and we have increased endpoint security and access control. We must continue to train all of our personnel across the DOD until they have a working knowledge of cybersecurity practices and hold leaders accountable for instilling that culture of cybersecurity discipline.

The second capability element dedicated to cyber defenses are arrayed in a defense in-depth posture with a focused level of tiered defenses. These defenses are broken into three tiers. Tier 1 is the Department's outer boundary of Internet access points defense suites. Tier 2 is the Joint Regional Security Stacks, and tier 3 consists of endpoint security systems like host-based security systems on work stations. These tiered defenses comprise our primary defense against external threats in cyberspace and will be increasingly reliant on automation to manage the

threats.

The final element, cyber forces, are categorized in two ways. The first are our fixed force defenders. Those are the people that operate and protect assigned network enclaves and associated systems. They are comprised of military cyber units that form the backbone of secure network operations, including service and agency network operations in security centers, cybersecurity service providers, and cyber incident responders.

The other and more often discussed category of forces, the Cyber Mission Force, is the Joint Forces maneuver force in cyberspace. The CMF is composed of 133 teams with objectives that directly align to the Department's three cyber missions and are directed by U.S. Cyber Command and its subordinate headquarters.

The Cyber Mission Force, all 133 teams, met their initial operating capability milestone in October 2016. All teams are also on track to meet their full operating capability in 2018, October. More than half the teams have already met their full operating capability milestone, and all of the teams are actively performing missions defending U.S. networks, defending DOD U.S. networks, protecting weapons platforms, and defending critical infrastructure.

Despite these successes, there are still significant readiness challenges that impact the cyber force. The Joint

Force completed a Cyber Mission Force training transition plan in January of this year. The plan introduced the federated joint training model and addresses the Cyber Mission Force active and a reserve component training demand. Through the institution of joint training standards and standardized readiness reporting, the Joint Force is beginning to identify trends that will help us better shape service policy and resourcing requirements for the future. Each service is working their unique cyber manpower challenges as part of their man, train, and equip responsibilities. They have learned and adapted over the past years instituting a number of changes to ensure the success of the Cyber Mission Force and its associated cyber tactical mission headquarters. You will hear more from my colleagues on all of their efforts.

Equally important to manning and training, equipping the Cyber Mission Force is evolving from the service platforms currently employed by cyber operators to a standardized joint capability that enables the force effectively and efficiently while integrating into existing planning and force development constructs. The framework for equipping the Cyber Mission Force for both defensive and offensive missions is built upon a family of interoperable systems from which the Cyber Mission Force can operate and synchronize operations. Prototyping and analysis of

alternatives is underway to determine the best composition of these systems under the unified platform of effort led by the United States Air Force.

As the Cyber Mission Force continues to grow and mature, so does the need to command and control and integrate the global efforts of this complex and geographically dispersed warfighting capability. The Joint Staff recently published a revised command and control model that streamlines the command relationships and synchronizes actions in support of the combatant command campaigns. The Office of the Secretary of Defense is currently working with the services to lay in resourcing ramps over the FYDP for the needed manpower and O&M costs for this C2 model.

Thank you, Mr. Chairman and member of the committee, for the opportunity to be here. I am grateful for the committee's interest and your support of our men and women in uniform.

[The prepared statement of Admiral Lytle follows:]

Senator Rounds: Thank you, sir.

Vice Admiral Gilday?

STATEMENT OF VICE ADMIRAL MICHAEL M. GILDAY, USN, COMMANDER, UNITED STATES FLEET CYBER COMMAND AND COMMANDER, UNITED STATES TENTH FLEET

Admiral Gilday: Chairman Rounds, Senator McCaskill, good afternoon.

On behalf of the more than 16,000 sailors and civilians of Fleet Cyber Command, thank you for the opportunity to appear before the subcommittee today.

I also want to thank you for your leadership in helping keep our Nation secure, particularly in the complex domain of cyberspace.

It has been my privilege to command Fleet Cyber Command for the last 10 months. Based at Fort Meade, Fleet Cyber is the operational headquarters for a globally deployed cyber force responsible for operating and defending Navy networks, operating our global telecommunications architecture, including satellites, and providing cryptology, signals intelligence, space, and cyber warfighting capabilities to support fleet and combatant commanders.

These are distinct but overlapping mission sets, and I wear three hats as the Navy cyber component to U.S. Cyber Command for cyberspace operations, NSA for cryptologic operations, and U.S. Strategic Command for space operations.

We are also designated as a Joint Force Headquarters-Cyber supporting both U.S. Pacific Command and U.S. Southern

Command. In addition to our Cyber Mission Force teams, we ensure full-spectrum cyber operations are considered within the joint planning environment.

In the maritime environment in which the Navy operates, it has become increasingly more complex, and this is due in no small part to the advancement and reliance on information technology that is tightly interwoven within the cyber domain. This growing integration of cyber into joint operations, as well as the rise in threats against our systems, are two trends that show no signs of slowing.

On those two points, the increased tempo in cyber operations and the upward trend in malicious cyber activity, we view our warfighting capability through a systems of systems approach focusing on people, processes, and technology. Our investments in people, processes, and technology, as well as our operational focus, has been guided by three goals: first, to operate our Navy networks as warfighting platforms; second, to deliver effects through cyberspace; and third, to field and sustain Navy's portion of the Cyber Mission Force. As of today, we have 27 teams at full operational capability, and I expect all of our teams to meet FOC before the October 2018 deadline.

Lastly, I still believe we have much room to grow. In particular, we will continue to benefit from maturing partnerships with the U.S. military services and our allies,

U.S. Government agencies, academia, and importantly, industry. Greater cooperation through information sharing, whether it is on common threats, new technologies, or best practices, is critically important in this shared domain.

Thank you again, Mr. Chairman. I look forward to taking your questions particularly, as you pointed out, those issues associated with recruiting, retaining, and sustaining our cyber force.

[The prepared statement of Admiral Gilday follows:]

Senator Rounds: Thank you, sir.

Lieutenant General Nakasone?

STATEMENT OF PAUL M. NAKASONE, USA, COMMANDING GENERAL, UNITED STATES ARMY CYBER COMMAND

General Nakasone: Chairman Rounds, Senator McCaskill, good afternoon. It is an honor to appear today on behalf of the men and women of U.S. Army Cyber Command and alongside Vice Admiral Lytle and my fellow service commanders.

My testimony today will focus on five different areas: first of all, the Army's progress in operations; its progress in readiness; its progress in resourcing; its progress in training; and its progress in partnering.

Three key priorities are guiding our operations.

First, we are aggressively operating and defending our networks, data, and weapon systems through network hardening, modernization, and active defense of Army networks.

Second, we are delivering effects against our adversaries, as illustrated by Joint Task Force Aries, which is contributing to the success of coalition forces against ISIS.

Third, we are designing, building, and delivering integrated capabilities for the future fight, focusing on defensive and offensive cyberspace operations.

Supporting readiness, the Army is building 62 total force cyber mission teams. The 41 active component teams are built and supporting real-world operations today. The

Army's reserve component is building 21 cyber protection teams, 11 in the Army National Guard and 10 in the U.S. Army Reserve. The Army will integrate the reserve component teams into our Cyber Mission Force.

The Army has also made strides improving network readiness. As the recent ransomware/malware incident has demonstrated, ensuring the security of our network must remain our number one priority requiring constant vigilance.

In the area of resources, the Army is implementing two talent management initiatives: first, a direct commissioning program to bring talented and experienced individuals on board at higher levels of responsibility and pay; secondly, a civilian cyber effects career program to unify multiple occupational specialties into one cross-disciplinary model for training and management.

In regards to training, since September 2014, the Cyber Center of Excellence has trained 1,500 soldiers. To ensure our teams are trained to USCYBERCOM standards, we will conduct approximately 80 collector training events and 48 internal mission rehearsals type training events during fiscal year 2017 to build proficiency and prepare teams for recertification, revalidation, and mission support operations.

To support training, DOD designated the Army as the acquisition authority for a joint cyber range, which will

provide high quality scenarios for individual and team and collective and mission rehearsal training for the joint cyber force.

Finally, partnerships are integral to our efforts. Army Cyber Command leverages the private sector and academic partnerships under various DOD umbrella programs to collaborate across the cybersecurity community.

Chairman Rounds, Ranking Member Nelson, Senators Fischer and McCaskill, thank you very much today. Your Army teams are actively protecting and defending Army and DOD networks, securing Army weapons platforms, protecting critical infrastructure, and conducting operations against global cyber threats. With the continued support of Congress, the Army will maintain its tremendous momentum building a more capable, modern, ready force that is prepared to meet any adversary in cyberspace today and tomorrow. Thank you.

[The prepared statement of General Nakasone follows:]

Senator Rounds: Thank you, General.

Major General Weggeman?

STATEMENT OF MAJOR GENERAL CHRISTOPHER P. WEGGEMAN, USAF, COMMANDER, TWENTY-FOURTH AIR FORCE AND COMMANDER, AIR FORCES CYBER

General Weggeman: Chairman Rounds, Ranking Member Nelson, and distinguished members of the subcommittee, thank you again on behalf of the men and women and the audacious men and women of 24th Air Force and Air Forces Cyber for the opportunity to appear before you today, alongside all my esteemed cyber colleagues. I look forward to discussing the Air Force's progress in advancing full-spectrum cyberspace operations and our contributions to joint operations globally.

Our headquarters is located at Joint Base San Antonio-Lackland, Texas, and we have airmen on mission around the world. Our warriors are operating globally as a maneuver and effects force in a contested domain delivering cyberspace superiority for our service and our joint partners.

Our forces exist to preserve our freedom of maneuver in, through, and from cyberspace while denying our adversaries the same. Our command places significant emphasis on operationalizing cyberspace as a warfighting domain across the range of military operations and continues to evolve our tradecraft to provide ready cyber forces to combatant and Air Force commanders across the globe.

Defense is our number one mission. We build, operate, secure, and defend the Air Force networks every day to ensure these networks remain secure and available in total providing on-demand capabilities to approximately 1 million users worldwide.

In collaboration with our service staff and our major commands, we developed and have begun implementation of three transformational efforts transitioning our cyber workforce posture towards a 21st century commander and cyberspace operator-driven cyber ecosystem centered on mission assurance.

The totality of these major Air Force efforts, plus our ongoing cybersecurity campaign plan, provides the Air Force with a full-spectrum framework for generating threat and risk-based mission assurance across the totality of our cyber terrain.

The Air Force is on track to achieve full operational capability for all service Cyber Mission Force teams by the end of fiscal year 2018. As of 1 May 2017, we have all teams at IOC and over 50 percent at full operational capability.

While we remain laser-focused on building and delivering our service teams to FOC, we have begun in earnest, along with all the other service components, to focus on team readiness, leveraging the Department of

Defense's established institutional readiness program and standards.

Our forces also support assigned combatant or joint force commanders by providing full-spectrum, all-domain-integrated cyberspace maneuver and effects in support of their assigned missions around the globe.

We train and fight as one team or one force, as we like to say, with all components: regular Air Force, Air National Guard, and Air Force Reserve. We are delivering cyber forces fully integrated with our total force partners in the Air National Guard and Air Force Reserve. The Air Force total force contribution to the cyber mission is comprehensive and impressive.

As a new and rapidly maturing warfighting domain, cyberspace operations continues to make huge advancements in the operationalization of missions and forces. However, there are challenges in our critical path. At the macro level, these challenges fall into four broad categories: manpower and training, cybersecurity of weapons systems, key enablers to cyberspace operations, and professionalization of our workforce.

I am proud of the tremendous strides made to operationalize cyber capabilities in support of joint warfighters in defense of the Nation. Despite the challenges of maturing and operating in stride across the

contested and diverse mission set, it is clear Air Force networks are better defended, combatant commanders are receiving more of the critical cyber effects they require, and our Department's critical infrastructure is more secure due to our cyber warriors' tireless efforts. They truly are professionals in every sense of the word.

Congressional support was essential to the substantial operational progress made and will only increase in importance as we move forward. And I am very glad to see the formation of this subcommittee to help us along the way. Resource stability and a formal national cyberspace strategy to guide force planning, resources, and prioritization of effort within DOD in the years ahead best enables our continued success in developing airmen and maturing our capabilities to operate in, through, from the cyberspace domain.

I am honored and humbled to command this magnanimous organization, and I look forward to your questions. Thank you.

[The prepared statement of General Weggeman follows:]

Senator Rounds: Thank you, General.

Major General Reynolds?

STATEMENT OF MAJOR GENERAL LORETTA E. REYNOLDS, USMC, COMMANDER, MARINE FORCES CYBERSPACE COMMAND

General Reynolds: Chairman Rounds, Ranking Member Nelson, Senators McCaskill and Fischer, on behalf of the marines, civilian marines, and their families of U.S. Marine Corps Forces Cyberspace Command, I thank you for your support to the work that we are doing, and I welcome this opportunity to highlight for you today what our marines are doing in cyberspace as we shift our focus from building this command to operationalizing, sustaining, and expanding capabilities in this warfighting domain.

I am humbled every day by the tenacity, professionalism, and commitment to mission success displayed by my team.

So as the Commander of Marine Forces Cyber, I wear two hats. I am the Commander of Marine Forces Cyber and I am the Commander of Joint Force Headquarters-Cyber Marines. In these roles, I command about 1,700 marines. We are a small force. Our force includes civilian marines and contractors across our headquarters and subordinate units. I organize operations along three lines of effort that I will briefly highlight for you today, and I use this framework to organize activities, allocate resources, grow capabilities, and measure our progress.

So my first priority is to secure, operate, and defend

the Marine Corps portion of the DODIN, which we refer to as the Marine Corps Enterprise Network, or the MCEN. The Marine Corps views the MCEN as a warfighting platform, as you have heard from my fellow commanders today. And so we must aggressively defend this network from intrusion, exploitation, and attack.

Our priorities this year for improving our defenses include actions to flatten the MCEN by collapsing domains and improving our ability to sense the environment. We want to harden the network through increased endpoint security, principally through WIN 10 deployment, and we want to implement a comply to connect capability. And finally, we are looking for ways to dramatically improve our continuity of operations capability of our cybersecurity service provider in Quantico.

My second priority is fulfilling our responsibility to provide ready, capable cyber forces to U.S. Cyber Command. We are on track to provide 13 fully operational capable Cyber Mission Force teams to meet U.S. Cyber Command requirements.

We have experienced tremendous growth in operational capability over the past year and have fully supported the delivery of operational cyberspace effects within named operations. I provide direct cyber support to U.S. Special Operations Command, and we are actively beginning actions to

hire manpower in my Joint Force headquarters and in a forward element embedded in SOCOM, organizations which will directly support SOCOM and their subordinate elements with cyber planning integration.

Across U.S. Cyber Command, marines are at the point of friction, increasingly relevant, and eager to contribute to the fight.

And my third priority is to add cyberspace warfighting expertise to the Marine Air Ground Task Force. Our Commandant, General Neller, understands the necessity to move forward quickly to build MAGTF capability to operate in all five domains. And so the first time this fiscal year, we have supported a training exercise within every Marine expeditionary force, which are our major warfighting commands, as you know.

In addition, we recently concluded a mission in support of a special purpose MAGTF in the CENTCOM AOR.

Across the board, the demand signal for marine cyber operators and capability is very high, and it increases with each successful mission.

Also this year we have participated in our service efforts to improve our information warfare capabilities that are organic to the MAGTF. Cyber will play a relevant part in that.

And for all these missions, this year we are building a

cyberspace MOS to improve readiness and retention of our operators, and we are also participating in the cyber excepted service for our civilian operators.

We have accomplished much in a short period working within the construct of these three lines of effort, but we still have a lot of work to do.

Thank you again, Mr. Chairman, members of the committee, for inviting me to testify before you today and for the support that you and this new committee have provided our marines and their families. I look forward to taking your questions and to maintaining an open dialogue with you in the future. Thank you.

[The prepared statement of General Reynolds follows:]

Senator Rounds: Thank you, General Reynolds.

I would note that all of your written statements will be included for the record of this meeting today.

Let me begin by addressing to all of you. According to testimony we received from the Defense Science Board earlier this year, for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. Do you agree with the Defense Science Board's assessment, and do you agree that because of that imbalance, we must have an effective cyber deterrence policy?

Admiral Lytle: I believe that statement is based on if we do not continue to invest in our cyber defensive capabilities of our country, and that could come true. What we need to do is really focus on increasing our capabilities to defend against those adversaries because unlike the other domains, in the cyber domain, there is a lot steeper learning curve for adversaries to gain capability. It takes a long time to build an army. It takes a long time to build an Air Force. It only takes about 6 months or less to hire some contractors and get capable as a cyber adversary in this domain. So we need to be on our game. We need to continue to look at ways to up the United States' game and the DOD's game in the cyber defense capability area.

Admiral Gilday: Sir, thank you for the question.

So a couple of comments. I think broadly we are concerned about the U.S. broad attack surface across a number of critical sectors that cover 16 in total.

I do think a good first step is the EO that was just signed out a week or 2 ago that essentially gives focus to those areas of critical infrastructure, the area of federal networks in terms of resiliency, and lastly the piece about cybersecurity for the Nation in terms of deterrence. So I think collectively the EO sets us off on a course of taking a deeper look in many different areas to come up with a collective strategy.

General Nakasone: Chairman, you know, as we have seen in this domain of cyberspace, the advantage is with the attacker obviously.

But in terms of what I think we need to do in looking at this, I do believe that there are three elements that we have to consider. First of all, our Nation needs, obviously, strong denial capabilities for its networks, its data, and its weapons systems. Secondly, there needs to be a series of response actions that we need to be able to provide to decision-makers and the President if required. And thirdly, I think it is the idea of resiliency. You cannot stop everything. You cannot defend against everything. But you have to have a degree of resiliency

that is built into your networks for this.

Senator Rounds: Any other thoughts?

General Reynolds: Sir, I would just completely agree with General Nakasone. I think what you heard all of us say is that our number one priority is the defense of our networks. And so from a deterrence perspective, ensuring that no matter what they send our way, we can deter and, if necessary, build a new network somewhere else when we need to. Resilience I think is what we are all seeking.

Senator Rounds: I think the Defense Science Board made it clear that at this stage of the game, as General Nakasone indicated, the attacker has the advantage, furthermore that we should be prepared here to make it as expensive as possible for them to make that attack. But second of all, based upon having an attack being successful, that we have to be able to rebuild and that we have to have resiliency. Would anyone like to comment on that and our capabilities today to provide that resiliency? Where are we at with regard to resiliency within our systems today?

General Weggeman: I will dive into this one.

I think what I would like to see and where I think we are going is we are focusing a lot more today than we were in the past on mission system resilience. We are focusing on both risk and threat-based resilience. And so our commanders are now involved in making sure that they can

fight hurt, as we like to say in the Department of Defense. And so all the things that all the services are working on are those PACE plans to make sure that we have a primary and alternate, contingency, and emergency capability on those key systems. We are going to commanders first and helping them translate their missions into the IT systems so that we can get a key functional analysis of what cyber mission systems we need to prioritize our defenses against.

And so I think that transformation of getting away from networks in a COM focus to resiliency based upon commanders' missions and the key things we have to do as the Department of Defense for our Nation is paying huge dividends. Obviously, there is a lot of ground ahead to hoe but I think we are making the investments. I am seeing the commanders talk about cybersecurity defense and resiliency far more now than they did 3 years ago.

Senator Rounds: Thank you.

Senator Nelson?

Senator Nelson: Thank you, Mr. Chairman.

You know, the Russian operation created or showed -- "exposed" is the word -- a serious vulnerability on our part. As you all have testified, we have created a Cyber Command and built the Cyber Mission Forces to operate in cyberspace, but as Admiral Rogers, the Commander, has recently testified, we have not trained or tasked these

forces to detect, to counter, and to go on offense to conduct this kind of information operation that the Russians did. Our cyber forces are focused on the technical aspects of cybersecurity, defending our networks from intrusions, as you all have stated that you are tasked to do, and in some cases, penetrating adversary networks. And we are not focused on the content of the information flowing through the Internet.

So you know what Putin is up to. The Chinese are up to it as well. So what can we do to make Putin feel enough pain to cease his aggression in cyberspace?

Admiral Lytle: Sir, there are a lot of things we could do, and it gets back to the deterrence topic we were talking about earlier. We need to be able to make all of our systems -- and this is not just the DOD system, but across the Nation, government systems -- more defensible and more resistant to this type of activity to keep the easy way in out of our systems. Right now, we do not have that level of cybersecurity awareness across the world.

We do have a number of efforts. We do not, obviously, focus just on the defensive side from the Cyber Mission Force point of view. There is a whole offensive capability that we could talk about in a classified environment that looks for activities, looks for ways, and sets up options for the President to take in case he wants to do something

about things like this.

Senator Nelson: Describe in this open session what you can about some of those offensive capabilities.

Admiral Lytle: The capabilities that can be prepared to deny adversary access, to manage adversary systems, to cause havoc amongst adversary systems -- those are a number of things you may be able to do within cyber using cyber techniques that cause kinetic effects on the other end of the wire.

Senator Nelson: Do you all see any natural specialization in each of your forces, natural roles that you would play?

General Weggeman: Senator, I cannot answer on behalf of all of my colleagues. But I think as an airman -- and I hope I speak on behalf of my colleagues. We have the air domain and the space domain. We are air-minded. We are space-minded. And I think what we bring is the unique perspective in terms of the application of cyber maneuver and effects related to air systems and maneuver in, from, and through the air domain as well. And I think that air-mindedness on both our offensive and defensive teams certainly supports very well our air component commanders around the world, but also offers air-mindedness to land, maritime, and space component commanders as well. And I think the Army does the same.

If you look across the totality of the Cyber Mission Force, there is a service team represented in each of the combatant commands there. So we have air-minded teams representing every combatant command in support of them with the exception, of course, of Special Operations Command because the Marine Corps has them all to themselves. So I think that diversity of what each service brings is actually being in play as the teams have a diverse presentation to the combatant commands.

General Nakasone: Senator, if I might. The Department has been open in terms of our actions against ISIS in cyberspace. We have Joint Task Force Aries, which I command, stood up to take on ISIS in a manner that Vice Admiral Lytle recently described.

To the point of your question, I think what we are learning is the importance of being able to counter our message, being able to attack a brand, in this case, attack the brand of ISIS. And then the other thing is how do we do this with the speed and accuracy that is able to get at an adversary that 6 months ago was moving uncontested in cyberspace. And I think we have learned those things over the past 6 months, and I think that we as a department have done that much better.

Senator Nelson: Have you all thought, since you need a lot of cyber talent, of putting Reserve cyber units located

in places like Silicon Valley, Boston, and Austin?

Admiral Gilday: Yes, sir. In fact, we have that presence now and continue to make additional investments through DIUx, which I know you are familiar with, in terms of helping the acquisition process get new technologies into the hands of the warfighters around those typically slow moving acquisition processes that currently exist. So we do have a presence in those areas.

Senator Nelson: A Reserve presence?

Admiral Gilday: Yes, sir. Navy has a Reserve presence.

General Nakasone: And, Senator, if I might add to that. The Army is building 21 cyber protection teams, and what we have learned and what we are attempting to do is to take places like Adelphi, Maryland, take places like Boston, take places like Pittsburgh and not only build teams there but bring the training to them. This is a new, I think, lesson that we have learned as the services. We have to do training a little bit differently for our Reserve component. Not everyone can take off from their homes and leave for 6 months to do training in a place like Fort Gordon, but if we can bring the training in a mobile aspect to places like Maryland, places like Pittsburgh, places like Massachusetts, we found it to have some success.

Senator Rounds: Senator McCaskill?

Senator McCaskill: I might add on that topic that we have some really terrific National Guard cyber units. We have one in Missouri that is now training across the country, a toolkit that they developed. The guy who runs that unit does the cybersecurity for Monsanto on a full-time basis. So he really knows what he is doing. So I think we need to build on that.

On that topic, General Weggeman, at the full committee hearing, Senator McCain brought up with Admiral Rogers his concern that -- and he confirmed this, by the way -- that out of 127 Air Force cyber officers that completed their first tour on CYBERCOM Cyber Mission Force, none went back to a cyber-related job. Now, that is an alarm bell as far as I am concerned. Would you address that briefly?

General Weggeman: Yes, Senator, absolutely, and I was expecting the question. And I appreciate Senator McCain's inquiry because it gets to a really, really important problem, which is how do all the services effectively manage force management and balance the weight of effort we have between growing and specializing a Cyber Mission Force, which is in its growth spurt right now, and balancing that against the broader enterprise needs of our services for a cyber IT workforce in our cybersecurity service provider roles, our cyber schoolhouses, and also balancing with the professional development of our airmen and civilians that

need to attend professional military education, to go to advanced cyber schools like the Cyber Network Operations Defense Program at NSA and also our Cyber Weapons Instructor courses, two great examples, which pays huge dividends when they come back. Those are the cyber jedis when they get back. And so how do you properly manage that balance?

And so, again, I do not have a lot of insights into the number without all the math that went into it, but I can tell you where we are at now, and that is we have the policies and the strategic framework in place where we are looking at two general officer-led bodies that manage our force down to the airmen. And what I can tell you and what I know to be true now is about one-third of the force is going from CMF to CMF each year, which is about where we need to be to balance build in the broader operational needs. And if you think about a 3-year rotation, that is about all you really want to do is one-third, one-third, one-third a year. And that allows us also then to get the rest of the bench in cyber, across the enterprise, talent and experience so when they come back, we have the force that we need on the CMF.

So I do believe starting in fiscal year 2013, fiscal year 2014, we may have had our eye off the ball a little bit, I think all the services were just kind of sorting out how do we stand up the enterprise that does the organize,

train, and equip.

But now the first thing I did when I took command, as an example, is I put a directive in place that said every person that is going to PCS off a Cyber Mission Force team that is not going to another Cyber Mission Force team now comes to me personally for review and approval.

Senator McCaskill: Well, I am glad that you are aware of it and working on it.

I got to tell you we are always blessed around here by our military fellows, and that is for all the military fellows that are in the room. I have got a really good one back here behind me. He tried to chart the national cybersecurity structure. Yikes. I mean, I have been studying it now for several hearings, and every time I have to start over again.

But here is what I am really worried about. I am also worried about how many vacancies we have in the sector-specific agency structure. If you look at USD policy, vacant. We have an acting. A principal USD policy, vacant. Acting, none. You know, Principal Deputy ASD-HDGS, vacant. Acting, none. There are a lot of problems with nobody home in a lot of these jobs.

But what I am really worried about is where we are plugging in the private sector. The only place we can find that the private sector gets plugged in is this unified

coordination group. Now, I guess you guys are all familiar with that? Yes? No? Okay.

But what is weird about that is we all know how we got to plug in the private sector because we are likely to be attacked in the private sector, not necessarily your all's networks. I mean, that is the cyber warfare that I think probably keeps some of you up at night in terms of the vulnerabilities in the private sector.

The only way it gets stood up is if directed by the NSC or requested by two agencies. In other words, it is kind of ad hoc. Well, that is not the way they do it in the UK, especially in light of what we have seen in the last 24 hours. Obviously, we need to be really on guard against what is going on on cyber in terms of preparing for even lone wolf attacks that the UK just suffered.

So can any of you address this structure where we do not have a standing group where we get plug-in from the private sector in terms of our cyber national security structure?

Admiral Lytle: Senator, the DHS is really the responsible player in that game through the end kick and their connections with all the sector-specific agencies and managing that, monitoring that. So what we do is we work through DHS to the private sector for the most part except for the defense industrial base area for that particular

sector. So DHS has the end kick, has the connections with all the major sectors of the private sector, and that is the primary way to go through that.

Senator McCaskill: Okay. So according to the NCIRP, when a cyber incident affects a private entity, the Federal Government typically will not play a role in this line of effort, but will remain cognizant of the affected entity's response activities.

I am ranking on Homeland Security. So I get the different hats here.

You know, you guys have a reputation of being rather siloed. I know that is a shocking revelation to you in this hearing. And I am just worried about how siloed these charts are, and that is the only alarm bell I am trying to sound today. It is pretty siloed. And I just worry that in this particular area of defense and danger, that being siloed is really, really a problem, much more so than in other areas where we have been traditionally siloed. So I am hoping that you all will take that back and look at it and make sure that we are having even from our military industrial base, if we have enough buy-in on something other than an ad hoc basis.

Thank you, Mr. Chairman.

Senator Rounds: Senator McCaskill, before you leave, I just wanted to make one -- after we are done with the first

round, I am going to ask General Nakasone or one of the others to explain how they are coordinating among themselves in terms of that flow chart. It made sense when each of them has had a chance to visit with me. I would like to have them share it with the entire committee. So if you have got the opportunity to stay for a few minutes, when Senator Gillibrand has completed -- thank you. We will have them share it for the record for sure. Okay?

Senator Gillibrand?

Senator Gillibrand: Thank you, Mr. Chairman.

Admiral Lytle and General Nakasone, what is the status of the inclusion of the Army National Guard cyber protection teams in the Cyber Mission Force? My understanding is that the Army and CYBERCOM have signed off on this. If so, what is the holdup?

Admiral Lytle: I will just do a quick start-off. The National Guard, Air Force and Army, and the Reserve teams are being fully integrated into the Cyber Mission Force. We talk about the 133 teams. Actually on top of that, there is the Guard and Reserve that are added to that skill set.

You kind of alluded to earlier in a previous question the Guard and Reserve folks bring some incredible talent to the game. A lot of these folks are doing this in their civilian jobs, and they are looking for a way to do it in their military hat. And from the Guard side, they offer

that capability to not only do it under their State authorities, but also, when called up, to do it under the Title 10 authorities of the DOD.

Paul, would you like to add?

General Nakasone: Senator, in terms of the 11 Guard teams that the Army is building now, the Army has approved the request to make them part of the Cyber Mission Force. It is our understanding that the Department of Defense will meet on that and likely approve that in the very near future.

But in terms of the man, train, and equip piece, which I think is even more important that you are asking about, so right now, we have met with the Guard on several occasions. The last week of January was our last total Army cyber summit. The next one will be on the 5th of June. We have three National Guard teams right now on active duty, 170, 171, and 172. And they are training for the next 400 days with us. So we have already begun to build teams such as 173, which you are very familiar with -- that is from the State of New York -- will be next on that. So we have a way ahead for the training where we will have all the Guard teams trained by the end of fiscal year 2022. And we will have them all to full operational capability by 2024. So we have the ability to man them. We have the ability now to train them, and now we are working on the equipping piece as

well, Senator.

Senator Gillibrand: So they are officially part of the Cyber Mission Force.

General Nakasone: So they are officially part of the Army's contribution to it. We are waiting for the Department of Defense to give that okay.

Senator Gillibrand: Because is that not important so they can receive their own equipment and they will be offered training spots if there is availability? Is that not required to like move them forward?

General Nakasone: No, ma'am. We have already started with the training. We have the training there. We have training seats at Fort Gordon. We are working the equipping piece of it. It is more in terms of making them part of the broader force. So, again, we will continue to move forward with that.

Senator Gillibrand: And do you think we are using them to their fullest potential right now? Do you feel like we are integrating on a level that we ultimately want to be?

General Nakasone: So I think there is always room for improvement, Senator.

Let me go back to Joint Task Force Aries, which I command. So 10 percent of that force today is a Reserve component. Among our best tool developers is from the U.S. Army Reserve. As we take a look at the National Guard teams

that we brought onto mobilization today, some very high talent. But the things that we have to do is we have to capture that talent. So being able to build a database, of which we are doing right now with the leading university, very important. And I think the last piece of it is are we able to recognize the very unique skills that we may need in our Nation's crisis.

Senator Gillibrand: Do you think that the Guard could ever serve as a conduit on cyber between State, local, and Federal Government, as well as the private sector, because of their unique authorities?

General Nakasone: Senator, that is an excellent point, and I certainly believe that. They have long-term presence in communities. So when you take a look at something like critical infrastructure, who better than someone that lives in the community to have an understanding of that? Who better to understand the State? Who better to have the relationships that have been developing there?

Senator Gillibrand: So I want to ask you a bigger question because I have been asking this in all our cyber hearings. I asked it earlier today. We now believe our election infrastructure is critical infrastructure. And we were just hacked by the Russians with the intent to undermine our democracy. I believe there has to be a federal component for elections moving forward. And I

believe although elections are run by States and are part of the purview of States rights, there needs to be at least some level of certification that each State has a capability and technological expertise to guarantee they cannot be hacked.

Do you see the National Guard perhaps fitting in this role? Because, obviously, this will be something you can consider being under Homeland Security, but the capabilities in cyber are really housed in DOD. So we have the state of the art technology. This is a foreign power trying to attack us. Some believe, including Chairman McCain, that it is on par to a declaration of war.

So would it be feasible or interesting or beneficial if perhaps the Guard would be that conduit to being able to have the most state of the art cyber defenses capable and available to it to be able to use that expertise in each State?

General Nakasone: So, Senator, if the Nation was to decide that there was a 17th sector for critical infrastructure, I think that obviously the means are in place for the Department of Homeland Security to request support from the Department of Defense through the means that are there such as defense support of civil authorities. And I am sure that with that, that would be considered at the time.

Senator Gillibrand: But would you specifically look to the Guard maybe to perform that role?

General Nakasone: Again, I would leave that to the policymakers. I think my role as the operational commander is to make sure that whatever decision is made to the utilization of the Guard, the Guard is very well trained and very well equipped and ready to meet those needs.

Senator Gillibrand: Thank you, Mr. Chairman.

Senator Rounds: Thank you.

Let us go back a little bit. It seems to me that there may be perhaps a lack of understanding in terms of how the entire force is set up. When we are training 133 different teams and we are doing it across the different forces, could you share with us how they share, coordinate, work together side by side, how the teams are made up, and how you are utilizing them and the reasons for it?

General Weggeman: Senator, I will take a stab at that.

And so I think we talked about it briefly in your chambers.

Senator Rounds: Yes.

General Weggeman: But I do not want to go too deep, but just to set the stage, the three unified command planned missions that we have in the Department of Defense for cyber that were mentioned by all of our opening statements are to defend the Nation in, from, and through cyber against an

attack of strategic consequence, to provide all-domain-integrated effects in support of our combatant commanders, and then to defend our networks but also to have defensive forces that defend our mission systems and our own space against adversaries in our own terrain.

So the three cyber mission team types were then designed against each of the mission types. So you have national mission teams, which are the cyber and cyberspace forces. So if the Russians, as an example, have a cyber force that are looking to impose costs on us, like we have been talking about, then our national mission team's job is to go into red space and cause effects and impose costs against that force. So cyber v. cyber in cyberspace.

The combat mission forces, the CMTs, are designed to provide all-domain integrated effects for what the combatant commands' problems are in their battlespace. A great example is General Votel in the ongoing campaign in Joint Task Force OIR against things he needs to do in Mosul and Iraq, et cetera. Aligned with his scheme of maneuver, whatever we can do in cyber to help him achieve his objectives, that is what the combat mission teams do. They are an offensive force.

And the last force and the majority of the force is our cyber protection forces. And they are an active force that is designed for active defense to operate in our weapons

systems and our networks to pursue and hunt for adversary presence and then clear and remediate that terrain and hold it so that they cannot get back in. And that is what those defensive forces do.

What we did back in 2013 is we said we are going to train all three team types using people from all four services in the standardized set of joint work roles and standards. And so every team has a standard unit of action and a standard unit of employment that looks exactly the same whether it is manned by marines, airmen, soldiers, or sailors. And that is how they are -- they are fungible in terms of they are the exact same thing. If you have a combat mission team, it is 68 people in the same work roles doing the same things. And that allows us to have the interoperability amongst the soldiers, sailors, airmen, and marines on the teams. They are all doing the same things. They have been through similar schoolhouses, all trained and certified to the same standards.

Senator Rounds: What is the benefit of having multiple forces on the same team? What benefits does that bring?

Admiral Lytle: It is the joint force concept, Senator. So having all the services represented on the same team or have teams made up of an entire service that are interchangeable, as with our other joint forces, it brings the particular nature of the service involved. We have Navy

teams that could -- we have the same skill set built, but they apply that skill set to different systems. So the Navy teams may understand naval systems better. The Air Force teams may understand Air Force systems better. Even though the skill set and the makeup of the team are designed to be exactly the same so they are interchangeable and the initial training is the same, they can then branch off and get specialized in particular systems because as with any cyber defensive team, you start off with the basic level of training. You start off looking the same. You start off being able to defend whichever. But then you need to learn the system that you are defending and know that system inside and out. So having the ability of those people to move about -- this also creates a better career path for cyber warriors so that as they move between service jobs and joint jobs, they can continue to stay in that cyber field, and there is a broader space they can work in.

Senator Rounds: You have to put together almost -- well, more than 6,000 members of these teams and you are going to do it in a very short period of time. Part of that requires security clearances. Can you share with us where you are at in terms of getting security clearances? I know contractors are telling us right now that there is a significant backlog for them. And if we are going to have them deliver work on a timely basis, they have to have

individuals who have security clearances. Do you have that same challenge? Can you share that with us, please?

General Reynolds: Sir, yes, we do. So we are actually having to adjust service manpower processes so that we can identify folks who are coming to the Cyber Mission Force early enough so that we can get them the top secret clearance and the poly and the access that they need. So it has been a challenge in growing the force rapidly.

The other thing that I would just add to the previous question, sir, is that part of our responsibility -- I think all of us -- is that aside from what we contribute to the Joint Force, we have a responsibility to teach cyber inside of our service. It is not a small mission. So bringing that skill set back, in my case, into the MAGTF -- nobody is going to do that better than another marine. And so that should not be lost because we are only 133 teams, but we really need other folks throughout the rest of the service to understand cyber in order to properly integrate it, sir.

Senator Rounds: Senator Gillibrand?

Senator Gillibrand: I have no questions.

Senator Rounds: Let me just continue on for just a minute here. I am just curious. Can you quantify the time which is lost or the delay for bringing people on the team, allowing them to move forward with their competencies based upon not being able to get a security clearance in a timely

fashion? Or if you would like, I would take that for the record.

Admiral Gilday: Sir, I think it depends on each person in terms of whether there are complicating factors like foreign contacts, for example, that lengthens the security process. What we are trying to do is begin that clearance process as early as we can, as soon as we bring those people on board in the services so we can get that lengthy process moving quickly.

The trades with that lengthy process, of course, are the insider threat that we want to avoid. So there is a balance there that this process is methodical and it is deliberate for a reason. It is just something that we have to deal with and factor into our team growth.

Senator Rounds: Senator Gillibrand?

Senator Gillibrand: I do have one extra question for Generals Nakasone and Weggeman.

Congress gave you authorization to direct commission service members with cyber experience. I understand that both of your services are now using this authority. Please tell me about how you are using this authority. And it has come to my attention that the reserve components are not included in these efforts perhaps because section 502 of the fiscal year 2014 NDAA regarding constructive service credit for cyber warriors did not include the reserve component.

Is that the case?

General Weggeman: So, ma'am, the first question is, yes, we are working constructive service credit or what we call direct accessions in the Air Force. Again, from what I know to be true -- it is a little outside of my lane as the operational commander -- I do not think we have a direct accession yet, but we have an Air Force cyber talent management that is in work with our headquarters Air Force A-1 and our SAFs, chief information officer, SAF-CIO. So that is in work.

And I do not know the answer to your second question about the reserve --

Senator Gillibrand: Why they were left out. Okay.

General Nakasone: Senator, in terms of the direct commission program, so we have put a program together. It will be announced later this summer. We anticipate our first direct commission needs being announced this fall and into the force by the spring.

As far as your second part of your question, I would like to take that for the record just to come back.

Senator Gillibrand: That is fine.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Gillibrand: And then I had a third related -- was the authorization issue resolved, and would you include them in your direct commissioning efforts? Do you have the authorization that you need to do this?

General Nakasone: Again, if I might, if I can take that for the record.

Senator Gillibrand: You will do that. That will be helpful.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Gillibrand: Thank you, Mr. Chairman.

Senator Rounds: Thank you.

I want to just touch on something which several of these Senators have brought up, and I just want to clarify it and give you the opportunity to differentiate. Let us just take the difference between infrastructure and identify election infrastructure, which is out there, versus an electric grid infrastructure. Homeland Security clearly would take the lead with regard to an electrical grid, which is identified as a critical infrastructure. Where would the DOD fit in with regard to responding to an attack on an electrical grid as part of our Nation's critical infrastructure versus Homeland Security?

Admiral Lytle: The PPD-41 process for the Homeland Security aspect would cover that initially. If the DHS or DOJ required assistance from DOD, then they can make their assistance up through the DSCO process and the President would make the call as to whether the DOD responds and assists in that.

Senator Rounds: So you basically, under today's policy, would not respond on a critical infrastructure attack unless requested back up through the manual channels. There is no preset, technically designed system which would automate a response or a protection mechanism.

Admiral Lytle: Correct, sir.

Senator Rounds: Is that a seam in the system which has to be explored further or more deeply?

Admiral Lytle: Yes, it could. Part of a cyber strategy to be laid out could address that. Looking at the process to decrease the cycle time to any response, if necessary, could be looked at. There is a lot of process we have to go through to respond.

There are a lot of other issues that would need to be addressed with the legality of DOD operating on a private entity or the private entity would even allow the Department of Defense to work on its network. There is a number of issues that the administration should work out.

Senator Rounds: Once again, you are talking about a policy which has to be developed yet.

There was a question earlier that I guess I was going to talk about, and that is with regard to weapons systems vulnerability. Section 1647 of the fiscal year 2016 NDAA had required a cyber vulnerability assessment of all major weapons systems by the end of 2019. I am just curious how each of your commands are supporting those assessments, if you are, and if you are not, are you aware of them and who is?

General Weggeman: From the Air Force perspective, we have begun in earnest on the cyber vulnerability assessments. Air Force Materiel Command has stood up an

office called Cyber Resiliency of Weapons Systems, or the CROWS Office. And they are what I would call our execution arm for the NDAA 1647 requirements. As Air Force cyber what we have done working with the CROWS office is we kind of train the trainers. Our cyber protection forces and our cyber service security protection forces have begun training and educating them on how to do a proper mission-based systems translation for what is key terrain on a weapons system and how to do a vulnerability assessment.

But the CROWS office has two primary missions, which were in my written submission. The first thing we want to do is they want to figure out how to bake in cybersecurity and defense bolted on an ongoing acquisition and future acquisition programs and systems that they manage, our systems of record. And the second thing is they want to do a mission and threat-based prioritization of shutting the doors and windows that are open in existing mission systems in partnership with us and our service reallocated cyber protection teams. And I believe the number that we have in execution for fiscal year 2017 is 50 systems we are doing vulnerability assessments on in fiscal year 2017, Senator.

General Nakasone: Senator, the Army is very aware of 1647. We have moved out in terms of looking at our key weapons systems. But this is a point where I guess I would say we have also learned a lot from looking at our service

cyber components that are to our left and our right, particularly the Navy where we have looked at how the Navy has done this, their methodology, the way that they have a governance structure set up because it is more than just looking at the vulnerabilities. It is how do you have a governance structure. How do you write the contracts? How do you ensure that what you do identify is actually mitigated in the future? So this is one where I would say we have tried to get out of our silo and look to our left and our right to see what the other services are doing and share some information.

Senator Rounds: Let me just move on. I am just going to ask another one. Section 1650 of the fiscal year 2017 NDAA required the cyber vulnerability assessment of the Department of Defense critical infrastructure by the end of 2020. How are each of your commands supporting those assessments, if you are, and is there anything that you can share with us in this unclassified forum?

Admiral Lytle: Senator, I would add 1650 -- that is actively being engaged with the OSD, AT&L, and the Joint Staff, and the services in terms of identifying those installations as required by 1650, and that process is definitely in play. It is being worked on.

Senator Rounds: Let me finish with this. I think sometimes when we get together, you are expecting that there

are certain questions which are being asked. Are there certain points that you would love to get across and sometimes in the forms that we are using, particularly in these subcommittees, you do not have that opportunity. I would like to take just a few minutes right now, and if you have the specifics that either you feel need to be addressed that have not been addressed with questions that have occurred here, areas which you want to reemphasize or you believe that should be emphasized that we have not taken into account, this is an opportunity for each of you to -- let me just say -- freelance somewhat. And if you would care to, in terms of additions to your statements and so forth, this would be the opportunity for you to do so.

Admiral Lytle: I will take an initial step.

Senator, one thing is on our Cyber Mission Force readiness, we have initially been using measures of IOC and FOC based on some percentages that we cannot get into in this forum. But as we mature that cyber force readiness measure, we are going to move from just kind of a rote measure of people and training to actual readiness. Our concern is as we get those initial forces in place in the Cyber Mission Force and the rotations start to occur, that we transition that from a full-out effort to get to that first level to a level that we could sustain and maintain. We do that by measuring readiness through the Defense

Readiness Reporting System, and it is based more on their mission roles and their capability to do the mission than actually having bodies in seats.

So as we transition to that -- and we just finished the cyber training transition plan that moves the training responsibility for the Cyber Mission Force over the next 2 years from U.S. Cyber Command to the services -- we get into the more normalized mode of man, train, and equip by the services to provide for the Joint Force. We need to make sure the services are online and resourced and capable to keep that pipeline rolling on the Cyber Mission Force, to keep that readiness up.

Senator Rounds: Anyone else?

Admiral Gilday: Sir, I will make a few points.

Three points from my view what is going very well. And I think personally I would say in terms of standardization across the force, in terms of cooperation across the Joint Force, and the synergy of the Joint Force, I think we are headed in the right direction and have been for a period of time.

I think in terms of the second point, the maturation of the force, I think on the defensive side, 2 years ago we could not stand on our own two legs to take on defensive incident response missions on our own without significant help from, let us say, NSA. We are now doing those missions

on our own and some pretty significant problem sets. And so I think that that belies the fact that we have been headed in the right direction.

And lastly, I would make a point about partnerships. I think across the U.S. Government I think with industry and I think across the services and again with allies and partners, we have made significant gains in terms of leveraging those relationships and improving the force.

Senator Rounds: Anyone else?

General Nakasone: So, Senator, I would offer, particularly as Admiral Gilday said, a lot of progress. And I would say within my own service, a lot of momentum. Some decisions that were made by my predecessors and by senior Army leaders that stood up a branch, established a schoolhouse, invested in infrastructure and capabilities, and also put money towards people -- that has really paid off for us.

But the key piece at the end of the day for me is being able to ensure that we do talent management right with all of that. Foundational to us is to be able to keep our best people -- not all of our people, but our best people. And that is where I think that myself and all of the commanders are going to be held to to make sure that we continue to make this an attractive place for our young people to continue to grow and contribute to this.

General Weggeman: Just to pile onto that, Senator, I will say it a little bit differently. The most critical element in successful cyberspace operations is not copper or silicon. It is carbon. And we have to be really, really focused on the human capital that it takes. So we need manpower. We are fielding 6,000-plus for a maneuver and effects force, but there are operational levels of command and control. There are those that do other security and defense operations. There are all of the other carbon DNA footprint we need around that to make it work. If we do not have the proper manpower at all echelons of a command and control framework, then it is only as strong as its weakest link. And so I echo what General Nakasone just said.

One other thing, just to highlight Senator Gillibrand's point about the Guard, I want to give an example. You have been talking about how do we do discovery learning on the role of DOD and specifically our citizen airmen, citizen soldiers to help in the private sector SCIR support. I will give you an example that we can provide you some further information on.

The 262 cyber operations squadron of the Washington Air National Guard has done discovery learning and has a process for how they can do security and defense, partnering with their domestic electric power companies, and they are now working their way through how they do it with a private

sector company in the same State, working with a band of lawyers, of course, and the Title 32 status and what we are offering. And so I think that is a great exemplar of the power to be.

And I would offer a slide for the committee that I had printed out. And it is a slide that just shows -- one of our cyber protection teams is a Guard team already in the active build, and they have already been on two rotations. And I had the team lead build a slide of where all the citizen airmen came from in their private sector jobs on that mission. And the slide is pretty powerful when you see the 18 to 21 cyber and IT companies and power companies that are on it. And I would just offer it to you. It is kind of an inspirational slide.

[The information referred to follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Thank you. Very good.

General Reynolds: Senator, thank you for the question.

I think so much of this has already been said, but I think that it has been important for us to realize that cyberspace is a brand new warfighting domain. And to General Weggeman's point, starting with that 6,000-plus number was really just a start. And so I want to thank the Congress for -- some of the growth that we recently got this year in the Marine Corps is going to fighting in the information domain. It is information warfare. Some of those are going to be cyber protectors in the MAGTF that I would coordinate very, very closely with as Marine Forces Cyber. Those are also offensive forces in electronic warfare. So how do you bring together electronic warfare, cyberspace, information operations, fighting in the information domain? We are investing in that in the Marine Corps, and I want to thank you for the end strength that we got.

But inside Marine Forces Cyber, I was just thinking the agility that we need to retain these very, very talented people -- we have to think of new ways to do that. And so it is very, very difficult to compete with industry on this. So we send these kids to -- I call them kids. They are a lot younger than I am. We give them the best training. We give them top secret clearances, and importantly, we give

them phenomenal experience and they are very, very highly recruited. And so having the retention incentives and not just for the uniformed but for the civilian marines as well-- so having more flexibility in retention incentives for these folks is important to us because I think most of them, in my experience -- they want to stay a marine. Hence, the cyberspace MOS I think is going to improve a lot for us in the Marine Corps.

But one of the things that we are dealing with right now is we have to compete. So there is no more direct hire of retired marines. So in the Department of the Navy, I got to compete. I have to compete a job before I can direct hire somebody that I know already has the clearance, already has the skill set, already has the experience. I have to compete that job before I can direct hire. And so we are working that. We have to work that in the Department. It is a policy issue for us.

And then finally, sir, just contracting agility, being able to quickly employ a tool on the network that we know is going to provide us the greatest defense is so important.

Thank you, sir.

Senator Rounds: And I appreciate all of your thoughts on this. This is one step forward as we move not just into the oversight but also into the legislative side of our responsibilities. I understand the need that you have

expressed with regard to being able to move with agility with regard to contracting for services and products.

We have got a small university in South Dakota, Dakota State University at Madison. And several years ago, they began a process that was specific to what they thought would be a limited amount of interest in, which was Internet security for financial institutions, which now has morphed into something with basically 1,000 different students that have an interest in that, but also with regard to cybersecurity itself and with relationships with the government today, will continue to grow.

And so it is fascinating to see how these young people have an interest not just in the private entity side of things, but they do feel a sense of patriotism and a sense of desire to learn and to move forward. And if we can make something like that happen, whether it be on reserve component or on a National Guard component, I think we should be exploring that as well as an additive to the ongoing full-time force as well.

So I most certainly appreciate your time today. Your service to our country once again is greatly appreciated. And I do not think we can say that enough times.

But unless someone has anything to add at this point -- yes, sir, Admiral?

Admiral Lytle: Senator, just one more add, just an

offer. I think it is already being worked, but this kind of relates to how we do operations and how the National Guard operates is our cyber guard exercise coming up. It is a day that we can bring you all down and have the entire subcommittee or as many as possible come down and actually see how the DOD works with DHS and DOJ and the Guard and Reserve units in a large exercise environment. I really look forward to having you down there, sir.

Senator Rounds: We have been advised of that, and we are looking forward to it. Thank you.

With that, I want to thank all of our individuals that are here with us today. Thank you once again for your service, and thanks for taking the time to come here prepared to answer our questions.

At this time, we will adjourn this committee meeting.

[Whereupon, at 3:46 p.m., the hearing was adjourned.]