May 23, 2017

Cyber Posture of the Services

Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

Available Webcast(s)*:

Full Hearing:
https://www.armed-services.senate.gov/hearings/17-05-23-cyber-posture-of-the-services

Compiled From*:

https://www.armed-services.senate.gov/hearings/17-05-23-cyber-posture-of-the-services

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

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.]

STATEMENT OF

VICE ADMIRAL MARSHALL LYTLE

DIRECTOR COMMAND, CONTROL, COMMUNICATIONS

AND COMPUTERS/CYBER, JOINT STAFF

BEFORE THE SENATE ARMED SERVICES

SUBCOMMITTEE ON CYBERSECURITY

MAY 23, 2017

INTRODUCTION

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, thank you for inviting us to discuss the Joint Force's efforts in cyberspace. I appreciate the opportunity to explain the progress made to improve America's cyber defense posture.

I will focus my comments on three primary missions in cyberspace and describe the current approach to strengthening the cyber warfighting capabilities of the Joint Force. Toward that end, I will describe the state of our ongoing efforts to man, train, and equip the Cyber Mission Force, as well as the Joint organizations needed to Command and Control them. Finally, while I cannot discuss particulars in an unclassified statement, I will broadly describe the cyber capabilities needed to support both offensive and defensive teams.

JOINT STAFF ROLE

As part of my duties as the Director for Command, Control, Communications and Computers/Cyber, I work with our Joint Staff Operations, Planning and Resourcing leaders to integrate strategic cyberspace matters, including synchronization with national strategies, readiness tracking of joint cyber forces, and development of capabilities and concepts to support the Chairman's decision making. We work closely with the Principal Cyber Advisor, the Office of the Secretary of Defense staff and the Services to assess, address and advocate for the Combatant Commands' cyber mission requirements and priorities in support of the National Defense Strategy.

PRIMARY MISSIONS IN CYBERSPACE

The Joint Force executes the Defense Department's three primary cyber missions in support of the National Defense Strategy. The Joint Force defends the Department's networks, systems, and information. The United States military's dependence on cyberspace for operations led the Secretary of Defense

in 2011 to declare cyberspace an operational domain for purposes of organizing, training, and equipping United States military forces. The Joint Force must be able to secure networks against attack and recover quickly if security measures fail. To this end, network defense operations are conducted on an ongoing basis to securely operate the Department of Defense Information Networks. When indications of hostile activity are detected within networks, the Joint Force has capabilities to react, recover and return the networks and systems to a secure posture. Accordingly, network defense operations on Department's networks constitute the vast majority of the Joint Force's efforts in cyberspace.

In addition to protecting Defense Department networks, the Joint Force must be prepared to defend the United States and its interests against cyberattacks of significant consequence when directed by the President or his national security team. This second cyber mission is performed on a case-by-case for significant cyber events that may include loss of life, significant damage to property, serious 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. Examples include cyber operations that disrupt and adversary's military related networks or infrastructure in order to terminate an ongoing conflict on United States terms, or to disrupt an adversary's military systems to prevent the use of force against United States interests. United States Cyber Command, in coordination with other United States Government agencies, may be directed to conduct cyber operations to deter or defeat strategic threats in other domains. These primary missions are underpinned by three main cyberspace capability elements used to assess Combatant Commands' ability to execute their operational plans.

ELEMENTS OF CYBERSPACE CAPABILITY

This statement will not include information about offensive force or capability due to its classification, however, offensive components are important and are coupled with our defensive forces and capabilities to achieve maximum effects.

Cyber forces, cyber defenses and defensible cyber terrain are the three main elements that determine the Joint Force's our ability to achieve the primary cyber missions. Together, these elements factor into our ability to prevail against determined and capable nation-state cyber threat actors.

Of the cyber forces, the first line of defense -- "fixed force defenders" -- that operate and defend assigned network enclaves and associated defenses. Sometimes referred to as "cyber enterprise defense forces", they are composed of military cyber units that form the backbone of secure network operations. They include Service and Agency Network Operations and Security Centers, Cyber Security Service Providers, and Cyber Incident Response Teams, among others.

The Cyber Mission Force (CMF) is the Joint Force's "maneuver force" in cyberspace. The CMF is composed of 133 teams with objectives that directly align to the Department's three cyber missions. These tactical teams are command and controlled by a planning and execution structure led by United States Cyber Command through its subordinate Joint Force Headquarters.

The second capability element, dedicated cyber defenses, are arrayed in a defense-in-depth posture with a focused level of tiered defenses including the Department's Internet Access Point defense suites, the Joint Regional Security Stacks, and Service and Agency network security boundaries at the organizational and installation levels. These tiered defenses comprise our primary defense against external threats in cyberspace.

The final main element of the Department's cyberspace capabilities is defensible cyber terrain. The nature of cyberspace means that individual end-user machines are directly susceptible to compromise, and that a single compromise can quickly proliferate laterally to other machines. This inside threat coupled with the human factor introduced by users necessitates the protection of all networked systems to a specified minimum level of cybersecurity. Over the past year, the Department made significant gains in hardening our systems under the Department Cybersecurity Scorecard effort. Coupled with increased end point security, we must continue to train all personnel until they have a working knowledge of cybersecurity practices, and hold leaders accountable for instilling a culture of cybersecurity discipline.

Further improving the defensibility of cyber terrain involves systematically identifying "Mission Relevant Cyberspace Terrain" and obtaining situational awareness of that terrain in support of critical missions. Executing the DoD Cyber Strategy line of effort on mission assurance, the Joint Staff led a Department-wide initiative to bring together expert planners from the cyber defense and mission assurance communities to forge and codify a new approach to identifying the key cyber terrain that underpins the Joint Force's critical missions. This approach was vetted and refined during exercises. A formal Planning Order was sent out to all Combatant Commands last month toward that end, the culmination of 18 months of effort.

As the senior Joint Staff cyber leader, my main focus is on the manning, training and equipping of the cyber force. The remainder of my statement will focus on the successes and unique challenges faced in building and maintaining the world's premiere cyber force.

CYBER FORCES

The Joint Force's ability to man the cyber force is predicated on the

assumption that the force is a net exporter of cyber talent. Much like pilots, air traffic controllers and other highly technical military specialties, the Joint Force does not compete with industry, but rather is focused on building training programs and strategies to grow talent, leverage Reserve Component expertise, and retain adequate numbers of seasoned cyber operators to meet the growing demands in cyberspace. By anchoring our personnel strategies in net production vice competition, in addition to leveraging direct hires and native talent, we will be better able to produce adequate numbers of cyber experts while enhancing the collective cyber defense posture of our Nation.

Developing a training program for cyber operators resembles the challenge faced in training pilots and aircrew to operate the world's most advanced aircraft, maintaining their skills on the latest aircraft systems, and sustaining their numbers to ensure a constant sufficiency of motivated and technically excellent personnel. Creating a "pipeline" in the United States military's air components took many years. I am unsurprised by the challenges encountered while constructing the training and personnel pipeline for the Cyber Mission Force.

The Joint Force completed the Cyber Mission Force Training Transition Plan in January of this year. The plan introduced a joint training model and addresses the Cyber Mission Force Reserve Component training demand. As part of this effort a training funding shortfall was identified, and the Joint Staff is working with the Office of the Secretary of Defense to mitigate this shortfall.

The make-up of the cyber force is unique in warfighting because one-third of its composition is civilian. This poses a unique recruiting and retention challenge. We appreciate the committee's focus on this unique challenge and Congress' efforts to improve our ability to address this issue with Section 1107 of the FY16 National Defense Authorization Act. The Department of Defense Chief Information Officer's office is pursuing a permanent fix via the implementation of

the Department's Cyber Excepted Service program.

Equally important to manning and training the Cyber Mission Force is evolving from the narrowly focused Service platforms employed by cyber operators to a standardized joint capability that equips the force effectively and efficiently with integration 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. The Joint Force is conducting an Analysis of Alternatives to determine how best to equip the Cyber Mission Force with Title 10 mission platforms.

The Cyber Mission Force – all 133 teams -- met their Initial Operating Capability milestone in Oct 2016. All teams are also on track to meet their Full Operating Capability milestone by Oct 2018. More than half of the teams have already met their Full Operating Capability milestone and all 133 teams are actively performing their assigned missions defending DOD networks, protecting weapons platforms, and defending critical infrastructure. Despite these successes, there are still significant readiness challenges that impact the cyber force. Joint training standards have been published and instituted standardized readiness reporting in the Defense Readiness Reporting System in order to track and address these challenges. This nascent tracking capability is beginning to identify trends that will help us better shape Service policy and resourcing requirements in 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 four years, instituting a number of personnel policy changes to ensure the success of the Cyber Mission Force and its associated cyber tactical headquarters. For example, all of the Services are leveraging their Reserve

Components to augment Cyber Mission Force teams, either in whole or in part, while adding Federal, State and local cyber surge capacity allowing the nation to collectively respond to major threat activity in cyber.

The Navy and Marine Corps continue to utilize individual augmentees to fill gaps in their active duty Cyber Mission Force teams and are looking at other ways to utilize their Reserve Components to address critical skillsets and shortages. Also, the Air Force utilizes its reserve component to present 3 full teams to the Cyber Mission Force as part of their total force contribution. Behind these 3 “full-time equivalent” teams are 15 rotating reserve teams comprised of Air Force Reserve and Air National Guard members that provide 12 teams of surge capacity in addition to the 3 full time teams required by United States Cyber Command. Finally, the Army Reserve Component began building an additional 21 teams to augment the original 133 Cyber Mission Force teams as well. Once fully built, the reserve Component will be providing approximately a fifth of the total Cyber Mission Force surge capacity of 166 teams. The build and training plan for these additional Reserve Component forces is included in the Cyber Mission Force Training Transition Plan referenced earlier should you wish further details.

The Cyber Mission Force continues to grow and mature, as does the increasing need to Command and Control and synchronize the global efforts of this complex and geographically dispersed warfighting capability. The Joint Staff recently completed a revised Command and Control model that streamlines the command relationships and synchronizes actions in support of Combatant Command campaigns. This model, coupled with manpower assessments performed by a team of joint manpower experts last summer and fall, informed a Joint Manpower Validation effort completed last month. The Department is currently working with the Services to review resourcing requirements for the

future.

CONCLUSION

Thank you again, Mr. Chairman, Ranking Member Nelson, and Members of the Committee for the opportunity to provide this statement. I am grateful for the Committee's oversight and your support for our men and woman in uniform.

NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

STATEMENT BY

VICE ADMIRAL MICHAEL M. GILDAY

COMMANDER

U.S. FLEET CYBER COMMAND

U.S. TENTH FLEET

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

1ST SESSION 115TH CONGRESS

MAY 23, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

Chairman Rounds, Ranking Member Nelson and distinguished members of the Subcommittee, thank you for your continued support of the men and women of U. S. Fleet Cyber Command, the U.S. Tenth Fleet, and the United States Navy. It is a privilege to represent those outstanding Sailors and civilians who comprise our Fleet Cyber/Tenth Fleet team, and I appreciate this opportunity to update you on how our Navy's cyberspace operations are evolving to remain competitive in a changing strategic environment.

U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for operating and securing Navy Enterprise networks, defending all Navy networks, operating our global telecommunications architecture, and providing Cryptology, Signals Intelligence (SIGINT), Information Operations, Electronic Warfare, Cyber, and Space warfighting capabilities to support Fleet Commanders and Combatant Commanders. With distinct, but overlapping mission sets, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Cyber Command for cyberspace operations, the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service and the Navy's component for space under U.S. Strategic Command.

Headquartered in Fort Meade, Md., U.S. Fleet Cyber Command exercises operational control of globally-deployed forces through a task force structure aligned to the U.S. Tenth Fleet. U.S. Fleet Cyber Command is also designated as the Joint Force Headquarters-Cyber aligned to U.S. Pacific Command and U.S. Southern Command for the development, oversight, planning and command and control of full spectrum cyberspace operations for assigned Cyber Mission Force teams.

U.S. Fleet Cyber Command's operational force comprises nearly 16,500 Active Duty and Reserve Component Sailors and civilians organized into 24 active commands and 32 reserve commands around the globe. The commands are operationally organized into a Tenth Fleet-subordinate task force structure for execution of operational mission. More than 35 percent of U.S. Fleet Cyber Command's operational forces are directly aligned to execute our cyberspace operations missions.

In the two years since my predecessor VADM Jan Tighe last testified before the Emerging Threats Subcommittee in April 2015, we developed and released our *Strategic Plan 2015-2020.* This plan charts our course to deliver on our responsibilities by leveraging our strengths and shrinking the Navy's vulnerabilities to a cyber adversary, which I detail throughout this statement. Across the wide-ranging responsibilities, we identified 5 strategic goals:

1. Operate the Network as a Warfighting Platform: Defend Navy networks, communications and space systems, ensure availability and, when necessary, fight through them to achieve operational objectives.
2. Conduct Tailored Signals Intelligence: Meet the evolving SIGINT needs of Navy commands, including intelligence support to cyber.
3. Deliver Warfighting Effects Through Cyberspace: Advance our effects delivery capabilities to support a full spectrum of operations, including cyber, electromagnetic maneuver, and information operations.
4. Create Shared Cyber Situational Awareness: Create a shareable cyber common operating picture that evolves to full, immediate awareness of our network and everything that happens on it.

5. Establish and mature Navy's Cyber Mission Forces: Stand up 40 highly expert Cyber Mission Teams and plan for the sustainability of these teams over time.

Since that time, we, as a command, along with our fellow Service Components, U.S. Cyber Command, and the Department of Defense (DoD), have continued developing organizationally, as well as evolving cyberspace capabilities and capacity. I thank you for opportunity to discuss the Navy's progress in cyberspace, where we have made much progress and are moving out smartly on the course ahead.

Operate the Network as a Warfighting Platform

We operate in an increasingly competitive environment where information is the fuel of decision making and protecting that information and our mechanisms for Assured Command and Control (C2) are critical to successful maritime operations. Loss of this information not only degrades our confidence and effectiveness of our C2, it also leads to loss of intellectual property and dulls our competitive edge. The margins of victory are razor thin, and we cannot afford to lose a step. To help ensure we retain our competitive edge, the forces of Fleet Cyber Command and the Tenth Fleet are highly integrated with our Navy's regional Fleet Commanders they support and are fully integrated to current and future Fleet operations so we may flex and adjust our cyberspace capabilities to maximize success of any assigned mission. Our leadership is fully supportive of U.S. Fleet Forces Command and U.S. Pacific Fleet's focus on distributed maritime operations and Fleet-centric warfighting.

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DoDIN). I can most succinctly capture our approach to cybersecurity by stating the Navy operates is networks as a warfighting platform. This concept has many facets, including as a warfighting platform it must be aggressively defended from intrusion, exploitation and attack. As a warfighting platform, the network must be agile and resilient and responsive to the C2, intelligence, logistics, and combat support functions that depend upon it. As a warfighting platform, it must be capable of and available to deliver warfighting effects in support of Combatant Commander operational priorities.

The Navy Networking Environment currently consists of more than 500,000 end user devices; an estimated 75,000 network devices (e.g., servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves. Reflective of the larger culture, the demand for interconnectedness continues to grow and cybersecurity solutions must keep pace.

Today's Navy's Enterprise Networks have benefited greatly from the nearly 1 billion dollar executed and proposed investments (through FY 20) that reduce the risk of successful cyberspace operations against the Navy Networking Environment.

The Navy took such aggressive actions implementing lessons learned during Operation Rolling Tide, during which U.S. Fleet Cyber Command fought through an adversary intrusion into the Navy's unclassified network. Some of our best investments have not only been in technology, but in the development of policies and Tactics, Techniques and Procedures. This investment of time and focus enabled significantly increased visibility into and more importantly increased awareness of the state of Navy's Enterprise Networks.

It was through the lens of our post-Operation Rolling Tide efforts that the Navy identified where immediate infusion of defensive network capabilities was most critical and where accelerated modernization of network infrastructure was most warranted.

Reducing the network intrusion attack surface

Opportunities for malicious actors to gain access to our networks come from a variety of sources such as known and zero-day cyber security vulnerabilities, poor user behaviors, and supply chain anomalies. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the size of the attack surface, the greater the risk to the Navy mission. The attack surface grows larger with aging operating systems and when security patches to known vulnerabilities are not rapidly deployed across our networks, systems, and applications. The attack surface also grows larger when network users, unaware of the ramifications of their on-line behavior exercise poor cyber hygiene and unwittingly succumb to spear phishing emails that link and download malicious software, or use peer-to-peer file sharing software that introduces malware to our networks, or simply plug their personal electronic device into a computer to recharge it.

The Navy is taking positive steps in each of these areas to reduce the network intrusion attack surface including enhanced cyber awareness training for all hands, enhancements to how we monitor our networks for compliance and vulnerabilities, and improving the process on how we inspect the cyber readiness of our networks. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through working with industry partners and academia on ways to utilize data analytics, machine learning, and other automation technologies. Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades:

The Navy's Next Generation Enterprise Network- Recompete (NGEN-R) is an evolution building on the successes of the current contract. Incorporating lessons-learned from Operation Rolling Tide, a large-scale network maneuver and operation to eradicate and adversary from the Navy's unclassified network, and combining our overseas networks into the Navy Marines Corps Intranet (NMCI), will offer improved situational awareness, ability to C2, operate and defend the network. Extending our CONUS NMCI to our OCONUS Network (ONE-Net) will leverage the operational and security capabilities of the NMCI and the unique requirements of our overseas warfighters, reducing the network attack surfaces. The improved situational awareness capability in NGEN-R will provide our headquarters and network defense subordinate forces the ability to make better informed network operational decisions, improving our network response actions, reducing the network intrusion attack surface and decreasing response time.

Often times, people are viewed as the largest vulnerability in this equation – by that same logic, we believe our people, each and every person touching a keyboard, can make the network stronger. In addition to cyber awareness training for all hands, we are working closely with U.S. Cyber Command to develop an innovative and robust persistent training environment for our network defenders. We are also working closely with the U.S. Naval Academy, the Naval Postgraduate School, and the U.S. Naval War College on ways to increase the relevance and currency of their cybersecurity and cyberspace operations education programs and initiatives.

Enhance our Defense in Depth Operations

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service counterparts, DISA, Inter-Agency partners, and commercial cyber security providers to enhance our cyber defensive capabilities through layered sensors and countermeasures from the interface with the public internet down to the individual computers that make up the Navy Networking Environment. We configure these defenses by leveraging all source intelligence and industry cyber security products combined with knowledge gained from analysis of our own network sensor data. As information sharing improves, so does mutual defense.

We cannot and will not assure our mission in this domain alone. We operate in and around an infrastructure that is largely commercially owned. The rise of dual-use technology has created vulnerabilities, but should just as well be leveraged for opportunity. Many of our challenges are not unique to the .mil domain. We fend off the same spectrum of adversaries, who are using the same playbooks against .govs and .coms. We work to plug and patch the same legacy networks. Industry is and will remain a critical mission partner through both technology development and responsible information sharing.

We are also piloting and deploying new sensor capabilities to improve our ability to detect adversary activity as early as possible. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities to behavioral sensing, and improving our ability to detect new and unknown malware. We also have the need to be able to analyze this sensor data at "machine speed," and are working with partners to investigate ways to utilize emerging data sciences technologies to help with the analysis of our networks.

I firmly believe the future lies in automation and machine learning for defense. Not only does this change the dynamic of speed and scale, but it allows us to use our people where they are most needed.

As my predecessor noted in her 2015 testimony, the Navy continues to support the spirit and intent of the Joint Information Environment (JIE), including the implementation of a single security architecture (SSA) that begins with the Joint Regional Security Stacks. The Navy and Marine Corps Intranet is our primary onramp into JIE, including incorporating JIE technical standards into the acquisition of the Navy Enterprise Networks as those standards are defined. In parallel, the Navy is setting internal technical standards for implementation of a Defense in Depth functional architecture across all our systems commands and networks, afloat and ashore – from standard desktop services to combat and industrial control systems. Additionally, the Navy is transitioning along with the rest of DoD to the Risk Management Framework, which is drawn from a solid basis using National Institute of Standards and Technology practices. Most importantly, we are integrating ways to better understand operational cybersecurity risk and defensive posture throughout an information system's life cycle. Operations in cyberspace are highly dynamic - we can only achieve a truly defensible architecture by investing in automation of the collection, integration, and presentation of data. This continuous monitoring is critical to our understanding of how consistently our systems are properly configured in accordance with standards. Only then can operational commanders make cyber maneuver decisions with confidence that they will deliver the intended results.

Together, these actions will help us to truly build cybersecurity and resilience in at the beginning of system development and avoid the pitfalls associated with trying to bolt it on at the end.

The Joint Information Environment's Joint Regional Security Stacks will become part of our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that Joint Regional Security Stacks (JRSS) v2.0 will be the first increment connected to the Navy Enterprise Networks. Accordingly, the Department of Navy is planning to consolidate under JRSS 2.0 as part of the technical refresh cycle for NMCI when JRSS meets or exceeds existing Navy capabilities. Integrating the Navy Enterprise Network with the Joint Information Environment's Joint Regional Security Stacks will allow shared visibility into the boundary capabilities for Navy and DOD integrated DODIN.

For our part, U.S. Fleet Cyber Command is operationally focused on continuously improving the Navy's cyber security posture by reducing the network intrusion attack surface, implementing and operating layered defense in depth capabilities, and expanding the Navy's cyberspace situational awareness.

Create Cyber Situational Awareness

Just like any other domain, success in cyberspace requires awareness of both ourselves and our enemies: it requires that we constantly monitor and analyze Navy platforms within both the classic maritime system and global information system. To succeed, we must understand both side's vulnerabilities and the potential consequences within both systems. To that end, we work to mature our abilities to detect, analyze, report, and take action in and through our Networks. The Navy has started down the acquisition path to expand our Navy Cyber Situational Awareness (NCSA) capabilities with a more robust, globally populated and mission-tailorable cyber common operating picture (COP). Additionally, we are working with our SPAWAR and NAVSEA acquisition partners to improve the network sensor information we can collect across our platforms into a single dedicated big data analytics platform that will bring with it a new level of fidelity and agility to our warfighting. This data strategy will enable us to work seamlessly with all DoD network operations and maritime operations data. The SHARKCAGE platform will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of machine learning and artificial intelligence to harness existing knowledge more rapidly. Building cyber situational awareness from the maritime tactical edge back, will bring with it a superior Joint warfighting force that will be capable of maneuvering through the electromagnetic spectrum and fight resiliently in the age of informationalized warfare.

U.S. Fleet Cyber Command Operational Forces

Status of the Cyber Mission Force

The Cyber Mission Force is designed to accomplish three primary missions: National Mission Teams will defend the nation against national level threats, Combat Mission Teams to support combatant commander priorities and missions, and Cyber Protection Teams to defend Department of Defense information networks and improve network security.

Navy and other cyber service components are building these teams for U.S. Cyber Command by manning, training, and certifying them to the U.S. Cyber Command standards. Navy teams are organized into existing U.S. Fleet Cyber Command operational commands at cryptologic centers, fleet concentration areas, and Fort Meade, depending upon their specific mission. Navy is responsible for sourcing four National Mission Teams, eight Combat Mission Teams, and 20 Cyber Protection Teams as well as their supporting teams consisting of three National Support Teams and five Combat Support Teams.

The Navy is currently on track to have full operational capability for all 40 Navy-sourced Cyber Mission Force Teams in 2018. As of 1 April 2017, we had 26 teams at final operating capability. We are in the process of manning, training, and equipping our teams to be FOC ahead to the October 2018 deadline. Additionally, by October 1st of this year, 298 cyber reserve billets will augment the Cyber Force manning plan.

Over the past year, we have focused on the integration of our Fleet's efforts, capacity and capabilities across the Navy and Joint force. In my role as the Joint Force Headquarters-Cyber commander aligned to U.S. Pacific Command this was an area where organizationally we have recently made progress. As a JFHQ-C Commander, I required an extension of my staff at PACOM to integrate cyberspace planning and force employment into Geographic Combatant Command operations alongside forces from other domains. So in February of this year, I organized my Cyber Mission Force teams in Hawaii to form an interim Cyber Forward Element as a one-stop-shop for full spectrum cyberspace operations in support of PACOM until permanent manning is available to support the Geographic Combatant Command. This Fleet Cyber Command-Forward Element is not a new command, but rather an extension of my staff to provide Offensive and Defensive Cyberspace planning to PACOM on a permanent basis. Our planning with PACOM must be robust enough to create cyber support plans that are integrated into their operational plans. This required a staff that is fully embedded into the supported daily battle rhythm processes while relying upon reach back to, and support from, my main staff at the Headquarters. This forward element has already improved relationship with PACOM in the short time they have been established, and it allows me to have the functionality and capacity I require to effectively C2 my operational Cyber Forces, which include three USAF CMF teams and two US Army CMF teams, as well as my Navy Cyber Mission Forces.

Reserve Cyber Mission Forces

Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve Cyber Mission Force Integration Strategy that leverages our Reserve Sailors' military and civilian skills and expertise to maximize the Reserve Component's support to the full spectrum of cyber mission areas. Based on this mission analysis, we like other services see the maximum value from our Reserve element within the high-priority Defensive Cyber Operations area. Accordingly the 298 Reserve billets, of which the final phase will come into service in October, are being individually aligned to Active Duty Cyber Protection Teams and the Joint Force Headquarters-Cyber. Each of these Navy-sourced teams will maximize its assigned Reserve Sailors' particular expertise and skill sets to augment each team's mission capabilities, rather than as a one-for-one replacement of team workroles. In this way, we can ensure access to the unique skillsets our Reserve Sailors bring to the fight, while at the same time building a cadre of highly trained personnel that can be called on for surge efforts now and in the future.

As our Reserve Cyber billets are fully manned and these personnel trained over the next few years, we will continue to assess our Reserve Cyber Mission Force Integration Strategy and adapt as necessary to develop and maintain an indispensably viable and sustainable Navy Reserve Force contribution to the Cyber Mission Force.

Recruit and Retain

In FY2016, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in FY2017. Currently authorized special and incentive pays, such as the Enlistment Bonus, should provide adequate stimulus to continue achieving enlisted accession mission, but the Navy will continue to evaluate their effectiveness as the cyber mission grows.

Today, Navy Cyber Mission Force (CMF) enlisted ratings (CTI, CTN, CTR, IS, IT) are meeting retention goals. Sailors in the most critical skill sets within each of these ratings are eligible for Selective Reenlistment Bonus (SRB). SRB contributes significantly to retaining our most talented Sailors, but we must closely monitor its effectiveness as the civilian job market continues to improve and the demand for cyber professionals increases. Additionally, we have requested, and anticipate approval of Special Duty Assignment Pay (SDAP) for one of most critical skills sets, Interactive On-Net Operators (IONs). SDAP would provide a monthly stipend of $200-$500.

Cyber-related officer communities are also meeting retention goals. While both Cryptologic Warfare (CW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining Officers in these communities at 93 percent overall. Both CW and IP are effectively-managing growth through direct accessions and through the lateral transfer process, thereby ensuring cyber-talented officers enter, and continue to serve.

With respect to the civilian workforce, we currently have 91 civilian positions within the Cyber Mission Force. Forty-seven of these positions are filling various workroles throughout the CMF and 44 are our Computer Scientists/Tool Developers. Currently we have 27 of the 47 positions filled throughout CMF; are in the initial recruitment phase for our 44 Tool Developers and have made 13 other selections to date. We are aggressively hiring to our civilian authorizations consistent with our operational needs and fully supported by the Navy's priority to ensure health of the cyber workforce. We have also initiated a pilot internship program with a local university to recruit skilled civilian and military cyber workforce professionals. Navy will measure the success of this approach as a potential model to harness the nation's emerging cyber talent. Our primary challenges in recruiting are the current compensation allowable and competition with industry and other DoD entities. With this in in mind, we are now offering various incentives to potential candidates which includes higher step (step 7) on the GS pay scale, 10% of salary as a one-time recruitment incentive, 10% of salary for relocation expenses, and several years of assistance in student loan payback (5K per year). Even with these incentives, we are not competitive with industry or NSA.

As the economy continues to improve, we expect to see more challenges in recruiting and retaining our cyber workforce.

Educate, Train, Maintain

To develop officers to succeed in the increasingly complex cyberspace environment, the U.S. Naval Academy offers introductory cyber courses for all freshman and juniors to baseline knowledge. Additionally, USNA began a Cyber Operations major in the fall of 2013, and in 2016, 27 Midshipmen were the first to graduate with the degree. This year, 46 Midshipmen will graduate with the degree and 72 have entered the major. Furthermore, the Center for Cyber Security Studies harmonizes cyber efforts across the Naval Academy.

Our Naval Reserve Officer Training Corps' (NROTC) program maintains affiliations at 51 of the 180 National Security Agency (NSA) Centers of Academic Excellence (CAE) at colleges around the country. Qualified and selected graduates can commission as Cryptologic Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Warfare Community.

For graduate-level education, the Naval Postgraduate School offers several outstanding graduate degree programs that directly underpin cyberspace operations and greatly contribute to the development of officers and select enlisted personnel who have already earned a Bachelor's Degree. These degree programs include Electrical and Computer Engineering, Computer Science, Cyber Systems Operations, Network Operations and Technology, and Applied Mathematics, Operations Analysis, and Defense Analysis. Naval War College is incorporating cyber into its strategic and operational level war courses, at both intermediate and senior graduate-course levels. The College also integrates strategic cyber research into focused Information Operations (IO)/Cybersecurity courses, hosts a Center for Cyber Conflict Studies (C3S) to support wider cyber integration across the College, and has placed special emphasis on Cyber in its war gaming role, including a whole-of-government Cyber war game under active consideration for this coming summer or fall.

With respect to training of the Cyber Mission Force, U.S. Cyber Command mandates Joint Cyberspace Training & Certification Standards, which encompass procedures, guidelines, and qualifications for individual and collective training. U.S. Cyber Command with the Service Cyber Components has identified the advanced training required to fulfill specialized work-roles in the Cyber Mission Force. Most of the training today is delivered by U.S. Cyber Command and the National Security Agency in a federated but integrated approach that utilizes existing schoolhouses and sharing of resources. The Navy is unified in efforts with the other Services to build Joint Cyber training capability, leveraging Joint training opportunities, and driving towards a common standard. These training events are not only aimed at the individual Sailors, but also provide operational team certifications and sustainment training. Once certified, our team training is maintained throughout the year via several key unit level exercise events which allow individuals and the collective team to demonstrate required skills against simulated adversaries.

Future Cyber Workforce Needs

The Navy's operational need for a well-trained and motivated cyber workforce (active, reserve and civilian) will continue to grow in the coming years as we build out the balance of Cyber Mission Force.

We will depend upon commands across the Navy to recruit, train, educate, retain and maintain this workforce including the Chief of Naval Personnel, Navy Recruiting Command, Naval Education and Training Command and Navy's Institutions of Higher Education (United States Naval Academy, Naval Postgraduate School, and Naval War College.) Additionally, the establishment of Naval Information Forces (NAVIFOR) in 2014 as a Type Commander has made a significant impact in generating readiness for cyber mission requirements. NAVIFOR works closely with the Man, Train, and Equip organizations across the Navy to ensure that U.S. Fleet Cyber Command and other Information Warfare operational commands achieve proper readiness to meet mission requirements. Navy is now enhancing the NAVIFOR capability with the establishment of the Naval Information Warfare Development Command (NIWDC), newly established in 2017, to advance the maturing of Information Warfare, including cyberspace operations, doctrine, training, Tactics, Techniques & Procedures (TT&P).

Fleet Readiness

The Navy's 2018 budget continues to prioritize readiness alongside the investments necessary to sustain an advantage in advanced technologies and weapons systems. Ensuring the cyber resiliency of networks is part of maintaining the readiness of warfighting platforms.

The budget continues funding to train and equip Cyber Mission Forces, provides investments in Science and Technology and information assurance activities to strengthen our ability to defend the network. To maintain our advantage in advanced technologies and weapons, funding is provided for engineering to improve control points and boundary defense across Hull, Machinery & Electrical, Navigation and Combat Control Systems and for Cyber Situational Awareness.

The Navy is requesting increased investment in Defensive Cyber Operations forces ability to detect adversary activities and analyze cyber attacks against Maritime Cyber Key Terrain (CKT) and to integrate all-source intelligence and Navy data to assess adversary capabilities. The goal of the investments are to improve the Navy's capacity to deliver to Operational Commanders, cyber situational awareness at all layers of the IT infrastructure and provide a cyber common operational picture (COP) at our Fleet Maritime Operations Centers.

Funding for training is necessary to ensure operator proficiency as Fleet systems are modernized and become more complex. I believe the Navy's ability to appropriately fund training of our operators in these new technologies will improve operational readiness.

Summary

Your Navy has recognized that we have not only witnessed a changing and evolving cast of competitors, but the very nature of our strategic environment has changed. We are witnessing a return to great power competition. In the Chief of Naval Operations' Campaign Design for Maritime Superiority, he points to the rise of the global information system and the rate of technological creation and adoption as two of the dominant global forces shaping the maritime environment our Navy must operate, and if called upon, fight in. Cyberspace will be a contested environment and we cannot take freedom of maneuver for granted. It is clear that our reliance on our networks will not diminish as we push toward distributed maritime operations.

U.S. Navy freedom of action in cyberspace is necessary for all missions that our nation expects us to be capable of carrying out including winning wars, deterring aggression and maintaining freedom of the seas.

There is no individual success, at least not in the long term. We will succeed by leveraging our strengths and shrinking our vulnerabilities. Operational success will be built upon a strong network of partners (DoD, Interagency, Industry and Academia), a resilient, defensible infrastructure, and complemented by our greatest resource and asymmetric advantage – our people.

Thank you again for this opportunity to update you on great work being done by the men and women of Fleet Cyber Command, Tenth Fleet and the U.S. Navy. I look forward to working closely with members of the subcommittee on cybersecurity and appreciate your support of these cyber investments included in the Navy's 2018 budget request. I'm happy to take your questions.

RECORD VERSION

STATEMENT BY

LTG PAUL M. NAKASONE

COMMANDING GENERAL U.S. ARMY CYBER COMMAND

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY

COMMITTEE ON ARMED SERVICES

UNITED STATES SENATE

FIRST SESSION, 115TH CONGRESS

U. S. ARMY CYBER POSTURE

MAY 23, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE

COMMITTEE ON ARMED SERVICES

Introduction

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, thank you for your continued support of U.S. Army Cyber Command (ARCYBER) and our efforts to operationalize cyberspace for our Army. It is an honor to address this subcommittee on behalf of the dedicated Soldiers and Army Civilians of ARCYBER who work every day defending the Nation in cyberspace. This testimony focuses on ARCYBER's ongoing progress in the areas of Operations, Readiness, Resources, Training, and Partnering,

The Army Cyber Enterprise has made significant progress operationalizing cyberspace since my predecessor's testimony before the Subcommittee on Emerging Threats and Capabilities in April 2015. Since then, Army Cyber Command has completed the initial build of the Army's Cyber Mission Force (CMF). All 41 Active Component Army teams are at Initial Operational Capability or better and all are on track to be at Full Operational Capability by the end of September 2017, a year ahead of U.S. Cyber Command's (USCYBERCOM's) mandated timeline. The Army is now building an additional 21 Reserve Component (RC) Cyber Protections Teams (CPTs), trained to the same Joint standards as the Active Component teams, which will be integrated into the Army's Total Cyber Mission Force.

Additionally, the Cyber Center of Excellence (Cyber CoE) graduated its first class of Cyber Branch Lieutenants in May 2016; its first class of Cyber Warrant Officers in March 2017; and began training its first class of new cyber enlisted recruits also in March 2017. The Cyber CoE trained a total of 582 Cyber Branch Soldiers during Fiscal Year (FY) 2016 and is scheduled to train another 1,200 Soldiers during FY2017. The Army cyber force now includes 2,331 Soldiers with career fields that include Cyberspace and Electronic Warfare operations. (557 Officers, 305 Warrant Officers, and 1,469 Enlisted). Furthermore, the Cyber Center of Excellence recently published Field Manual (FM) 3-12, Cyberspace and Electronic Warfare Operations, which provides overarching doctrinal guidance and direction to the Army for conducting cyberspace and electronic warfare (EW) operations in unified land operations. Army Cyber Command is continuing its Cyber Electromagnetic Activity (CEMA) Support to Corps and Below pilot program and is now working with our Army partners to determine

enduring support requirements at the combat training centers and ultimately, cyber force structure and requirements at the tactical level within the Army.

The Army also recently made several important organizational changes to the Army Cyber Enterprise to improve our ability to conduct cyberspace operations and support Joint and Army commanders. First, the Army elevated ARCYBER to an Army Service Component Command (ASCC) ensuring ARCYBER receives the same level of resourcing as other ASCCs supporting Combatant Commanders. Second, the Army reassigned the Network Enterprise Technology Command to ARCYBER to better align responsibilities and authorities to support USCYBERCOM and Army requirements and to better align roles and responsibilities for the Army's portion of Department of Defense Information Network (DoDIN). Third, the Army established an Army Cyber Directorate within the Headquarters Department of the Army (DAMO-CY), to advocate and coordinate cyberspace doctrine, policy, organization, and resourcing issues within the Pentagon. The DAMO-CY Directorate joins the Army's Cyberspace Tetrad that includes the Army Cyber Institute, the Cyber Center of Excellence, and ARCYBER. Finally, the Army broke ground for the new Army Cyber Headquarters Complex at Fort Gordon, Georgia in November 2016, and has committed to future investments in new Cyber Center of Excellence facilities in which to train our Soldiers.

Army Cyber Command is building on the Army's past progress while focusing on three key priorities: Aggressively Operating and Defending Our Networks, Data, and Weapons Systems; Delivering Effects Against Our Adversaries; and Designing, Building and Delivering Integrated Capabilities for the Future Fight. Today, Army cyberspace forces, including Reserve Component forces, are improving the Army's cybersecurity posture; protecting and defending Army and DoD networks, systems, and critical infrastructure; supporting Joint and Army commanders; and engaging our adversaries in cyberspace every day.

While ARCYBER has made significant advances building the Army's cyberspace capacity and capabilities over the past six years, our progress will be overshadowed by the inability to maintain overmatch against near-peer competitors due to a lack of sustained, long-term, and predictable funding. As evidenced by the recent threat of a year-long continuing resolution, the Army would have been forced to stop funding for

Army National Guard Cyber Protection Teams. This would have slowed the Army's ability to fulfill the congressional mandate to integrate Army Reserve Component Cyber Protection Teams into the Cyber Mission Force. The Continuing Resolution delayed the fielding of the Joint Persistent Cyber Training Environment leading to greater costs and delays in building DoD cyber capability and capacity. Further, a major impediment to improving Army cybersecurity through network modernization has been a lack of predictable funding. The Army needs an end to the year-after-year continuing resolutions and relief from the Budget Control Act of 2011 to help restore readiness levels and build force capacity and capabilities to counter emerging threats, including those in cyberspace.

Operations

Cyberspace operations encompass three interrelated areas: Department of Defense Information Network (DoDIN) operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). Army DoDIN operations are the most complex, most important mission ARCYBER conducts. They include building, operating, defending, and maintaining the Army's portion of the DoDIN. Our five Regional Cyber Centers conduct DoDIN operations around-the-clock, serving as the Army's Cybersecurity Service Providers (CSSP). The Army continues to work with U.S. Strategic Command and the Joint Chiefs of Staff to realign our DoDIN force structure in accordance with the 2017 NDAA and to gain better command and control over the global cyber theater.

To support DoDIN operations and improve cybersecurity, the Army is building a more reliable, secure and ready network through system hardening and modernization. A new effort between ARCYBER and the Army's Chief Information Officer/G6 (CIO/G-6), called the "DoDIN Initiatives" is key to our system hardening efforts. This initiative focuses on information sharing to include tracking progress, identifying gaps and issues with policies or resources to unify the way ahead for the Army.

The greatest challenge and most critical aspect of a ready, secure, and available network is a modern and resilient infrastructure. In the Army we refer to our efforts to achieve this as Network Modernization (NETMOD). The Army's NETMOD efforts

include: Joint Regional Security Stack (JRSS) migration, Multiprotocol Label Switching upgrades, and Installation Campus Area Network upgrades. The Army is partnering with the U.S. Air Force and the Defense Information Systems Agency (DISA) in deploying JRSS to centralize the Army's existing perimeter security infrastructure. The Army has completed the upgrade of 22 of its installation's network infrastructure and migrated them to the JRSS. The Army continues to upgrade its installation's network infrastructure and migrate within the JRSS. The current plan is a phased approach upgrading installations within CONUS, Southwest Asia and European Theater, followed by the Pacific Theater, to include Korea and Alaska, with main installations being complete by fourth quarter FY 2019. At the next layer of Network Modernization, DISA has completed upgrading the Army's fiber optics and Multiprotocol Label Switching circuits of 18 installations and is focused on completing seven more sites this year. These initiatives, in combination with the increased capabilities of our operational force, will enable stronger cyber protection, detection, and response to cyber threats across the DoDIN.

In order to take advantage of these DoD network improvements at the Army Base/Post/Camp/Station level, we must modernize our own infrastructure through Installation Campus Area Network upgrades. This is an enduring effort to stay current with technological advances. A top DoD and Army priority, aimed at hardening our endpoints and infrastructure, is the implementation of assuring appropriate upgrades to our operating system and applications. The DoD-managed common secure host baseline will allow the Army to strengthen our cybersecurity posture while concurrently streamlining the IT operating environment. Additional end-point efforts include one focused on security and one on management. All these efforts combined enable us to provide the Army with a ready, secure, and available network that supports Mission Command and supports the projection of combat power. While the Army's investment in network hardening and modernization has paid dividends, ARCYBER would benefit from predictable funding for DoDIN operations. A lack of predictable funding is the major impediment to improving Army cybersecurity through network hardening and modernization.

In addition to building a more defendable network, ARCYBER conducts both passive and active Defensive Cyberspace Operations to protect and defend the Army portion of the DoDIN. Defensive Cyberspace operations are mission focused, prioritized on critical assets, and threat specific. Our Cyber Protection Brigade, (CPB) and its Cyber Protection Teams, conduct critical active defense of the DoDIN. The CPB's ability to conduct active recon for advanced persistent threats distinguishes them from the functions of a CSSP that is dedicated to protecting our network against known threats. Our CPTs are a maneuver element in cyberspace that reinforce the protection mission of a CSSP based on analysis of the mission relevant cyber terrain and threats provided by national intelligence and our own internally-collected cyber intelligence. The CPB also helps protect and defend the Army's critical infrastructure and support both national requirements and Joint and Army commanders around the globe. The Brigade includes 900 Soldiers and Civilians who make up 20 Active Component Cyber Protection Teams.

Importantly, our Cyber Protection Brigade supports Army Mission Assurance, providing Critical Infrastructure Risk Management assessments to identify potential vulnerabilities and threats. The CPB works with Department of the Army, Army Material Command, U.S. Army Corps of Engineers (USACE), and other stakeholders in an Army-wide approach to ensuring the cybersecurity of critical Army systems and infrastructure, including the Nation-wide systems of dams and hydroelectric plants USACE manages. Our CPTs deploy worldwide (including austere environments) with mobile capabilities within hours of notification, employing platforms and tools across the breadth and depth of our network. Our teams also provide "reach-back" support to deployed forces that allows us to put the right person on the right task at the right time.

The pace of operations and dynamic nature of the threats means our cyberspace forces engage with our adversaries in cyberspace as they are being built, usually before they achieve full operational capability. Both defensive and offensive Army cyber forces are rapidly maturing and building credibility with our combatant commanders in warfighting operations every day; continually learning and innovating their tactics, techniques, and procedures against determined, adaptive and aggressive adversaries.

Our Army Cyber Mission Forces execute Offensive Cyberspace Operations, to

project power by the application of force in or through cyberspace, under the authorities of Combatant Commanders and USCYBERCOM. Established by USCYBERCOM in June 2016 and commanded by the ARCYBER Commander, JTF-ARES is a Joint cyber operational headquarters providing cyber capabilities in support of US Central Command's counter-ISIS operations. The Task Force has brought cyber out of the shadows and successfully demonstrated the value and capabilities of cyberspace operations to the Joint Force when integrated as part of broader coordinated military effort.

Readiness

Readiness is the Army's overriding priority. To support readiness, the Army is building 62 Total Force CMF teams, all trained to the same joint standards, to support Joint and Army commanders. The 41 Active Component (AC) teams are built and conducting cyberspace operations supporting real world operations today. They are also defending DOD networks, protecting Army weapons systems, and defending critical infrastructure. Currently, 33 of the Army's 41 AC teams are at full operational capability, while eight teams remain at initial operating capability. By 30 September 2017, all 41 teams will be fully operational. With the completion of the CMF build, the Army is now progressing from building its cyber force to measuring the readiness of this force. Army Cyber Command is working with USCYBERCOM to implement metrics to measure CMF readiness through the Defense Readiness Reporting System.

Reserve Component Cyber Protection Teams

The Army's Reserve Component (RC), comprised of the Army National Guard (ARNG) and U.S. Army Reserve (USAR), is critical to Army readiness. The RC is building 21 Cyber Protection Teams (11 ARNG, 10 USAR) creating a Total Force solution, all trained to the same Joint standards as the Active Component. As required under Section 1651 of the National Defense Authorization Act of Fiscal Year 2017, the Army is implementing a Total Army RC cyber strategy to integrate the 21 RC CPTs into the Army's Cyber Mission Force to support Joint and Army cyberspace requirements.

Network Readiness

Network readiness is a component of Army readiness. Today the Army and the Joint Force depend on unimpeded access to the DoDIN for everything from business operations to missile defense. The network is now not only a critical enabler, but also an operational capability for cyberspace operations, vital to our operational readiness, and therefore important to measure. The Army currently measures network compliance with policy, regulation, and law through the Cybersecurity Scorecard, Command Cyber Readiness Inspections, and Command Cyber Operational Readiness Inspections.

Army Cyber Command partnered with JFHQ-DoDIN to execute the next evolution of Cybersecurity inspections under the Command Cybersecurity Operational Readiness Inspection (CCORI), to replace the Command Cyber Readiness Inspection. The CCORI moves cybersecurity inspections from a compliance-based systems inspection to a risk-based Operational Commander's Mission focused inspection. The CCORI highlights the risks to operational missions within a Command by employing active external and internal threat actors against a Commander's mission critical systems. The CCORI outcome provides an operational risk measurement to mission by mission critical task and a system to assist Commanders in prioritizing cybersecurity resources.

The DoD Cybersecurity Scorecard has brought basic cybersecurity hygiene to the forefront at the DoD level and has forced the Army to prioritize basic cybersecurity requirements. The Army has made strides towards remediating identified critical vulnerabilities across the enterprise and capturing the effectiveness of remediation efforts. The Army continues to work with DoD CIO to refine the Scorecard metrics to move from cybersecurity compliance to risk-based scorecard measurements to provide a mission assurance focus.

Training

Army Cyber Mission Force training has three key components: individual, collective, and mission rehearsal. Individual training is focused on formal training, work role specific training, and job-specific qualification and certification training conducted at

the work center. Individual training focuses on building individual core competencies, proficiencies, skills and knowledge necessary to accomplish assigned tasks.

During collective training, team members train in realistic environments and to relevant threats. Army CMF teams will conduct approximately 80 collective training events, throughout FY2017 to ensure they are fully trained to USCYBERCOM joint standards. Live, virtual, and constructive scenarios are used to ensure that training is holistic, repeatable, and measureable. Collective training is used to increase team proficiency, certify teams for operations, and allow leaders to build trust and confidence within their teams. Participation in USCYBERCOM exercises, CYBER GUARD and CYBER FLAG, helps achieve certification or revalidation.

Mission rehearsal training events are conducted to ensure that leaders understand their missions, the threats and risks they will face, and are prepared for contingencies. Army CMF teams are scheduled to conduct 48 internal mission rehearsal type training events during FY17 in order to build team proficiency, preparation for recertification/revalidation and mission preparations to support operations. These events occur at home station, training centers, and in deployed areas. Army Cyber Command teams also participate with Joint, interagency and coalition partners through Combatant Command training exercises for operational mission sets.

The Cyber Center of Excellence (CCoE) located at Fort Gordon, Georgia, operates the Army's Cyber School and trains Army Cyber Branch Soldiers and members of the other Services. All three cohorts, officer, warrant officer and enlisted, conclude their training by participating in Joint exercises ensuring they are well prepared to support Army units at all levels.

The CCoE is explicitly charged with incorporating Joint standards into the curriculum. The Joint Cyber Training and Certification Standards set work roles and training to a single joint standard applied across multiple Services building like teams. It unites the Services' efforts to train and certify their respective CMFs to perform in a joint environment. The CCoE focuses on individual training and has begun training key USCYBERCOM J7 pipeline courses including Cyber Common Technical Core (equivalent to Intermediate Cyber Core), CPT Core Methodologies, Cyber Operations Planner Course, and the Joint Advanced Cyber Warfare Course. Since the Army

established the Army Cyber Branch, Career Field 17 in September 2014, the CCoE has trained 1,500 Cyber Branch Soldiers. Fiscal Year 2018 will see more Soldiers trained in the Army 17-series pipeline, and Soldiers will continue to attend Military Occupation Specialty qualification courses. Graduates of these courses will provide a steady stream of trained 17-series Soldiers, thus decreasing the individual training burden on units and improving force readiness.

Establishing a Persistent Cyber Training Environment (PCTE) is central to training the Joint Cyber Mission Force and maintaining high levels of proficiency. In support of section 1645 of the FY16 National Defense Authorization Act, DoD designated the Army as the acquisition authority for the PCTE. The PCTE will provide high quality scenarios and event management for individual, team/collective, and mission rehearsal training for all four Services and USCYBERCOM. At maturity, we envision the DoD Joint PCTE platform as a constellation of federated, interoperable common training capabilities—enabling training from individual competencies at the team, unit, group and force training levels; including exercises, tactics, techniques, and procedures development, up to mission rehearsal.

CEMA Support to Corps and Below

In 2015 the Army initiated a Cyber Electromagnetic Activities (CEMA) Support to Corps and Below (CSCB) pilot program. The CSCB effort serves four primary purposes: Define what offensive and defensive cyber effects to integrate at the echelon Corps and below; Determine expeditionary Defensive Cyberspace Operations, Offensive Cyberspace Operations, Electronic Warfare, and Information Operations capability for deployed tactical forces; Leverage Combat Training Centers (CTCs) and operational deployments to inform CEMA Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, and Facilities development (DOTMLPF); and Determine the enduring CEMA environment at CTCs.

Army Cyber Command recently completed its sixth iteration of the CSCB pilot and will conduct another one in June 2017. Lessons learned from the pilot program are helping to inform CEMA requirements across the Army's DOTMLPF and Policy development. Army Cyber Command is now working with DAMO-CY to determine

enduring support requirements at the CTCs that would routinely embed cyber teams in combat brigades during their CTC rotations to continue providing realistic training for our cyber operators, Army units, and commanders.

The Cyber Center of Excellence published the Army's first Cyberspace and Electronic Warfare doctrine in April 2017, FM 3-12, Cyberspace and Electronic Warfare Operations. Army FM 3-12 is nested in joint cyberspace and EW doctrine and provides the doctrinal context to understand the fundamentals of integrating and synchronizing cyberspace and EW operations. Through the planning and synchronization of cyberspace and EW operations, Army cyberspace forces integrate CEMA functions and capabilities across warfighting functions, defend the network, and provide critical capabilities for commanders at all levels during unified land operations.

Resources

People are the most important resource in cyberspace. To ensure we will prevail over all adversaries in the cyber domain, the Army is committed to executing a vigorous cyber talent management program built on four talent management pillars: recruit, develop, employ, and retain talent. The Army achieved a major milestone in cyber talent management in 2014 when it became the first service to launch a dedicated career field (Career Field 17) to centrally manage Soldiers throughout a career in cyberspace operations. This allows the Army to recruit, develop, employ and retain Soldiers specific to cyber skills and operations.

To ensure we continue to maintain high levels of end strength in the cyberspace force, the Army is now implementing several key talent management initiatives to improve recruitment, training, and retention across all components and all Soldier and employee cohorts. First, the Army is developing a direct commissioning program to find highly talented individuals with industry experience and laterally enter them into the force. Second, the Army has initiated a Civilian Cyber-effects Career program. Additionally, ARCYBER is offering opportunities to many members of our force, including the chance to train with industry and opportunities for academic degrees through our Advanced Civil Schooling program. Finally, we are partnering with the U.S.

Digital Service and the Defense Digital Service to help us look internally at our processes and provide an outside perspective from a group of technical experts.

The Army direct commissioning program, authorized under section 509 of the National Defense Authorization Act for Fiscal Year 2017, will bring in talented individuals with highly technical skills at ranks of increased pay and responsibility. The Army hopes to attract individuals with skills that include computer programming, mathematics, network operations, cryptology, data science, or nanotechnology. Beyond technical knowledge, we're looking for people with aptitude, dedication, and desire for mission- and team-oriented problem solving.

The Army recently approved the new Civilian Cyberspace-effects Career Program which will unify all Cyberspace Effects civilian employees into a single cross-disciplinary model for training and management of multiple Occupational Specialties This new career program will align Army Civilians performing Cyberspace Effects with their Soldier counterparts in Cyber (17 series). The Cyberspace Effects work role qualifications will be governed by USCYBERCOM Joint training requirements. The Department of Defense is also finalizing work on a new Title 10 excepted service civilian cyber program similar to the civilian intelligence career program.

Integration of Electronic Warfare

To better manage its Electronic Warfare Soldiers, in 2014, the Army approved the integration of cyber effects and electromagnetic spectrum operations into the Army's new Cyber Branch. The Army Cyber Center of Excellence is developing a phased approach to convert Soldiers in the Army Electronic Warfare Military Occupational Specialty, Functional Area 29, into the Cyber Branch beginning in FY2018. Concurrently, the Army is analyzing and developing an integrated Electronic Warfare, Cyber, and Signals Intelligence capability that will be capable of sensing and disrupting adversary systems that operate within the electromagnetic spectrum while providing Electronic Protection to Army systems.

Equipping the CMF

Army Cyber Command is focused on equipping the Cyber Mission force with integrated capabilities and organic development environments. To ensure that our capabilities are dynamic and evolving to counter future threats we are focusing on two mission areas of development: Defensive Cyberspace Operations and Offensive Cyberspace Operations. These two areas include the development of a scalable Big Data platform, building advanced cyber analytics, development operations support for payload development, malware analysis, threat detection, and infrastructure.

The Army has also invested in developing home station and deployable platforms that will provide our Defensive Cyber Operations CPTs with systems to support the defensive force with tools to prevent, mitigate, and recover systems at risk from cyber threats at near real-time speed. We are sprinting to build and institute a complete OCO architecture purpose built to enable operational agility, reduce training complexity, and maximize our ability to present multiple dilemmas to our adversaries. This effort includes the integrated build of a tool developer environment, operational infrastructures and foundational tools that support current and future mission requirements for the Army's Total Cyber Mission Force.

Road to Fort Gordon, Georgia

Army Cyber Command Headquarters is currently split-based at Fort Belvoir, Virginia, Fort Meade, Maryland, and Fort Gordon, Georgia, in overcrowded and inadequate facilities. The Army has begun building a $180 million, state-of-the-art Army Cyber Headquarters Complex alongside National Security Agency-Georgia at Fort Gordon, Georgia. Occupation of the new facility is planned to begin in 2020 with the full transition of ARCYBER Headquarters to Fort Gordon expected no later than 2022. The colocation of these operational forces with the Cyber Center of Excellence at Fort Gordon, will create significant synergy, allowing for the immediate incorporation of lessons learned and operational knowledge into our training curriculum.

Partnering

Partnerships are crucial to staying ahead of our adversaries in cyberspace. The Army Cyber Enterprise partners with industry, academia, the intelligence community, and our interagency partners to share information and find solutions to cybersecurity challenges. The Army is also adapting its acquisitions systems and reaching out to smaller “non-traditional” companies on the cutting edge of technology to keep pace with cyber threats.

To better leverage private sector and academic partnerships the Army has undertaken initiatives under DoD umbrella programs such as Defense Innovation Unit Experimental, or DIUX, the Defense Digital Service, and “Hacking 4 Defense” efforts to further reach-out and collaborate with non-traditional partners. Through DIUX, Active and Reserve Soldiers collaborate with private industry in Silicon Valley to quickly leverage commercial innovations into acquisition solutions.

During November-December 2016, working with a private sector partner, the Army launched the "Hack the Army" initiative, to crowdsource cyber vulnerabilities of selected Army Websites and databases. The Army paid a modest “bug bounty” to selected ethical hackers which helped the Army discover dozens of vulnerabilities. Army Cyber Command subsequently shared these vulnerabilities with the Intelligence Community.

To help foster innovation and partnerships between the Army Cyber Enterprise and the greater cybersecurity community, the Army Cyber Institute (ACI) at West Point serves as the Army's bridge to academia, government, and the private sector. The ACI facilitates state, local, public, and private partnerships in the cyber domain across the United States and Internationally. The ACI creates relationships that build capacity within major metropolitan centers and through exercises designed to integrate all levels of national cyber response. For example, in October 2016, ACI partnered with the NATO Cooperative Cyber Defence Centre of Excellence to develop a robust international conference on cyber conflict that will be repeated in November 2017.

In all partnering activities, the Army Cyber Enterprise is preparing for a future that includes machine learning, intelligent systems, virtual/augmented reality, and Big Data; in conjunction with ubiquitous computing, autonomous, and semi-autonomous robotic systems. The Army's partnering activities help prepare forces that bridge the military-civilian and peacetime-wartime boundaries needed to deal with the gray space nature of cyber conflict.

Conclusion

The Army has made significant progress operationalizing cyberspace since it established Army Cyber Command a little more than six and a half years ago. The Army now has 41 Cyber Mission Force teams and is building an additional 21 RC teams. The Army also has a Cyber Branch to support Cyber Soldiers throughout their careers and will soon have a Civilian Cyberspace Effects Career Program, tailored to our unique mission. The CyberCoE is training Cyber Soldiers and preparing to integrate the Electronic Warfare force into the cyber career field. We have broken ground on the Army Cyber Headquarters Complex on Fort Gordon, Georgia which will transform the Fort Gordon region into a cyberspace hub for the Army and the Nation. And the Army has also implemented important organizational changes to the Army Cyber Enterprise that enhance our ability to conduct cyberspace operations and support Combatant and Army commanders. These accomplishments have happened because the Army, with the support of Congress, has made protecting and defending the Nation in cyberspace a priority.

Our investments in the Soldiers and Civilians who carry out our critical mission are paying off. Today our teams are actively protecting and defending Army and DoD networks; securing Army weapons platforms; protecting critical infrastructure; and conducting operations against global cyber threats. These teams are delivering effects against our adversaries, giving our ground commanders and the Joint force the competitive advantage they need to win. With the continued support of Congress, the Army will maintain its tremendous momentum in cyberspace, building a more capable, modern, ready force that is prepared to meet any adversary in cyberspace, today and tomorrow.

PRESENTATION TO THE
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY
UNITED STATES SENATE

SUBJECT: Military Cyber Programs and Posture

STATEMENT OF: Major General Chris P. Weggeman
Commander, 24th Air Force and
Commander, Air Forces Cyber

May 23, 2017

Introduction

Chairman Rounds, Ranking Member Nelson, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, along with Vice Admiral Marshall Lytle from the Joint Staff and my fellow Service Cyber Component Commanders. I look forward to discussing the Air Force's progress in advancing full-spectrum cyberspace operations and our contributions to joint operations globally. I have the distinct honor to lead a triple-hatted organization; 24th Air Force, Air Forces Cyber (AFCYBER), and Joint Forces Headquarters (JFHQ) – Cyber AFCYBER. These three-hats encompass service, component, and functional roles, responsibilities, and authorities which I will expand upon shortly. Our headquarters is located at Joint Base San Antonio-Lackland, Texas and we have Airmen and civilians on-mission around the world, diligently increasing our capability to deliver full spectrum cyber effects in support of our joint warfighters.

AFCYBER warriors are operating globally as a maneuver and effects force in a contested domain, delivering cyber 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.

As Commander, 24th Air Force, I report directly to the Commander of Air Force Space Command and am responsible within the Air Force for classic Title 10 organize, train, and equip functions. 24th Air Force also serves as the Cyber Security Service Provider (CSSP) for our Air Force networks and other designated key cyber terrain. Under the AFCYBER hat, I am the Air Force's Cyber Component Commander who presents and employs Air Force cyber forces to United States Strategic Command, delegated to United States Cyber Command. These ready forces plan and execute full-spectrum cyberspace operations across the Air Force portions of the DoD Information Network (DoDIN), and other cyber key-terrain as directed. Finally, under my third hat, as Commander, Joint Forces Headquarters (JFHQ) – Cyber AFCYBER, I lead a United States Cyber Command subordinate headquarters with delegated Operational Control

of assigned cyber combat mission forces employed in a general support role to both United States Strategic Command and United States European Command. We execute assigned cyberspace operations missions through six distinct but inter-related lines of effort—Build, Operate, Secure, Defend, Extend, and Engage, or what we refer to as "BOSDEE".

DEFENSE is our #1 Mission

In our 24th Air Force and AFCYBER roles, we build, operate, secure, and defend the Air Force networks every day to ensure these networks remain available and secure for assigned missions, functions, and tasks. The broader mission includes base infrastructure, business, and logistics systems, as well as mission and weapon systems; in total, providing on-demand capabilities to approximately one million users worldwide. The Air Force CIO designated 24th Air Force as the CSSP for all systems within the Air Force enterprise. In this capacity we are responsible for protecting, monitoring, analyzing, detecting, and responding to malicious cyber activity across the Air Force network. We are working with our Service Staff and Air Force Space Command, to determine resource and manpower requirements to execute this expansive mission-set. Earlier this year, we partnered with the United States Army Research Lab to contract and provide a fee-for-service cyber security framework for system cybersecurity similar to what they are providing the United States Army. This partnership and approach aligns the Air Force CIO delegated cybersecurity responsibilities with our AFCYBER defensive mission forces and capabilities, generating coherent mission coordination and integration across the enterprise.

Cyber Security and Defense in the 21st Century

24th Air Force, in collaboration with our Service staff and Major Commands, developed and began implementation of three transformational efforts which transition our force and Information Technology posture towards a 21st century, Commander and cyberspace operator driven, threat and risk-based mission assurance cyber ecosystem. These three major efforts include; 1) evolving towards the Air Force Information Dominance Platform (AFIDP), 2) maturing and resourcing our Air Force CIO Cyber Squadron Initiative and inherent Mission Defense Teams, and finally 3) the development and fielding of Air Force Material Command's Cyber Resiliency of

Weapons Systems (CROWS) Office capabilities. This last initiative was developed to address last year's NDAA Section 1647 weapon system cyber security mandate. These three major endeavors, deliver a coherent approach to cyber security, cyber defense, weapon system resiliency, and the ever critical "every Airmen a sentry" cyber hygiene culture across our Air Force.

The AFIDP is a network reference architecture designed to smartly divest the costly and manpower intensive network operations, maintenance, and customer-service support demands of our Service's dated, Information Technology infrastructure via outsourcing to commercial and industry partners. This strategy allows us to improve our network while repurposing portions of our legacy Information Technology workforce to deliver essential services, data security, and cyber-based mission assurance. The AFIDP moves the Air Force towards a risk-managed, Network and/or Infrastructure as a Service model (NaaS/IaaS). AFIDP, with Cloud Hosted Enterprise Services, which is currently in operation under the moniker "Collaboration Pathfinder", is securely hosting over 60,000 user accounts across ten bases. This service delivery model will enable improved network performance, reliability and scalability. It also fuels superior cyber security and defense, while generating superior speed, agility and precision of maneuver in, through, and from cyberspace.

The AFIDP roadmap leverages on-going Joint Information Environment (JIE), Joint Regional Security Stack (JRSS) migrations and fielding in close partnership with the United States Army and the Defense Information Services Agency (DISA). All DoD components will ultimately utilize JRRS with the United States Air Force and Army currently undergoing migration. Combatant commands, Coast Guard, and other Defense Agencies are scheduled to begin JRRS migrations later in FY17 and into FY18. To date we have successfully migrated two CONUS regions, to include 170,334 users across 32 bases. JRSS provides state of the art security stacks and capabilities at our Tier-2 gateway boundaries. AFIDP also employs the Automated Remediation and Asset Discovery (ARAD) capability suite.

ARAD is an instantiation of the commercial Tanium product, enabling operators to perform vulnerability management, incident response, system health diagnostics, as well as asset identification and optimization in a matter of seconds to minutes vice days

to weeks using current capabilities. ARAD achieved Initial Operational Capability on the Air Force Network in December 2016, installed on nearly 600,000 end-points with powerful results and exceeding all expectations. The ARAD team drove an unprecedented eight-month acquisition schedule to deliver tools that enable operators to identify and fix network vulnerabilities in seconds instead of weeks, and it provides the ability to detect, track, target, engage, and mitigate adversarial activities in near real time. The 24th Air Force ARAD team was awarded the 2016 Department of Defense Chief Information Officer Award for Cyber and Information Technology Excellence for their pioneering innovation. The demonstrated potential of ARAD is truly revolutionary, and we are diligently experimenting, evolving, and developing operational concepts and applications to close key mission capability gaps in close partnership with the Tanium experts. The intrinsic operational value and potential of ARAD/Tanium was formally acknowledge by the Air Force CIO, Lieutenant General William Bender, who recently directed ARAD implementation across the Air Force network to include mission systems and enclaves.

The second transformational effort is the Air Force Cyber Squadron Initiative (CSI). It is centered on an active cyber defense model across all echelons of Air Force organizations, designed to deliver enterprise mission assurance in a contested domain, in the presence of a maneuvering adversary. Cyber Mission Defense Teams (MDTs), the primary unit of action, are tailored, trained, equipped and task-organized to survey, secure, and protect key cyber terrain in order to deliver mission assurance. The Cyber Squadron Initiative is a Commander and mission-driven force employment model. Mission Defense Teams employ a spectrum of cyber security and defense tactics, techniques, and procedures in addition to their own suite of tailored cyber defense sensors and tools to provide active defense at the base level. In FY16 the Air Force executed fifteen Mission Defense Team “pathfinder” initiatives across a diverse set of Air Force missions and organizations to test and validate the operational concept and tool requirements. These designated units focused on functional mission analysis, planning, and network characterization. FY17 programming designates another fifteen Service-funded initiatives, as well as sixteen Major Command-funded initiatives. Although the Mission Defense Team concept is a nascent cyberspace defense

capability, these teams are already proving their worth; providing mission assurance for operational commanders' priority missions and mission systems. Laying the foundation, the 50th Space Communications Squadron's Mission Defense Team provided the Wing Commander with an understanding of cyber risk being accepted on the Air Force Space Control Network. The 52nd Communication Squadron Mission Defense Team integrated with AFCYBER Cyber Protection Teams to resolve a Combat Air Force cyber incident, defending Commander's key cyber terrain and allowing Wing Commanders to understand the operational risk if cyber hygiene is not a priority.

The third transformational effort is Air Force Materiel Command's Cyber Resiliency of Weapons Systems, or CROWS office. Their mission is to increase cyber resiliency of Air Force weapon systems across our acquisition and life cycle management processes to maintain mission effective capability under adverse conditions. CROWS have two primary objectives; first, to "bake-in" cybersecurity into developmental and future mission and weapons systems, and second; to employ a prioritized threat- and risk-based, cyber vulnerability assessment of existing systems to best mitigate risk to missions and forces. Their roadmap to cyber resiliency advances from systems assurance to the institutionalization of cyber security, cyber hygiene, and resiliency across all Air Force weapons systems. Their comprehensive strategy includes sustainable and programmable tools, infrastructure, and a skilled cyber workforce of operators, system engineers, and acquisition professionals to deliver end-to-end mission and weapon system cyber security.

The combined effects and capabilities of these three major Air Force transformational efforts, plus our ongoing AFCYBER cyber security campaign plan leveraging signals intelligence (SIGINT) and all-source intelligence, industry, National Institute of Standards and Technology, and DISA best practices, provides the Air Force with a full-spectrum, coherent framework for generating threat- and risk-based mission assurance from networks and infrastructure. This mission assurance strategy is girded by an acquisition and life-cycle sustainment enterprise empowered, organized, and resourced to deliver cyber security and resilience for our Air Force.

Cyber Mission Force: Transitioning from Build to Readiness

The Air Force is on track to achieve Full Operational Capability (FOC) for all Service CMF teams by the end of FY 2018. As of 1 May 2017 we have all teams at Initial Operational Capability and over fifty percent at FOC. The FOC criteria are designed to ensure construction of all teams to a common standard and set of work roles. While we remain laser-focused on building and delivering our Service teams to FOC, we have begun, in earnest, to measure and review team readiness across well-established institutional standards such as Personnel, Training, Equipment and Supply. This ongoing road to formal CMF Defense Readiness Reporting System (DRRS) integration will normalize CMF force presentation and force management while generating critical mission capability and capacity gap analysis needed for Commanders to drive force readiness.

At 24th Air Force we know the most critical element in cyberspace operations is not copper or silicon, it's carbon. Our innovative and audacious Airmen are the centerpiece to our AFCYBER capabilities; they have demonstrated time and again their agility and dedication towards generating mission outcomes for our Service, the Joint Force and our Nation. We have thrust them directly from build to battle throughout the CMF build evolutions. Therefore, we remain committed to recruiting, training, developing, and retaining the right cyber talent. We owe it to the incredible men and women that make-up these teams to see they are properly trained, equipped, and prepared for all assigned missions. There must be an evolving dialogue centered on resourcing and procuring the capabilities and capacity required for our CMF to be properly postured for success beyond the build.

"One Force" in AFCYBER

In cyber, we train and fight as one team with all components; Regular Air Force, Air National Guard, and Air Force Reserve. We are delivering cyber forces in support of the Department's CMF framework fully integrated with our Total Force partners in the Air National Guard and Air Force Reserves. These "One-Force" teams are providing United States Cyber Command with capabilities to defend the nation, support Combatant Commanders, and defend the DoDIN. The Air Force's Total Force cyber mission contribution is impressive. They are providing both National and Cyber Protection Teams, Cyberspace Command and Control and a separate Continuity of

Operations Ops Center facility, a Cyberspace workforce training and skills validation course, and niche Industrial Control System cyber-security and defense teams.

The Air National Guard has already completed two extremely successful Cyber Protection Team six month mobilizations in support of United States Northern Command air defense missions and associated key cyber terrain security and defense. These Total Force professionals bring a unique blend of experience and expertise to the full spectrum of cyberspace missions. Many work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness. A prime example from the Washington State Air National Guard is their ability to harness their expertise to establish unique Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) threat prevention and response packages or Unit Type Codes (UTCs) for mobilization and deployment. These ten-person UTCs provide a capability to detect, deter, degrade, and deny an adversary freedom of action within Cyber Physical Systems, Industrial Control Systems, and Critical Infrastructure and Key Resources Networks. Further, the Air National Guard established two units to provide resident initial assessment and cyber skills training as well as delivering on-line cyber training to the Air Force. These vital capabilities allow us to refine training capability requirements that drive future training curriculum design. In addition, the Air Force Reserves, in coordination with our formal cyber school house are focused on development of advanced resident and distributed learning for the CMF.

Operational awareness focused on the mission, Commanders' priorities, and resources are key to forging a lasting partnership with our Total Force brethren. On 26 April, 24th Air Force hosted 27 states Adjutants General, Assistant Adjutants General, and Wing Commanders for the first-ever TAG Cyber Symposium. This historical gathering enabled critical collaboration and information flow regarding personnel, equipment, requirements, and authorities and generated insights into optimizing force presentation and harnessing our citizen Airmen's industry expertise to solve tough cyber operations problems.

Cyberspace operations are a "team sport" and 24th Air Force/AFCYBER is wholly committed to strengthening our relationships with other Air Force partners, our sister Services, interagency counterparts, Combatant Commanders, coalition allies, as well as

civilian industry partners. Given the proximity of our headquarters and close mission alignment, 25th Air Force continues to be a critical strategic partner across all of our missions. The 25th Air Force Commander, Major General B.J. Shwedo, has been a vital force provider and steadfast supporter of the CMF build and operationalization of the cyber domain.

Joint Forces Headquarters-Cyber (JFHQ-C AFCYBER)

Cyberspace is an inherently global domain that impacts every function of our Joint Force. This force is increasingly dependent upon cyber capabilities to conduct modern military operations. JFHQ-C AFCYBER supports assigned Combatant or Joint Force Commanders by providing full-spectrum, all domain integrated cyberspace maneuver and effects in support of their assigned missions. JFHQ-C AFCYBER delivers Cyber IN War, not Cyber War, for our Combatant Commanders. As Commander, I retain Operational Control of assigned Service and joint Cyber Mission Forces providing general support to both United States European Command and United States Strategic Command. We recently concluded a combined Joint, Tier-1 Combatant Command Exercise, Austere Challenge/ Global Lightning 2017, supporting both of these Combatant Commands. United States Cyber Command designated JFHQ-C AFCYBER as the Cyber Component to the Joint Task Force Commander, enabling fully integrated joint planning, maneuver, targeting and fires coordination for cyberspace maneuver and effects operations. Our team effectively integrated within existing, institutional planning, targeting and fires processes to provide cyber effects across the full range of military operations within the exercise. Our capabilities and effects were fully synchronized with the timing and tempo dictated by the supported Commander. Cyberspace domain operations were employed using extant processes, fully integrated with all other classic warfighting domains propagating force awareness, comprehension and intrinsic value across all participants, agnostic of professional pedigree or experience.

Partnerships

24th Air Force also understands the cyberspace domain is primarily provisioned by private industry and our ability to collaborate with our industry partners benefits the

nation's cybersecurity posture. We have developed Cooperative Research and Development Agreements with 25 industry leaders in Information Technology, Defense, and Banking to share and collaborate on innovative technologies and concepts. These collaborative efforts allow us to advance science and technology in support of cyberspace operations, as well as share best practices with industry partners. We continue to leverage this program and are currently in the process of enhancing our partnerships with academia.

In July 2015 the Cyberspace Multi-Domain Innovation Team (CMIT) was established as a partnership between 24th and 25th Air Forces to meet the CSAF's intent to optimize the rapid and cost effective generation of operational all domain integrated effects. CMIT achieves this through the integration and convergence of Cyberspace Operations; Intelligence, Surveillance, and Reconnaissance; and Electronic Warfare capabilities to deliver innovative multi-domain planning support and capabilities. To date, this team has planned and delivered multiple cyber capabilities to ongoing operations and has a number of multi-domain initiatives underway to better enable operations in an Anti-Access/Area Denial (A2/AD) environment.

We are also fortunate to have a long-standing close relationship with San Antonio, Texas, also referred to as "Cyber City USA." The local community has committed significant resources to support the growth of cybersecurity both locally and nationally. Our leadership team participates in a variety of civic leader engagements to share lessons related to cybersecurity. By partnering together, 24th Air Force supports a broad array of programs designed to reach young students, essential to our nation's success in this arena. A good example is the Air Force Association's "CyberPatriot" STEM initiative in which our Airmen mentor cyber teams as part of a nationwide competition involving nearly 10,000 high school and middle school students.

We are also making gains in improving our acquisitions process to support the ever changing technology of cyberspace. The Air Force Life Cycle Management Center has worked diligently to streamline our ability to provide solutions to support our cyber missions through "Rapid Cyber Acquisition (RCA)" and "Real Time Operations and Innovation (RTOI)" initiatives. RCA is part of Air Force Space Command's Integrated Agile Acquisition Construct applied to meeting cyber needs by providing faster solutions

to cyberspace needs through traditional acquisition channels. RTOI are activities that produce critical cyber weapons system and platform modifications, capability improvements, and related changes to operational procedures at the "speed of need."

To enable the execution of these efforts, in April 2016, in partnership with the Air Force Lifecycle Management Center, we established the Cyber Proving Ground (CPG). Its mission is to identify, enable, and accelerate the fielding of innovative, operationally-relevant concepts to improve Air Force, Joint, and Coalition cyberspace operations capabilities. The CPG leverages 24th Air Force's innovation and development capabilities and the existing cyber acquisition capabilities of Air Force Lifecycle Management Center's Crypto and Cyber Systems Division. The CPG is a foundry which brings together cyber operators, air force acquisition and engineering professionals, and private sector vendors with potential solutions to close capability gaps. While CPG projects are small in scope and timeframe, they comprise a broad spectrum of challenges, from complex development and testing efforts, to simple technical evaluations of existing technologies.

I want to highlight two recent efforts from the CPG. First, in just six weeks the CPG developed and fielded the Service's first defensive Solaris capability which enabled our Cyber Protection Teams to secure and defend the Air Force Satellite Control Network. Second, the CPG recently completed development, testing, and fielding of two unique capabilities to support United States Cyber Command's ongoing Joint Task Force Ares operations. Other CPG efforts fielded capabilities that thwarted adversary exploitation of user authentication certificates, the unauthorized release of personally identifiable information, and the blocking of sophisticated intrusion attempts by advance persistent threat actors. These technical solutions were forged, tested and fielded in weeks to months, versus years.

Challenges and Opportunities

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 significant challenges in our critical path towards delivering required capability and capacity for assigned missions. 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 cyberspace domain workforce. These broad categories closely mirror Admiral Rogers' focus areas for United States Cyber Command and the Service Cyber Components. His charges direct us to secure and defend weapons and mission systems and the data that resides on them, as well as increase speed, agility, precision, readiness and lethality of an effectively manned and trained cyber workforce in coordination with Guard and Reserve forces to deliver all domain integrated effects across all phases of operations that support DoD strategy and priorities.

Manpower and Training

Significant manpower shortages across our C2 elements at all echelons hampers our ability to support geographic and functional commands. Manpower deficiencies in our units that operate, secure, and defend our networks force a constant high-pressure, deployed in place operating environment of competing priorities and risk decisions with insufficient force structure to meet critical operational demands. We are actively examining our training pipeline to find smarter more agile methods which get our operators to their units and on mission faster. In 2015 we added a local San Antonio detachment to our cyber school house to increase training capacity. The detachment is crucial in enhancing formal training throughput and efficacy due to the proximity to the majority of Air Force CMF units and their cyber weapon systems. Since June 2015, the detachment has graduated 518 CMF operators and saved one million dollars per year in TDY costs by collocating the training with the operational units. Formal cyberspace operations training must remain rigorous and comprehensive enough to meet operational requirements but also agile and responsive enough to accommodate the pace of change in the cyber domain.

The Service Staff in conjunction with Air Education and Training Command are currently developing custom Air Force Specialty Code training tracks based on a modular syllabus that utilizes the latest training assessment innovations and provides placement flexibility through the training pipeline. The concept allows Airmen to "test-out" of portions or modules of the curriculum. This methodology provides incentives and opportunities to our Airmen who possess an advanced cyber aptitude, whether via formal or informal training or education, to advance through the pipeline and arrive on

station at an operational unit in a significantly shorter time frame. In order for this concept to be effective, resourcing is required to design and validate assessment tools and develop an agile and responsive curriculum development framework that keeps pace with the advancement of technology, tradecraft, and our adversaries.

Cybersecurity of Weapons Systems

There are insufficient weapons system sustainment dollars going towards system cyber security and defense. The majority of all sustainment dollars today goes toward functional capability upgrades in any mission or weapons system program. Our current process of "bolting on" weapons system cyber security after the fact, levies excessive mission-risk and is extremely manpower and resource intensive to properly secure and defend the system. It is more complex and expensive to defend mission systems where there is no inherent or "baked in" cybersecurity framework. As previously mentioned, the CROWS office is getting after this today as directed by the NDAA, but much more needs to be done from a resource and execution perspective.

Key Enablers

The Department has begun planning for and resourcing a multiple phenomenology approach to access. Each Service is exploring multiple pathways to get to the target and deliver effects against our adversaries in cyberspace. The Air Force is also planning and provisioning for its own organic platform and tool development capabilities, separate and distinct from NSA. This will ensure assigned cyberspace mission priorities and requirements are being met. Critical to accessing the target with the appropriate tools to deliver the desired effect is timely, relevant, domain specific, all-source intelligence.

While achieving and maintaining a depth of knowledge in cyberspace is technically challenging, all source Target System Analysis (TSA)s that are domain agnostic is a proven approach to providing timely, relevant intelligence support to operations. The Intelligence Community (IC) must perform this function due to the vast amount of resources and the ability to leverage existing partnerships outside the Department and the United States Government. The methodology employed purposely resembles target development in any other warfighting domain. A thorough understanding of the Commander's intent, specifically the objectives and effect desired

for a particular target set is required. Center of Gravity analysis is conducted to analyze the functions and interconnectivity of those components critical to the target. Systems engineering and network analysis is developed to map out the key terrain within the target, to enable operators to conduct Intelligence Preparation of Environment (IPOE) and refined Target Development. Based on the analysis and reporting from the IPOE, the operators develop a strike package based on an understanding of the target environment and the tools and capabilities they have developed in order to deliver the desired effects. The current approach of contracting these cyber TSAs has been successful, but we view it as a temporary solution until the IC transforms their on-going intelligence support to cyber analysis and resourcing challenges and takes on this critical intelligence requirement in earnest.

Professionalization of the workforce

The Air Force established a Cyber Project Task Force to monitor progress, identify challenges, and collaborate on manpower and personnel efforts to "get after" building the Air Force portion of the CMF. The Air Force also instituted a Service-wide policy to encourage back-to-back CMF tours for our CMF-trained personnel, thereby ensuring proper return on investment. Furthermore, the Air Force recognized the positive value of embedding limited CMF-trained personnel back into Service non-CMF cyber positions, in order to better operationalize the total Service cyber enterprise. Although, these cross-pollinated CMF-trained personnel may not have specific CMF-related or associated jobs, they are assigned to cyberspace-related positions growing their depth and breadth of operational expertise. Finally, the Air Force also has the responsibility to develop our portion of the CMF to meet Operational Commanders' requirements in a method that also ensures Air Force Cyber Airmen stay competitive with long-term career projections and a "Path to Greatness" for cyberspace Airmen. In addition, cyber Airmen may attend professional developmental opportunities such as Air Force Institute of Technology, Computer Network Operations Development Program, or the Air Force Weapons School, all of which will positively impact the operationalization of the cyberspace domain within the Air Force and in turn, the future of the CMF.

Conclusion

I am proud of the tremendous strides made to operationalize cyber capabilities in support of joint warfighters and defense of the nation. Despite the challenges of growing and operating across a contested and diverse mission set with a rapidly maturing work force, it is clear Air Force networks are better defended, Combatant Commanders are receiving more of the critical cyber effects they require, and our departments' 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. Without question, resource stability in the years ahead will best enable our continued success in developing Airmen and maturing our capabilities to operate in, through and from the cyberspace domain. Resource stability will also foster the innovation and creativity required to face the emerging threats ahead while maintaining a capable cyber force ready to act if our nation calls upon it.

I am honored and humbled to command this magnanimous organization and look forward to a thorough and continuing dialogue.

NOT FOR PUBLICATION UNTIL RELEASED BY
THE SENATE ARMED SERVICES COMMITTEE
CYBERSECURITY SUBCOMMITTEE

STATEMENT BY

MAJOR GENERAL LORI E. REYNOLDS

COMMANDER

MARINE CORPS FORCES CYBERSPACE COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY

CYBER POSTURE

1ST SESSION 115TH CONGRESS

MAY 23, 2017

Major General Loretta E. Reynolds:

Major General Reynolds was commissioned a Second Lieutenant in May 1986 upon graduating from the United States Naval Academy. Throughout her career she has served in a variety of command and staff billets in the operating forces. As a Lieutenant, she served as a Communications Watch Officer at the Base Communication Center, and later returned to the Division Communications Company where she served as a Communication Center Platoon Commander, Multichannel Platoon Commander, Operations Officer, and Radio Officer. As a Captain and Major, she served with Marine Wing Communications Squadron 18, 1st Marine Aircraft Wing Okinawa, Japan as a Detachment Alpha Executive Officer and Commanding Officer. She served with the Ninth Communication Battalion, 1st Surveillance, Reconnaissance, and Intelligence Group as the Assistant Operations Officer and Commanding Officer, Bravo Company. As a Lieutenant Colonel, she commanded Ninth Communication Battalion, I MEF and deployed in support of Operation Iraqi Freedom II in Fallujah, Iraq. As a Colonel, she commanded I MEF Headquarters Group and deployed the Group to Camp Leatherneck, Afghanistan in support of I MEF FWD/Regional Command Southwest in Helmand Province during Operation Enduring Freedom. She recently served as the Commanding General, Marine Corps Recruit Depot/Eastern Recruiting Region, Parris Island, SC.

In the Supporting Establishment, she has served as an Acquisition Project Officer at the Marine Corps Systems Command, Candidate Platoon Commander for Charlie Company, Officer Candidate School, Commanding Officer of Recruiting Station Harrisburg, Pennsylvania, an Action Officer and Deputy Division Head for Strategic Plans Division, Command, Control, Communications, and Computers (C4) Department, Headquarters Marine Corps and as Division Chief (J6) at the Joint Staff in the Pentagon. Her most recent assignment was as the Principal Director (Asia & Pacific), Office of the Deputy Under Secretary of Defense (Asia & Pacific).

Her professional military education includes the United States Naval Academy, The Basic School, the Basic Communication Officer's Course, Command and Control Systems Course, the Navy War College and the Army War College. She has earned Master's Degrees from both the Naval War College and the Army War College.

Her personal decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star, Meritorious Service Medal (with gold star), the Navy and Marine Corps Commendation Medal (with gold star).

Introduction

Chairman Rounds, Ranking Member Nelson, and distinguished members of this Committee, on behalf of the Marines, civilian Marines, and the families of U.S. Marine Corps Forces Cyberspace Command (MARFORCYBER), I thank you for your continued support of the important work we are doing to secure, operate, and defend the Marine Corps Enterprise Network (MCEN) and defend the nation in cyberspace. I welcome this opportunity to highlight what our Marines are doing in the cyberspace domain and how we are shifting our focus from building the command to operationalizing, sustaining, and expanding capabilities in this warfighting domain. I am pleased to be sitting alongside my colleagues from the other Service Cyber Components of the United States Cyber Command (USCYBERCOM).

I am humbled everyday by the tenacity, professionalism, and commitment to mission success displayed by my team. It gives me great pride to highlight the many accomplishments of the Marines and civilian Marines of MARFORCYBER, and the work they are doing in support of warfighting and in defense of our nation.

It will come as no surprise to the members of this committee that we face a growing cyber threat - one that is increasingly persistent, diverse, and dangerous. Malicious cyber activity from both state and non-state actors continues to intensify and every conflict around the world includes a cyber dimension. The traditional fight we have envisioned across the domains of air, land, sea, and space has expanded to the cyber domain. The United States' technical superiority is not yet established in this domain: we have to earn superiority in each fight. We can never take our superiority for granted. Our enemies will test us.

This year we established MARFORCYBER's motto – *Semper in Proelio*. It is Latin for "Always in Battle." This is the reality of cyberspace. The American people rightfully expect their Marines to fight our Nation's battles and win – always, including in the domain of cyber. We work hard each and every day to ensure we are prepared to fulfill this expectation.

Mission and Organization

As the Marine service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum cyberspace operations. That includes operating and defending the MCEN, DoD Information Networks (DoDIN) operations, conducting Defensive Cyberspace Operations (DCO) within the MCEN and Joint Force networks, and when directed, conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. We do this to enable freedom of action in cyberspace and across all warfighting domains, and deny the same to our adversaries.

As the Commander, MARFORCYBER, I wear two hats. I am Commander, MARFORCYBER, and I am the Commander of Joint Force Headquarters – Cyber (JFHQ-C) Marines. In these roles, I command about 1700 Marines, civilian Marines, and contractors across our headquarters and subordinate units. MARFORCYBER is comprised of a headquarters organization, a JFHQ-C, and two colonel led subordinate commands: Marine Corps Cyberspace Warfare Group (MCCYWG) and Marine Corps Cyberspace Operations Group (MCCOG). Through the JFHQ-C construct, we provide direct cyber operations support to U.S. Special Operations Command (USSOCOM). We are currently in the process of developing and manning a Joint Force

Headquarters – Forward, which is part of an effort to meet the growing demand of cyber operations throughout USSOCOM's global operations.

Within the MARFORCYBER headquarters, we currently have 189 authorized billets for Marines and 32 authorized billets for government civilians. We have an additional 65 authorized billets for contract employees. In a field where technology is paramount, our people continue to be our most valuable resource and greatest strength. Simply put, they represent the very best our nation has to offer - they are patriots, who are doing the arduous and necessary work to defend against increasingly capable adversaries.

I organize operations along three lines of effort that I will highlight for you today. I use this framework to organize activities, allocate resources, grow capability, and measure our progress.

Secure, Operate, and Defend the MCEN

My first priority is to secure, operate, and defend the Marine Corps' portion of the DoDIN, the MCEN.

We accomplish this mainly through one of the two subordinate commands mentioned previously – the MCCOG. The MCCOG is responsible for directing global network operations and computer network defense of the MCEN. It executes DoDIN Operations and DCO in order to assure freedom of action in cyberspace and across warfighting domains, while denying the efforts of adversaries to degrade or disrupt our command and control.

This past December, the MCCOG was activated during a re-designation ceremony from the former Marine Corps Network and Operations Security Center (MCNOSC). This re-designation was not simply a name change. The missions and roles assigned to the MCNOSC transitioned from that of a Supporting Establishment command to that of an Operational Force command apportioned to U.S. Strategic Command (USSTRATCOM).

The Marine Corps views the MCEN as a warfighting platform, which we must aggressively defend from intrusion, exploitation, and attack. Cyberspace operations favor the attacker, and our operational dependencies require us to conduct a formidable, continuous defense. Real-world defensive cyberspace operations have informed and sharpened our ability to detect and expel threats on the MCEN. Since May 2016, the MCCOG has responded to 4,050 events on the MCEN. These events include unsuccessful attempts to access the network, non-compliance with security standards, reconnaissance of the network, and explained anomalies (configuration errors). This number encompasses only the events that require our attention and further analysis. There are thousands of events that occur on the network daily that are blocked and contained by our network defenses and filters.

Our priorities for improving our defenses this year include actions to flatten the Marine Corps network and improve our ability to sense the environment, harden the network through increased endpoint security, and decrease incident response time. To do this, we are aggressively seeking to consolidate legacy domains, implement a comply to connect capability and the WIN 10-operating system, and collapse regional service desks to an enterprise service desk. Each of these priorities are described briefly below.

Network Access Control, Compliance, and Remediation (NACCR). NACCR provides defense in depth by positively identifying devices that attempt to connect to our networks, ensuring the device is compliant with the latest set of security updates, and, if non-compliant, NACCR initiates quarantine and remediation actions.

Enterprise Service Desk. We are transitioning eight regional service desks into a central, standardized Enterprise Service Desk (ESD) in Kansas City, Missouri. The ESD will be under the operational control of MARFORCYBER. Users' requests for IT support and incident response, once centrally managed, will provide valuable insights into trends on the network. Long term benefits will include supporting a top down governance structure, increased efficiency in supporting the warfighter, and providing a holistic view of the network that informs and complements defensive actions on the MCEN.

Domain Consolidation. In order to flatten, harden, and secure the network, we must have full visibility of all networked assets. We are undertaking efforts to bring remaining disparate legacy networks into a homogenous and secure network. Legacy networks contribute to the Marine Corps' cyber footprint and unnecessarily increase attack surfaces for adversaries. This deliberate effort for domain consolidation will provide much needed standardization and increase the cybersecurity posture of the MCEN.

Windows 10. The Marine Corps is transitioning its Microsoft Windows end user devices to the Windows 10 (WIN 10) operating system (OS). WIN 10 OS will improve the Marine Corps' cybersecurity posture, lower the cost of information technology (IT), and standardize the Marine Corps' IT operating environment. The WIN 10 OS has numerous embedded security features that earlier Windows OS's lack. These features include protection such as encrypting hard drive data while powered off or preventing the execution of unknown system commands.

Like the Internet itself, many of our Programs of Record and warfighting systems were not built with security in mind. To combat these vulnerabilities, we are reviewing each one to determine how we can improve security. We have also conducted a review of all vulnerable end of life hardware and software on the network and developed expedited strategies to upgrade, consolidate or remove systems that cannot be adequately hardened. Projects that focus on auditing, analysis and tracking of cyber events and anomalous activity have been developed and implemented to improve our situational awareness of system status and cyber monitoring capabilities. Programs that test and audit our defensive posture are continuously reviewed for relevance and improvement to address the changing cyber threat environment and support the intelligence operations cycle on a shortened timeline. Cyber is a dynamic, competitive environment, and we are continually responding to the increasing capability and capacity of our adversaries.

As we have built Cyber Protection Teams (CPT), we have employed them across the MCEN. This year, our CPTs have conducted named cyber operations to include focused internal defensive maneuver missions (IDM), ensured security of Personally Identifiable Information (PII) repositories, and completed security enhancement missions for cyber key terrain, countering known threats to the network. In all DCO activities, the Marine Corps consolidates findings and actionable lessons for dissemination to the broader operational community.

We are making efforts to better understand system data, and have employed Service aligned CPTs to harden Service PII repositories. In 2015, MARFORCYBER began efforts to secure PII repositories across the service. The MCCOG and Service CPTs assessed the security posture of our 40 largest PII repositories. While the overall security posture of our systems was within established standards, we identified areas for improvement we needed to address. Our Service aligned CPTs conducted on-site visits to several repositories that were deemed critical high risk. There, we identified and remediated vulnerabilities and trained system owners and administrators. We continue efforts to ensure these systems maintain the highest levels of security.

We have identified a requirement for a more robust MCCOG Continuity of Operations (COOP) capability. The MCCOG COOP is effectively a MCEN COOP capability. MCCOG lacks the ability to comply with DoD Directive 3020.26 of 9 Jan 2007 requiring up to 30 days Mission Essential Services and Functions performance for no-notice events. The Marine Corps IT Center (MCITC), located in Kansas City, Missouri, is the recommended COOP site, allowing us to leverage available space and integrate with other MCCOG operations already at MCITC. We have conducted thorough analysis and research to develop an effective COOP capability, but currently lack the financial resources to put our plan into action.

We are participating in efforts to shape our battle space by designing a more defensible architecture. As we move toward implementing the Joint Information Environment, we are also working to unify and centralize our network to better see, understand, and defend the MCEN. We are integrating and standardizing cyberspace threat reporting, intelligence production and analysis to better inform commander's situational awareness and decision making. Our network must be resilient, redundant and interoperable, and extend from garrison to the tactical edge of battle. In other words, we need a seamless MCEN that provides a defensible capability providing enterprise services from "fighting hole to flagpole." We are moving out in this direction.

Provide a Cyberspace Warfighting Capability

My second priority supports our responsibility to provide ready, capable cyber forces to USCYBERCOM. Creating this capability in a new command is a tremendous undertaking. We are on track to provide our Combat Mission, Cyber Protection, National Mission, and Combat Support teams in time to meet USCYBERCOM Full Operational Capability (FOC) requirements.

The Marine Corps is responsible for 13 of USCYBERCOM's 133 Cyber Mission Force (CMF) teams: one National Mission Team (NMT), eight Cyber Protection Teams (CPTs), three Combat Mission Teams (CMT), and one Cyber Support Team (CST). These 13 teams are aligned against USCYBERCOM (Cyber National Mission Force), USSOCOM, and Marine Corps missions. Three of the eight CPTs are service retained and oriented to service missions, (23% of the total Marine Corps CMF).

Of our 13 teams, nine teams have reached and four teams remain at Initial Operating Capability (IOC). All 13 teams are scheduled to reach FOC in FY 18. It's important to note, that all 13 teams designated as having reached IOC are employed against real-world problem sets and are fully engaged in supporting the mission. It is also important to note that achieving FOC is also not an indication that work is done. We must continually ensure we are training and sustaining the force to ensure we remain agile, adaptable, and ready to defeat all enemies.

To that end, we are moving forward with the creation of a cyberspace occupational field. We have learned a great deal in the past several years about the training, clearance, and experience requirements across the cyber mission force. We know that in order to be effective, we must retain a professional cadre of cyberspace warriors who are skilled in critical work roles, and we know that many of our Marines desire to remain part of the cyber work force. The Commandant has told us to move out, and we are planning with Headquarters, Marine Corps (HQMC) to design a cyberspace occupational field to address offensive and defensive team readiness requirements. We intend to begin assigning Marines to the cyberspace MOS in FY18. This will significantly improve both readiness and retention of the force.

In the spring of 2016, we activated the MCCYWG. This new command is a colonel led command with the responsibility for identifying capability requirements, training, certifying, and sustaining readiness for our CMF teams. In the future, my vision for this command is to develop it into one of service as the Cyber Warfighting Center for the Marine Corps, where it will provide standardized advanced cyber training and certifications that support Marine cyber training and readiness across the Corps.

While building the CMF, members of MARFORCYBER were dual-hatted as the Joint Force Headquarters staff. This year, the pace of cyber operations demanded that we begin to man a standing JFHQ-C. The JFHQ-C provides the planning, targeting, intelligence and cyber execution support to supported commanders, and provides command and control for CMTs and CST. This summer, we will begin hiring JFHQ staff who will be positioned forward and integrated into USSOCOM planning and intelligence processes in Tampa, Fort Bragg, and across Theater Special Operations Commands.

This year the Marine Corps continued its initial investment in specialized tools for defensive cyberspace operations. The Deployable Mission Support System (DMSS) hardware and software tools comprise the weapons system CPTs use to meet any mission they may be assigned, from readiness and compliance visits to incident response or Quick Reaction Force missions. This year, we championed an ability to conduct split based operations with the DMSS, enabling the CPT lead to forward deploy a small element and push information back to a home station "war room" for remote analysis and remediation. This initiative and concept of employment will reduce deployed time and costs and increase our ability to collaborate more freely with other CPTs or across the mission force.

We are rapidly establishing relevant operational capability in support of the warfighter. We have experienced tremendous growth in operational capability over the past year as we have fully supported the delivery of operational cyberspace effects under Joint Task Force Ares, a USCYBERCOM led effort designed to support C-ISIS efforts in U.S. Central Command (USCENTCOM). Our Joint Force Headquarters is providing relevant support to more fully integrate planning cyber operations, intelligence and fires, and we continue to refine procedures with each exercise and operation we support. On the defense, our CPTs are contributing to Cyber National Mission Force priorities around the globe, and at USSOCOM. Across USCYBERCOM, Marines are at the point of friction, increasingly relevant and eager to contribute to the fight.

We are also active participants with other Service components and USCYBERCOM in a variety of new processes, infrastructure and tool development, acquisition initiatives, training transition,

and Tactics, Techniques and Procedures (TTP) development for the CMF. We know we must continually adapt, innovate, and change to meet future threats.

Add Value to the MAGTF

My third priority is to add cyberspace warfighting expertise to the Marine Air Ground Task Force (MAGTF). Our Commandant, General Neller, understands the necessity to move forward quickly to build MAGTF capability to operate in all five domains. This is not the fight of the future, but the current fight we are in right now. Consistent with our Commandant's guidance, we want to develop the Marine Corps' cyber capacity at the tactical level of war, so that in the future the Marine Corps will more effectively preserve the ability to fight and win in a contested environment and deliver effects in cyberspace.

Since our establishment in 2009, our Marines and civilians have implicitly understood the need to provide a high return on the Marine Corps' investment in cyber. In 2010, we began participating in Service training, exercises and concept development to institutionalize cyber across the Service, and have built momentum ever since. Cyberspace operations are now codified in scenarios at Marine Corps Tactics and Operations Group, Marine Corps Logistics Operations Group, and Marine Aviation Weapons and Tactics School, and the Marine Expeditionary Forces (MEFs) better understand the integration of cyber through our participation in MEF Large Scale Exercises. For the first time, this Fiscal Year we will have supported a training exercise within each MEF, our major warfighting commands. In addition, we recently concluded a mission in support of a Special Purpose MAGTF in the USCENTCOM AOR. Commanders across the Marine Corps and combat commands have seen the capability our defensive teams bring to the fight. Across the board, the demand signal for Marine Corps cyber operators and capability is high, and increases with each successful mission.

The Marine Corps Operating Concept (MOC) describes a future operating environment where Marines will fight with and for information, engage in a battle of signatures and be required to maneuver throughout networks even as we design networks that are maneuverable themselves. Last year, the Marine Corps developed a new force design to meet the needs of the MOC. This effort, called Force Design 2025, includes Defensive Cyber Operations-Internal Defensive Measures (DCO-IDM) companies and electronic warfare companies for each MEF. The DCO companies will provide MAGTF commanders with a trained and organized capability to conduct activities as maneuver elements for deployed networks, data stores and weapons system. As an element of the MEF Communication Battalion, the DCO-IDM Companies will support the defense of MAGTF communication networks and maintain a commander's ability to command and control. Their primary function will be mission assurance actions such as actively hunting for advanced internal threats that evade routine security measures, performing incident response actions, and performing digital forensics. MARFORCYBER is leading the DCO-IDM Training Pilot Program this month, which will inform the DCO-IDM Company concept of employment.

The Electronic Warfare companies, built inside our Radio Battalions, will employ similar intelligence, targeting and effects generation TTPs as offensive teams and will provide full spectrum electromagnetic support capability to the MEF commander.

To increase cyber readiness across the Service, we have emphasized the role of the Commander in the security and defense of the MCEN, and are conducting Cyber Readiness Visits at

commands throughout the Marine Corps to identify cyber key terrain, assess readiness and culture, and bolster our defenses. As the Marine Corps establishes the cyber career field for Marines, we will aggressively build cyber operators to ensure the MAGTFs, bases and stations have the expertise and capacity to enhance cyber readiness not only at MARFORCYBER, but across the Marine Corps.

As we have transitioned from building the CMF to sustain readiness of the CMF, we are looking more carefully at how we retain manpower, prioritize training, ensure that our tools are current and sufficient to counter the growing threat, and whether we will have sufficient infrastructure, tools and facilities available for the force. We look forward to working more closely with Congress to address needs as we identify them.

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

Cyber Workforce Management

MARFORCYBER is conducting a multi-year, Service-integrated, bottom-up approach to grow both our headquarters element and the MCCYWG headquarters, which includes growth within manpower, training, facilities and equipment. Our growth is in-line with the Commandant's vision and Future Force 2025.

Since our last testimony before the House Armed Services Committee in March of 2015, we have initiated plans to significantly increase our headquarters staff. While MARFORCYBER has seen manpower growth in support of our CMF, as directed by the Secretary of Defense, we have not seen growth for the headquarters element that supports the CMF. Growth will require resources to hire personnel for the enabling operational and strategic headquarters staff, and for facilities where we can train and employ them.

MARFORCYBER was established with an initial staff of eight personnel. In 2011, we received additional personnel when the Service conducted a Force Structure Review. Since that time, the mission of MARFORCYBER has changed several times, including the requirement to grow a JFHQ-C, and our alignment to support USSOCOM. Concurrently, USCYBERCOM has developed new processes, working groups and planning teams to address the growing mission and relevance of cyberspace, while we have seen a steady increase in capability of adversary nations. In short, the scope of our mission has increased substantially, exceeding our existing capacity, and we have identified significant growth requirements to HQMC. One of the key requirements to grow and maintain an effective CMF is our ability to hire and retain the highest quality cyberspace professionals.

In workforce management, we are being challenged by the policy issues discussed below as well as the increasing demand for workers with cyber experience in industry and government. Private industry remains an attractive prospect for our cyber personnel with salaries and incentives we cannot compete with. On the uniformed side, we are successfully leveraging our Reserve forces to help close manpower gaps. This capability has given us a tremendous boost, with Reservists agreeing to come on orders for anywhere from one to three years.

The establishment of the cyber career field outlined earlier is one way we are addressing this challenge. We surveyed a sample of our CMF and found that 54% of respondents indicated that his or her work role was the most important consideration concerning re-enlistment with only 38% of respondents indicating pay was the most important (8% were undecided). Marines want to stay cyber Marines, and we will soon allow them the opportunity to do that.

The Marine Corps also has other initiatives underway to help address the manpower challenges identified above. We are scheduled to brief HQMC in early June on manpower growth requirements for both the MARFORCYBER and MCCYWG Headquarters. Our requirement is for additional intelligence professionals, logistics and administration personnel, network experts, acquisition and contract management teams and tool development experts. The Service is conducting a holistic analysis to ensure our growth is realistic, valid and complete.

On the civilian side, policy that exempted cyberspace positions during the recent hiring freeze was helpful in supporting our civilian workforce growth. However, the recruitment of recently retired or separated service members that are cleared and fully trained has become substantially more difficult after the expiration of policy suspending the 180-day cooling off period required before taking a government position.

We are well into the development of a new headquarters building for MARFORCYBER designed to meet the demands of our increased mission. I want to thank you for the Military Construction funding that enabled the East Campus Building – Marine Corps (ECB-MC) project. ECB-MC is a 148,000 square foot, 550 seat building that will provide full spectrum cyber operation capabilities. The project broke ground in October 2015 and the steel work "topped out" in November 2016. MARFORCYBER and our partners have developed a phased turnover plan to facilitate the fit-up of the building's complex systems and we expect the final turnover of spaces in December 2017. Assuming the construction and fit-up schedule is maintained, we expect to move MARFORCYBER into the new building during the 4th quarter of FY 18. This space is much more than administrative offices. It will serve as the Marine Corps' premier cyber warfighting platform.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to testify before you today, and for the support that you and this Committee have provided our Marines and their families.

I have outlined just a handful of examples that share how our Marines are leaning in to increase cyber capability and capacity across this command and the Marine Corp through our lines of effort to secure, operate, and defend the MCEN, provide a warfighting capability, and provide value to the MAGTF. The success of these efforts depend on our Marine Corps cyber team – a team made up of warfighters, who are dedicated to their warrior craft. They are professional, competent, and committed to mission success. Simply put, they represent the very best.

I look forward to continuing this dialogue in the future and would be happy to take your questions.