[H.A.S.C. No. 114–19]

CYBER OPERATIONS: IMPROVING THE MILITARY CYBERSECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD
MARCH 4, 2015

U.S. GOVERNMENT PUBLISHING OFFICE
94–221 WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

JOE WILSON, South Carolina, *Chairman*

JOHN KLINE, Minnesota
BILL SHUSTER, Pennsylvania
DUNCAN HUNTER, California
RICHARD B. NUGENT, Florida
RYAN K. ZINKE, Montana
TRENT FRANKS, Arizona, *Vice Chair*
DOUG LAMBORN, Colorado
MO BROOKS, Alabama
BRADLEY BYRNE, Alabama
ELISE M. STEFANIK, New York

JAMES R. LANGEVIN, Rhode Island
JIM COOPER, Tennessee
JOHN GARAMENDI, California
JOAQUIN CASTRO, Texas
MARC A. VEASEY, Texas
DONALD NORCROSS, New Jersey
BRAD ASHFORD, Nebraska
PETE AGUILAR, California

KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
JULIE HERBERT, *Clerk*

CONTENTS

CYBER OPERATIONS: IMPROVING THE MILITARY CYBERSECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, March 4, 2015.

The subcommittee met, pursuant to call, at 3:33 p.m., in room 2118, Rayburn House Office Building, Hon. Joe Wilson (chairman of the subcommittee) presiding.

OPENING STATEMENT OF HON. JOE WILSON, A REPRESENTATIVE FROM SOUTH CAROLINA, CHAIRMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. WILSON OF SOUTH CAROLINA. Ladies and gentlemen, I call this hearing on the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee to order.

I am pleased to welcome everyone here today for the very important hearing of the fiscal year 2016 budget request for cyber operations programs of the Department of Defense [DOD].

One need only read the headlines of almost any newspaper on almost any day by way of the media to see the challenges we face as a Nation when it comes to hacking and cyber threats. The array of threats both from state and non-state actors pose significant challenges to our military forces, our economic well-being, and our diplomatic activities worldwide.

The recent government accountability report on the vulnerabilities to our air traffic control networks vividly illustrate the need to work across departments, agencies, and even internationally to ensure our security. We recognize that the Department of Defense capabilities will be critical to those efforts, but must be provided the resources and the authorities to be effective. As we look at this budget request and as the witnesses describe their plans for how they will execute their activities in fiscal year 2016, I ask that you address the following questions. What specifically are you requesting in the budget, and what major initiatives do you expect to fund? If defense sequestration caps are enforced in the budget request, what impacts do you expect this year? How are you measuring or assessing the cybersecurity posture of the Department of Defense networks, and what vulnerabilities do you see?

Today we have invited a panel that represents the top military leadership for cyber operations across the Department of Defense. Our witnesses include Admiral Michael Rogers, Commander of the U.S. Cyber Command [CYBERCOM]; Lieutenant General Edward C. Cardon, Commander, U.S. Army Cyber Command; Vice Admiral

Jan Tighe, Commander at Navy Fleet Cyber Command, 10th Fleet; Major General Daniel J. O'Donohue, Commanding General Marine Forces Cyber [MARFORCYBER]; and Major General Burke E. Wilson, Commander, 24th Air Force.

Now I would like to invite the subcommittee ranking member, Mr. Langevin of Rhode Island, to make any comments that he might have.

[The prepared statement of Mr. Wilson can be found in the Appendix on page 33.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Well, thank you, Mr. Chairman.

And I want to thank our witnesses for being here today, and I look forward to hearing your testimony, and, as always, I thank you for the work you are doing on behalf of our country. Thank you all for your service.

The 2014 Quadrennial Defense Review stated that, and I quote, "The importance of cyberspace to the American way of life and to the Nation's security makes cyberspace an attractive target for those seeking to challenge our security and economic order," end quote. I could not agree more. Last year the Director of National Intelligence placed cyber threats number one on the list of strategic threats to the United States.

Most recently, the National Security Strategy cites the danger of destruction and even destructive cyber attack is growing. The cyber domain is complex. We all understand that. Threats in this space continuously evolve based on emerging technologies and techniques to counter our efforts. Threats are carried out by a diverse set of actors. Securing, defending, and operating freely in this space presents a nontraditional challenge requiring an immediate but thoughtful response.

Since the creation of U.S. Cyber Command, the Department has made substantial strides in understanding and enabling freedom of action in the cyber domain, as well as understanding and protecting Department of Defense networks. Significant investments have been made. In fact, cyberspace is the only area of growth in the Department of Defense's budget in the last few years. I commend the Department's efforts, and I am proud of what has been achieved so far, yet there is still much to be done. Confronting this challenge will continue to require dialogue between the Department and Congress on the policies, capabilities, and other resources needed to appropriately and successfully operate in the cyber domain. That is why this hearing is so important.

Together we can build and maintain a ready cyber force for the Nation. I look forward to receiving an update from the witnesses on the buildout of our cyber capacity and the fiscal year 2016 budget request. I hope the services will provide us an understanding of total force requirements for cyber operations, both service-specific and for the U.S. Cyber Command to enable the subcommittee to better understand all resources needed and provide for a ready force.

Specifically, I am eager to hear about how the services are recruiting and retaining qualified military and civilian personnel, managing cyber as a career field, and any challenges associated with those fields. I look forward to hearing how the services are incorporating the Reserve Components into the cyber mission forces. Additionally, I would like to understand how science and technology investments are being leveraged now and in the future to deliver the latest and best capabilities.

I would also like the witnesses' perspective on whether the current acquisition process delivers tools in time to meet and stay ahead of the threat, which as we know as technology changes so quickly, that is a significant challenge on our hands. So there is much to discuss on this issue, and in order to allow for dialogue, I am going to end my remarks here.

And again I want to thank our witnesses for appearing before the subcommittee and to you, Mr. Chairman, for holding this hearing, and I yield back.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Mr. Langevin.

Before we begin, I would like to remind our witnesses that your written statements will be submitted for the record, so we ask that you summarize your comments to 5 minutes or less.

Admiral Rogers, we begin with you.

STATEMENT OF ADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND

Admiral ROGERS. Thank you, sir.

Chairman Wilson, Ranking Member Langevin, and distinguished members of the committee, I am honored to appear before you today to discuss our military cybersecurity posture, and I would like to thank you for convening this forum.

I am equally pleased to be sitting alongside my colleagues from each of the four service components of the United States Cyber Command. It gives me great pride to appear before you today to highlight and commend the accomplishments of the uniformed and civilian personnel of U.S. Cyber Command and its components, and I am both grateful for and humbled by the opportunity that I have been given to lead this cyber team.

The current threat environment is, as you have just described in your opening remarks, uncertain. That said, we are certain of one particular thing, and that is the pervasive nature of these cyber threats and the sophistication of the adversaries we face. Our military networks are probed for vulnerabilities literally thousands of times a day. The very assets within our military that provide us formidable advantages over adversaries are precisely the reason that our enemies seek to map, understand, exploit, and disrupt our global network architecture.

The cyber intruders of today not only want to disrupt our actions, but they seek to establish a permanent presence on our networks. Quite simply, threats and vulnerabilities are changing and expanding at an accelerating and significant pace. Compounding this threat is the fact that we are dependent on cyberspace. Operating freely and securely in cyberspace is critical to not only our military and our government, but also to the private sector, which is respon-

sible for maintaining much of our Nation's critical infrastructure to including that of key parts of the Department of Defense.

The bottom line is weakness in cyberspace has the potential to hold back our success in every field where our [Nation] is engaged. And I would like to focus in our comments today on the progress we have made so far, the achievements that we are doing in the operational arena, and what I think is the way ahead, and I look forward to that discussion.

With that, I will conclude my opening remarks.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 35.]

Mr. WILSON OF SOUTH CAROLINA. Thank you very much.

And General Cardon.

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

General CARDON. Chairman Wilson, Ranking Member Langevin, members of the committee, it is an honor to be here on behalf of the U.S. Army Cyber Command and Second Army alongside Admiral Rogers and my fellow commanders.

We appreciate the work of this committee to protect the American people from emerging threats and ensure our military has the capabilities we need to defend the Nation. Over the last few years we have had tremendous momentum, both within the institution and operationalizing cyberspace, but a lot of work remains. For the institution, we have consolidated cyberspace under one commander. We have created the Cyber Center of Excellence in Fort Gordon, Georgia, and the Army Cyber Institute at the United States Military Academy.

The Army is currently establishing the necessary frameworks to build capabilities for the Army, and by extension, the Joint Force. Operationally, we are making progress with mission-focused approaches supporting Army and combatant commanders. We made progress this year developing the Army's portion of the Cyber Mission Force with 25 of 41 teams on mission now, and we expect to have all 41 on mission by the end of fiscal year 2016 as planned.

In the face of determined adversaries, though, we are employing these teams as they reach initial operating capability and will continue to bring forces and capabilities online through 2017. The threat, vulnerabilities, and missions set, demand this sense of urgency. This also includes bringing online 21 U.S. Army Reserve and Army National Guard Protection Teams that will be trained at the same standards as the Active Component cyber force.

We are going to need more personnel beyond the Cyber Mission Force to build out the support required to fully employ the Cyber Mission Force and to build capabilities for Army formations. To better manage our people, the Army created a cyber branch, and we are exploring the creation of a cyber career field for civilian personnel.

For training, we have a centrally funded joint model for individually training, but we are working to also build collective training capabilities and their associated facilities within a joint construct. For equipping the forces, we are developing and refining the necessary framework to give us the agility that we will need in pro-

gramming, resourcing, and acquisition for infrastructure platforms and tools. And for a more defensible architecture and network, we are partnered with the Army's Chief Information Officer and Defense Information Systems Agency [DISA] in the Air Force for an extensive network modernization efforts.

These are essential for the security, operation, and defense of our Department of Defense networks. We have made tremendous progress, and with your support we have the necessary program resources to continue our momentum, but we cannot delay for the struggle is on us now.

Thank you, and I will be happy to answer your questions.

[The prepared statement of General Cardon can be found in the Appendix on page 53.]

Mr. WILSON OF SOUTH CAROLINA. Thank you very much, General.

Admiral Tighe.

STATEMENT OF VADM JAN E. TIGHE, USN, COMMANDER, U.S. FLEET CYBER COMMAND/U.S. 10TH FLEET (FCC/C10F)

Admiral TIGHE. Chairman Wilson, Ranking Member Langevin, and distinguished members of the subcommittee, thank you for your support to our military and the opportunity to appear before you today.

Since my Fleet Cyber Command predecessor, Admiral Mike Rogers, last testified before this subcommittee in July of 2012, the Department of Defense, U.S. Cyber Command, and the service components have significantly matured our operations and cyber operational capabilities. I appreciate the opportunity to outline Navy-specific progress over the past 2 years, where we are headed to address an ever-increasing threat, and how budgetary uncertainty is likely to impact our progress and operations.

Fleet Cyber Command directs the operations to secure, operate, and defend Navy networks within the Department of Defense Information Network [DODIN]. We operate Navy networks as a warfighting platform which must be aggressively defended from intrusion, exploitation, and attack. The Navy network consists of more than 500,000 end user devices, approximately 75,000 network devices, and nearly 45,000 applications and systems across 3 security enclaves.

We have transformed the way we operate and defend over the past 2 years based on operational lessons learned. Specifically, beginning in summer of 2013, we, with Admiral Rogers at the helm at the time, fought through an adversary intrusion into Navy's unclassified network.

Under the named operation known as Operation Rolling Tide, Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy commanders, U.S. Cyber Command, the National Security Agency, the Defense Information Security Agency, and our fellow cyber service components. Although any intrusion upon our network is troubling, this operation served as a learning opportunity that has both matured the way we operate and defend our networks and simultaneously highlighted gaps both in cybersecurity posture and in our defensive operational capabilities.

As a result of this operation and other cybersecurity initiatives inside of the Navy, we have already made, proposed, or planned for a nearly $1 billion investment between the years of fiscal year 2014 and fiscal year 2020 that will greatly reduce the risk of successful cyberspace operations against Navy networks. Of course, these investments are built on the premise that our future budgets will not be drastically reduced by sequestration.

Specifically, if budget uncertainty continues, we will have an increasingly difficult time addressing this very real and present danger to our national security and maritime warfighting capabilities. Operationally, and on a 24-by-7 and 365 days a year, Fleet Cyber Command is focused on configuring and operating layered defense in-depth capabilities to prevent malicious actors from gaining access to our Navy networks in collaboration and cooperation with our sister services, U.S. Cyber Command, Joint Forces Headquarters-DODIN, DISA, and the National Security Agency. Additionally we are driving towards expanded cyber situational awareness to inform our network maneuvers and reduce risk in this space.

As you know, Navy and other service components are building the maneuver elements in the Cyber Mission Force for U.S. Cyber Command by manning, training, and certifying teams to the U.S. Cyber Command standards. The Navy is currently on track to have personnel assigned for all 40 teams, all 40 of the Navy-sourced Cyber Mission Force teams in 2016, with full operational capability in the following year.

Additionally, between now and 2018, an additional 298 cyber Reserve billets will also augment the cyber force manning plan. In delivering on both U.S. Cyber Command's and the U.S. Navy's requirements in cyberspace, I am fortunate to have these component commanders as partners in addition to the many organizations who are not represented here but are every bit a member of team cyber.

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

[The prepared statement of Admiral Tighe can be found in the Appendix on page 66.]

Mr. WILSON OF SOUTH CAROLINA. Thank you, Admiral, very much.

And General O'Donohue.

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

General O'DONOHUE. Thank you, sir.

Chairman Wilson, Ranking Member Langevin, and distinguished members of this subcommittee, it is an honor to appear before you today. On behalf of your Marines, our civilian Marines, and their families, I thank you for your continued support as we pursue a multi-year joint cyberspace strategy.

Marines have a legacy of operating in any clime or place. Whether at sea with the Navy, or working shoulder to shoulder with our joint, interagency, and coalition partners, we are standing ready to respond to crises around the globe, bringing to employ combined arms across the air, land, and sea domains. We are now entering

an era of transition where the cyber domain will be fully integrated in the same way.

Our Commandant has laid out a clear vision to increase the capacity and capability of the Marine Air-Ground Task Force to fully integrate cyberspace operations. MARFORCYBER [U.S. Marine Corps Forces Cyberspace] is leading the effort to ensure that we institutionalize this vision across the Marine Corps, to include by participating in over 30 exercises last year. As a service component to U.S. Cyber Command, MARFORCYBER in conjunction with its service partners, conducts full-spectrum cyberspace operations to enable freedom of action across the cyberspace domain and deny the same to our adversaries. Additionally, MARFORCYBER provides direct support to United States Special Operations Command's missions worldwide.

To support these operations, we are building the Cyber Mission Force, and these forces are achieving operational outcomes today. These achievements are helping us to shape the vision for the future of cyberspace operations for the Marine Corps, as part of the joint, interagency, and combined force.

Last June, U.S. Cyber Command certified our first Cyber Mission Team and our first national Cyber Protection Team. During this time our second Cyber Mission Team reached its initial operation capability. MARFORCYBER is on track to have over 75 percent of its teams resourced by the end of 2015. To expedite this force build, the Marine Corps has dedicated 16 percent of its retention bonuses for our cyberspace professionals. And based on lessons learned, we have streamlined our personnel and training pipeline as we deal with the surge requirements of a startup force.

In addition, we have expanded the opportunities and developed procedures for our teams to work with increasing effectiveness across the joint and interagency force. This has been a combat multiplier. At the bottom line, we are fielding the cyber forces required by our strategy and provided by the President's budget, ready, on time, and with increasing operability in ways that we had not imagined. As we build the force, MARFORCYBER is achieving operational outcomes in stride by supporting joint, interagency, and coalition partners at home and overseas. Every day we are planning cyberspace operations, defending the network, and standing ready when directed by U.S. Cyber Command to conduct offensive cyberspace operations. Increasingly, combatant commanders and special operation forces now see cyberspace operations not as a special staff function, but essential to everything that warfighters do.

Currently, we are pursuing a considered joint and service strategy for the multi-year development of a unified network that will facilitate command and control, provide real-time situational awareness, and assist with decision support to commanders at all levels. For the Marine Corps, this network will be optimized for operational support to forces as they are deployed across the globe and as they train for crisis response. In an unstable and unpredictable security environment, the Marines provide a ready, forward, expeditionary extension of cyber capability for the joint, interagency, and combined force.

Thank you for the opportunity to appear before you today, and thank you for your continued support to our national treasure, our

Marine civilians and their families, I look forward to answering your questions.

[The prepared statement of General O'Donohue can be found in the Appendix on page 79.]

Mr. WILSON OF SOUTH CAROLINA. General, thank you very much.

And General Wilson.

STATEMENT OF MAJ GEN BURKE E. WILSON, USAF, COMMANDER, AIR FORCES CYBER AND 24TH AIR FORCE

General WILSON. Chairman Wilson, Ranking Member Langevin, and distinguished members of the subcommittee, thank you for the opportunity to appear before you today with my fellow commanders.

It is an honor to represent the outstanding men and women of Air Forces Cyber and 24th Air Force. I am extremely proud of the work our airmen, officers, enlisted, and civilians do each and every day to field and employ cyber capabilities in support of combatant and Air Force commanders. In the interest of time, let me share just a few examples to highlight how our airmen are making positive lasting impacts to our Nation.

Since we last briefed the subcommittee, the Air Force completed migration of our unclassified networks from many disparate systems into a single architecture. We transitioned over 644,000 users across more than 250 geographic locations to a single network and reduced over 100 Internet access points into a more streamlined 16 gateways. The end result has been a more reliable, affordable, and most importantly, defensible network.

The Air Force has also championed the fielding of next-generation technology by partnering with the Army and Defense Information Systems Agency to support the transition to a Joint Information Environment [JIE]. Together we are implementing Joint Regional Security Stacks and making enhancements to our networks in order to achieve a single DOD security architecture. The combined team achieved a critical milestone last September when they fielded their first security stack, and we have continued to push hard on these efforts, which will benefit the entire Department by reducing our network attack surface and increasing network capacity and capabilities.

Like the other services, we have made significant progress towards fielding and employing our initial Cyber Mission Forces. Today, Air Forces Cyber has 15 teams that achieved initial operating capability, and 2 teams have reached full operating capability. In addition to providing unprecedented support to joint and coalition combat forces in Afghanistan and Syria, these cyber forces are wholly engaged in support of combatant and Air Force commanders around the world, as well as in defense of the Nation.

I am proud to report our Air Reserve Component is a full partner in the Cyber Mission Force build, in addition to our other day-to-day cyber operations. We are leveraging traditional reservists, Air Reserve technicians, and Air National Guardsmen across the command to meet our warfighting commitments. Whether it is commanding and controlling cyber forces from one of our operation centers, deploying as part of our combat communications team, installing cyber infrastructure around the world, or any other task, each

of our total force members meet the same demanding standards and serve alongside our Active Duty counterparts. In my humble opinion, it is a tremendous example of total force integration in action.

The Air Force has also instituted several key initiatives to better recruit, develop, and retain our cyber forces. Most recently, we approved a Stripes for Certifications Program which provides the opportunity for candidates to enlist at a higher grade when entering the Air Force with desired cyber-related certifications. We have also continued our selective reenlistment bonus program to provide additional incentives for enlisted members to continue to serve in the demanding cyber and intelligence specialties.

For our officers, we have complemented the cyber warfare operations career track which we established several years ago with a new cyber intermediate leadership program. The objective is to identify qualified cyber and intelligence officers and provide them the right professional growth opportunities. We held our first board just recently and competitively selected 83 majors and senior captains from across the cyber fields to serve in key command and operational positions, many as integral members of the Cyber Mission Force.

And finally, we continue to support a host of initiatives aimed at improving the outreach to our Nation's youngest generation. I would like to highlight just one that will be culminating here in DC on March 12. It is called CyberPatriot and sponsored by the Air Force Association in partnership with local high schools and middle schools around the country, several industry partners, as well as cyber professionals from the Air Force.

CyberPatriot's goal is to inspire students to pursue careers in cybersecurity or other STEM [science, technology, engineering, and mathematics] career fields. At the beginning of the school year in September, over 2,100 teams, 2,100 teams, involving nearly 10,000 students in the U.S., Canada, United Kingdom, and our DOD schools overseas, participated in cyber training and competitions. We have seen a 40 percent increase in participation this year. As I mentioned, CyberPatriot will culminate here locally at the National Harbor with 28 teams competing in the national finals. Students will earn national recognition and scholarships. Without a doubt, the program is an exemplar of how public-private partnership can make a real difference. Personally, it has been rewarding to see our airmen giving back to our younger generation.

These are just a handful of examples to share how our airmen are pushing hard to increase cyber capability and capacity across the command. Believe me, Air Forces Cyber and 24th Air Force are all in and fully committed to the mission.

Our cyber force is more capable than ever before and continues to get better every day. None of this would be possible without your continued support. As you have heard from my counterparts, the need for the support will only increase in importance as we move forward. It is clear 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. Simply put, our cyber warriors truly are professionals in every sense of the word, and they deserve our full support.

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

[The prepared statement of General Wilson can be found in the Appendix on page 87.]

Mr. WILSON OF SOUTH CAROLINA. Thank you very much, General, and that was fascinating to find out about the involvement of students. What a great opportunity. And I know it has to be reassuring to the American people, your service, your personnel, the families that are supportive of your personnel, and I just thank each of you for protecting American families and advancing our national security.

We will now go into our round of 5 minutes of each member. Kevin Gates, who is our professional staff person, will keep the time. Members of Congress need timekeepers more than other people, beginning with me.

And so as we begin, Admiral Rogers, given the increasing and evolving cyber threats, what are critical steps that Congress can do to enable CYBERCOM accomplish your mission?

Admiral ROGERS. My first comment would be ensure a steady resource stream here. If you look at sequestration, the implications of the Budget Control Act for us, if you executed that, would have significant impact on our ability to execute the operational vision and would have impact on our ability to defend our own Department's networks, the expectation from the rest of the Nation that the Department of Defense is going to be there to provide capability to defend critical U.S. infrastructure.

It will slow and in some cases stop our ability to generate teams. It will lead us into contractual default issues. For example, we are in a MILCON [military construction] project right now that you have funded to actually create physical infrastructure for U.S. Cyber Command. Because we are new, we have only funded two out of the three years of that, so if we have another issue with that we will have contractual issues.

Bottom line, though, our ability to defend the Nation and our Department from a cyber perspective in the world that we are facing, with the threats we are facing, is significantly impacted if we can't sustain the resource budget picture that we have developed.

Mr. WILSON OF SOUTH CAROLINA. And I share your concern to the point it would be very helpful to me, Admiral, if you could provide a written response to that question which specifically would address specific delays and levels of confusion. Our colleagues need to know this because it is not as appreciated, I think, as it should be. So that would be very helpful.

Admiral ROGERS. Yes, sir.

[The information referred to is for official use only and retained in the committee files.]

Mr. WILSON OF SOUTH CAROLINA. Admiral Tighe, in your testimony you mentioned designing resiliency in programs through common standards and protocols. Could you give us an example of what you mean by that?

For the others, how do you think that we will be able to measure the resiliency of your programs?

Admiral TIGHE. Yes, Chairman.

Our approach to building in resiliency runs the gamut from technological innovation in our networks to the notion of fighting through cyber attacks when we are under attack. The people, the processes that we have, the method by which we fight through a cyber attack, is really a very large part of our warfighting approach to how we defend our networks.

And so when we talk about the technological side, that is about getting the capabilities from the boundary of the Internet all the way down to our individual host systems in a way that we can monitor and understand our own networks, and monitor and understand any threats that may be traversing through our networks. And so having that built in, which many of those new capabilities are coming in as a result of Operation Rolling Tide, we have learned where we had gaps and are instituting some of those defense-in-depth capabilities and standardizing interfaces across systems and networks that talk to each other.

Beyond our corporate networks that I am responsible for operating and defending, as you know, we have many applications, weapons systems, and other types of systems in the Navy that are necessary to accomplish our mission that hang off of our networks. And so making sure we understand how we are interfacing with those networks, how we are extending our protections to them, is a big part of our program and budget subnet in building those capabilities in and codifying across all of the acquisition commands who build systems for the Navy, building on technology, building on operating systems, all coming potentially with cyber vulnerabilities if we haven't built it into the front end of that acquisition process.

So in summary, I think the resiliency that we are looking for includes both the technological advances we have planned into our system and how we organize and defend with the personnel and the analytic capability to understand what is going on in our network so we can respond quickly.

Mr. WILSON OF SOUTH CAROLINA. Well, we certainly appreciate your professionalism. And this is going to be a really quick question, General Cardon. What is the status of establishing the Cyber Command in the district, in the community next door to me at Fort Gordon, Georgia?

General CARDON. Sir, we have a $90 million appropriation that should break ground here October, November of this year. So we are really excited about that. That will be the focal point for cyber for the Army.

Mr. WILSON OF SOUTH CAROLINA. Central Savannah area is really looking forward to your presence.

I now proceed to Congressman Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

Again, thanks to all of our witnesses. Admiral Rogers, I would like to start with you if I could, on your perspective on initiatives become more and more acute in recent years. I don't think anyone would argue that we as a Nation have developed and continue to develop some exquisite capabilities in cyberspace. It is without question.

However, I am concerned that we are developing capabilities faster than we develop the doctrine and policy that guides their

use. And, we all would agree that cyber operations obviously are critical to how we operate now and in the future, but there appears to be a real need for greater definition of legal structures for cyber activities and operations in defense of the Nation.

And there appears to even more of a gray area around support of civil authorities when it is not under a Title 10 construct with a Title 32, 50, 18 or 5 drill status, or how we utilize our Reserve Components and many of the ways that our service men and women can interface outside the DOD.

So my question for you, can you speak to your command's efforts to work through these policy challenges?

Admiral ROGERS. So, I think you raised some significant issues. Clearly they are much broader than just U.S. Cyber Command, although we are an important part of this dialogue, we are an important part of this process. If I could, I will start with the second half first and then work my way back.

In terms of how we make sure that we are maximizing the capabilities that we are building across the total force from the Reserve, the Guard, and the Active Component, particularly as you have indicated, when are applying it outside the Title 10 framework, the argument, you know, my part of the discussion is, look, we have a very competent, mature structure in the form of defense support to civil authorities that we currently use already in many other mission areas in the Department.

I think that is a good starting point for us when we look at how we are going to apply capability in Title 18, Title 5, Title 52. So I think there is a good framework for us to build around, and that is kind of the starting position, if you will, that we are taking as a Department, broadly speaking.

The first part of the question that you raised about how do we make sure that even as we are generating capability we are also thinking about the doctrine and the legal authority, if you will, that helps frame how we apply it in a way that maximizes outcomes and it does it in a framework that we are all comfortable with.

I think on the doctrinal side, I am pretty comfortable that we have got a broad vision. If you look, we have got publications. We have got a broad dialogue about how we are going to do it. I think the biggest challenge in some ways that we are still trying to wrestle our way through here is if we are going to generate or apply these capabilities outside the DOD framework, let's say in defending critical U.S. infrastructure, that is an area that we still have to work through the details.

Okay, so what is the legal and policy framework that we are going to use? I am comfortable that in a crisis we will work our way through it, but the point I am trying to make is we don't want to wait until a crisis to do this. You want to have this all laid out. You want the private sector to understand it. You want the rest of our governmental partners, because we are going to do this teaming with others in the government, DHS [Department of Homeland Security], FBI [Federal Bureau of Investigation], other partners, and we want to make sure that we have laid that all out in advance.

So there is a variety of steps we are taking between exercises, between ongoing policy deliberations, and through the legal frameworks we are trying to create, for example, what the Congress is looking at for cyber information-sharing legislation. That is all a part of the efforts we are trying to move forward to address the important issue that you have highlighted.

Mr. LANGEVIN. Well, thank you. I hope we can continue to work through those things. And that is something that I want to pay particular close attention to. So thank you for where we are right now, and I look forward to continuing this dialogue.

Cybersecurity obviously is an incredibly important field, but it also has lots of synergies with other areas of DOD activities, SIGINT [signals intelligence], electronic warfare [EW], information operations, and many more.

General, if I could ask you, I know the Army has recognized this in particular with their doctrinal recognition of the merging of cyber and EW, and certainly the Navy's Information Dominance community is in this as well, as our Navy witnesses know quite personally.

So my question is, are the interactions between cyber and these communities clear or ad hoc, and how do training, manning, and equipping get balanced across these synergistic investments? Are we building cyber in concert with or on the shoulders of these other communities?

General CARDON. In this case we have doctrine, we call it CEMA, cyber electromagnetic capabilities. And we built these organizations into our Army service component commands, corps, divisions, and brigades.

Now, the capabilities to deliver all that don't fully exist yet, because we have recognized this convergence. But, for example, we already have experiences using this in some of the war zones, former war zones, such as Iraq, where you had CREW [counter radio-controlled improvised explosive device electronic warfare] devices to protect against IEDs [improvised explosive device], tactical SIGINT forces. And it is really how do you organize these in time and space to accomplish a specific mission?

So we are trying to harness what we have learned in Iraq and Afghanistan, and what we are learning today and bring that forward. I think this is a journey, and we still have a lot of work to do on what are the additional capabilities we need at those levels.

Mr. LANGEVIN. Thank you.

Mr. WILSON OF SOUTH CAROLINA. Thank you very much, Mr. Langevin.

We now proceed to Navy SEAL [Sea-Air-Land] veteran, Congressman Ryan Zinke of Montana.

Mr. ZINKE. Thank you Mr. Chairman.

You know, from the perspective of a ground-pounder, you know, I was just a frogman, it seems to me when you say your ability to defend the Nation, and I am concerned about the chain of command. You know, we have had earlier discussions about, you know, what is the difference whether a missile attack is incoming or whether it hits a military facility or a piece of our major infrastructure or our banking system, it is an attack.

And I am concerned that the chain of command doesn't allow you to quickly react to an attack because somehow we have to go through and determine whether it is a bank or whether it is a—you know, what article it is under. And it seems to me that we need to take a fast look at this and so we are not responding to a crisis, but preparing for what we will, I think most in this room believe, is an eventual attack.

So I guess my question is are you comfortable with the current—your current ability to defend this Nation and the shipyards and infrastructure and everything there is, the cyber? And if you are not, what are the benefits of looking at streamlining our chain of command and so we can have accountability, we can have, you know, cost and efficiency? What do you see as the path forward?

Admiral ROGERS. So if I could, Congressman, let me take a look at—give you an initial thought. The positive side, in my mind, is we have clearly delineated who has what responsibilities. And I say that, if we go back 2, 3 years ago, we literally spent years debating about who was going to have what role. And it literally probably took us 2 years to generate an internal consensus as to who was going to do what.

The positive side for me—I have now been in command coming up on approximately a year. The positive side for me is, hey, we have moved beyond a discussion of who ought to do what to, okay, now we have clearly identified who has what responsibilities. Now let's roll up our sleeves and focus on how we are going to make this work. Clearly we are not where we want to be yet.

The argument—not the argument—the point I try to make to my DHS because the vision as currently constructed is DOD will apply its capabilities in a supporting role, if you will, with DHS largely being the supported entity within the Federal Government as having the primary responsibility for cybersecurity outside the dot.gov domain, if you will, in the broader civilian infrastructure.

The point I am making with my teammates at DHS and the FBI, for example, are my military culture teaches me you got to train, you got to exercise, you got to get down to the execution level of detail, and you got to do that all before the crisis. You know, as you have learned in your own life, discovery learning while moving to contact is an incredibly bad way to go about generating insights and getting more proficient at the mission.

What I would suggest is we need to make this current. We need to wring this current system out, and before we go back again and spend more time on this, and one of the inputs I have provided is, hold us accountable for executing what we have created. And if in that experience we come to the conclusion that, hey, we made some assumptions that turned out to be flawed, then we ought to step back and relook at it. But for me at least, I am not there yet.

Mr. ZINKE. Thank you, sir.

Mr. Chairman, I yield the remaining part of my time.

I look forward to working with you on this and support you in any way I can.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Congressman Zinke.

We now proceed to Congressman Joaquin Castro of Texas.

Mr. CASTRO. Thank you, Chairman, and thank each of you for offering your testimony today.

Welcome to Washington. I know you all are here frequently.

A special welcome to Major General Wilson, who is in from San Antonio, Texas, Lackland Air Force Base. We are very proud of the work you all are doing there.

Let me ask you all a question about training people in cybersecurity in our country because this issue and the need for that skill is only going to become more pronounced in the coming years.

This Congress is in the process of taking up our big education reauthorization bill for example, ESEA [Elementary and Secondary Education Act]. What programs in our school should we be expanding or growing, not only in our high schools, but also in our colleges, to prepare more students to take on roles in cybersecurity and so that you all have a pipeline of qualified people who can take on these jobs, a job that is becoming more in demand not just in the military or in government, but also in the private sector? And I will open it up.

Admiral ROGERS. Why don't you take that first cut because you have done some interesting work at the high school level.

General WILSON. Thank you, sir.

When you look at the young generation, really it's a STEM problem we have seen for years, no matter what the mission that we need in the DOD. And so when you take a look at it, you have got to get young folks excited about cybersecurity in this case. And what we find is is they yearn for interaction with people that are really doing the job. And it is fascinating to watch them in front of young airmen. It would be the same with a soldier, sailor, marine—it wouldn't make any difference—to be able to share, to put an 18-, 19-, 20-year-old in front of them because it is not hard for them to project themselves in the roles that we do every day.

And so what we found, probably the most successful, is this CyberPatriot. There is others like it. We have a Troops for Teens program there in San Antonio, that you are familiar with, sir. When we are able to interact with the schools at the grassroots level, seems to be the most effective. I would argue the CyberPatriot is very effective because we bring private industry in to enable from a funding perspective, so they are able to partner in the private—public-private partnership. We find that to be very, very powerful.

So in our case, I am proud to be wearing an Air Force uniform and that the Air Force Association sponsors the CyberPatriot program. We think we got a good thing going there. But the feedback from the local schools, teachers, mentors that we bring in to work with the kids, they just need more mentors. They need more attention.

And so while we can put more curriculum in place, that is a wonderful thing, to get kids excited, and I will give you just a couple of statistics in some of the, you know, studies that we have looked at in terms of kids that are coming out of the CyberPatriot program, the national average is typically 9 to 15 percent, depending, kids that are interested in cybersecurity or other STEM fields just across the student population.

We are seeing about those numbers when kids come in, but we are seeing graduates out of CyberPatriot at the 80, 85 percent rate that are interested in cybersecurity or STEM degrees when they go off to college. You could argue maybe that is because of the people that are joining the program. But I would argue that when you look at the caliber and the content of what they know when they walk in the door—they don't know a lot about cybersecurity—and when they walk out the door, they know a lot about it. And so it is getting them motivated. I think they can see themselves in those career fields. And so that exposure—the biggest reason we saw a 40 percent increase this year is we got into the middle schools. We incorporated the middle schools into the CyberPatriot program. Next year we are going to take a stab at the upper tiers of the elementary school and get them excited about doing cybersecurity.

I would argue that all of the services have similar programs, you know, and sometimes it is about flying or space out in the Air Force. Cyber is one of those. It is an exciting career field, and people see themselves in it.

And so I think that is the key, is to get our young folks excited about what the potential is for them.

Mr. CASTRO. Sure.

Admiral TIGHE. Congressman, if I may, I think the point on the STEM is really, really important. And as early as we can get the STEM, get our young kids motivated in STEM, the better. We need them to be comfortable with technology and be comfortable as analysts, if you will.

We have to connect the dots a lot of time. We need our workforce to be able to connect dots, not just understand technology but understand what is really happening when you don't have the full picture.

And so the STEM programs tend to do that for our young people. I think at the same time—so puzzles and things of that nature. But I think at the same time there are also programs that we have been able to leverage sponsored by National Science Foundation and others. Scholarships For Service is a program that gets graduate-level education and college education and contributes to that education with a stipend, for example, but then they come into the Federal service in cyberspace. And so some of those kinds of programs are also, I think, very valuable in exposing our young people and our college-age students to cybersecurity challenges, but also sort of bringing them into the government as a first job.

Mr. CASTRO. Thank you very much. I yield back.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Congressman Castro.

We now proceed to Congressman Doug Lamborn of Colorado.

Mr. LAMBORN. Thank you, Mr. Chairman.

And I would like to build on this theme of education. Admiral Rogers, the University of Colorado at Colorado Springs in my district and the Army Reserve just announced a partnership to educate cyber warriors. Is this a good model, and should we support it?

Admiral ROGERS. Well, let me be honest, Congressman, I don't know the details of the model, so I am not in a good position to tell you is it good or bad. Having said that, one of my takeaways

in this area is clearly this is all about partnerships, and those partnerships have to include the private sector but not just the corporate or network owners, if you will, the educational piece, the academic piece, the ability to generate insights to go to the doctrine and the policy kinds of issues we had talked before.

I try to remind people, look, this has got to be a broader discussion. Look at, for example, some of the initial work we did in the nuclear world when we were first trying to develop deterrence theory that we take for granted now. The academic world played a huge role in that if you go back 50, 60 years. I would like to see us do the same thing.

And the other thing that concerns me about the academic world is, and one reason why I as a commander, I spend a fair amount of time at academic institutions from collegiate level down to I was just at a charter school in Harlem yesterday, as a matter of fact, as a follow-on to some work I was doing in New York City. As I remind them, you are educating our workforce. I have a vested interest in partnering with you to help us do that because the technology we use is important. And clearly, we can't execute our mission without it, but where we really gain our advantage, our true strength, is in the men and women who apply that technology.

Mr. LAMBORN. Okay. Thank you. And obviously this is something I think we are all really excited about pursuing.

General Wilson, recently I visited the 561st Network Operations Squadron which is in my district at Air Force Base Peterson, and they told me that their structure and approach to network cybersecurity could be a model for the other service branches. Is that something you would agree with, and if so, why?

General WILSON. So, sir, I think you were with Lieutenant Colonel Rocky Rockwell and the team of the 561st.

Mr. LAMBORN. That's right.

General WILSON. Thank you for visiting. They really enjoyed the visit.

Sir, what they were referring to was this migration that I hinted at, getting the Air Force network, which is part of our larger DOD information network, to one centrally managed with a single architecture, which is really an early interim step towards the Joint Information Environment. So we are huge believers in it.

Many of the lessons that we learned out of the migration actually have been incorporated with the Army and with DISA and with all the services as we look at the JIE, this Joint Information Environment architecture, and the way that we are transitioning all of our networks. And so, it is a model. I think there is a lot of good, hard lessons. The team that you met at the 561st, we have a sister unit that is the 26th down in Montgomery, Alabama, at Gunter Air Force Base, is actually formed, about 40 people are on the joint management team that are working to transition with JIE.

And so we have taken the lessons from the people that have the bruises from going through a transition of that magnitude and trying to apply that to the JIE so that we are successful. So I absolutely believe that it is directly applicable, and we are excited about moving forward.

Mr. LAMBORN. Well, I know that there can be value with each service branch learning its own lessons and standing something up.

But on the other hand, there is also on the other side of the balance, why reinvent the wheel? If one of the branches has really done forward work, maybe that should be a model for others to follow.

General WILSON. So, sir, JIE, which we have all bought into in terms of the services, is really the next generation beyond where we are at today in the Air Force. And so it is really the interim step. So we shouldn't be satisfied with where the Air Force is. We need even a more defensible network. It is the best we can do with decades-old, 5-year-old technology. We need to move the DOD forward with the newer technologies, the next generation technologies, cloud architectures, single security stacks through our gateway, if that makes sense.

Mr. LAMBORN. Thank you. Thank you all for your service.

Mr. WILSON OF SOUTH CAROLINA. Thank you very much, Congressman Lamborn.

We now proceed with Congresswoman Elise Stefanik of New York.

Ms. STEFANIK. Thank you, Mr. Chairman, and thank you to all of our witnesses here today for your service and the time you took to prepare for today's hearing.

My question is for Lieutenant General Cardon. Last month at a conference you discussed the military's need for flexibility, it is something we hear quite often, and that the traditional top-down way of operating is a challenge in its organizational approach, especially as it relates to cybersecurity. Can you explain this further? And then I am also interested in how this is applicable to the current mission in Afghanistan.

General CARDON. So I come at it from an operational approach, and so the challenge in operations is what level of a centralization do you need, and what level of decentralization do you need. And so some operations require a high degree of centralization, and some operations work best decentralized.

The art is figuring out which one is most applicable. And in cyber, I think we have a centralized framework with a decentralized execution. But I will go further building on what Admiral Rogers talked about. It is when you start to bring coalition and private, because this affects—it affects all of us, so anything that happens to any one of us, all of us are talking to each other here, and with CYBERCOM it is going wider because everyone could have this same problem.

So you create more like a fusion cell. I describe it as being mission focused, not organizationally focused. So everyone looks at the mission, everyone is working on the problem. So when you take an example something like Heartbleed, which was a severe vulnerability that affected everyone, not just in the military but in private industry, that is a fusion sort of approach. Looks different inside the military, but everyone was working on this problem across the country.

In Afghanistan, operations are very decentralized. There is a limited amount of capability. It is prioritized by General Campbell, and then we use it accordingly. And so the decentralized nature of the operations there, often driven by the terrain, has I think been pretty effective.

Ms. STEFANIK. Thank you very much.

My second question relates to sequestration and funding at Budget Control Act [BCA] levels. Can you talk about what the risks are to the Army networks campaign plans, network modernization efforts, should the DOD and the Army have to execute funding at BCA levels?

General CARDON. So General Wilson just talked about the Air Force collapsing their networks, and the Army has not yet done that, and that is why we are partnered with the Air Force to do that.

So the Army would take about a $6 billion reduction off the top. That is going to affect training. It is going to affect our network modernization. It is going to affect our installation support, and it is going to affect the procurement of weapon systems. More importantly, it is the software upgrades that we need to do to those weapons systems to reduce cyber vulnerabilities.

If the cuts stay, the Army is also going to have to cut force structure. That is estimated to be 30,000. And while cyber is still ranked very high in the Department of the Army, I think it is fair to say that cyber will be part of that discussion. So this is very concerning. It is still very, very highly ranked in the departments, and it is a very high priority. But the nature of those two things together makes a very difficult problem for us.

Admiral ROGERS. Can I make one other comment on the sequestration piece? The other thing that concerns me is the longer term implication. I watched the way at U.S. Cyber Command, particularly our civilian workforce, reacted to the government shutdown in the beginning of fiscal year 2014. And as we said to them, trust us. We want you to stay with us, this is a burp. And now I watch us repeat this kind of scenario where this time it is just significant funding cuts.

One of my concerns is, does our workforce start to believe, you know, I am not so sure that there is this long-term commitment, and given the skills that I have and the fact that I could make more money going elsewhere on the outside. The other concern I have, quite frankly, is that we are going to start to see elements of our workforce, civilian and potential military, start to walk away. And as I said, the technology is incredibly powerful, but the greatest edge that we have is our men and women. And when we lose them, we have got real problems.

Ms. STEFANIK. I agree with you, Admiral, and I also share your concerns. Particularly from my perspective representing New York's 21st District, home of Fort Drum, but we are also home to not only members of the military and service men and women, but many Federal employees in the district. So I share your concerns, and we are working very hard on this committee to address the negative implications of sequestration and these cuts which are so devastating to our readiness.

Thank you.

Mr. WILSON OF SOUTH CAROLINA. And thank you very much, Congresswoman Stefanik. And Congresswoman Stefanik has been a real leader trying to address the issue of defense sequestration. We appreciate her extraordinary service.

Additionally, we appreciate your extraordinary service. And the issues that you are dealing with are so important we have another round for anyone who would like to participate.

And for each of you, in your testimony, the military and civilian personnel needed for the Cyber Mission Forces were discussed, but are there enablers out there in other communities not included in the workforce numbers which you rely on significantly?

How are these enablers faring in the budget? What impact would you expect, again, with defense sequestration on these forces?

And we can begin with the Admiral and proceed.

Admiral ROGERS. So one of my comments—and I, in fact, just raised this to the Joint Chiefs of Staff last week—was to remember cyber is much more than just the maneuver elements, the teams, if you will, that we are creating, that like every other mission set, cyber counts on a core set of enablers that we often tend to take for granted.

So rather than take a lot of time, I will highlight one area to you, and that, for example, is the power of intelligence, the fact that we rely on a broader intelligence structure to generate knowledge and insight about what is going on in our cyber environment and we use that insight then to apply this capability we're generating.

Without that kind of insight, we have real challenges, as we do in every other domain, about how do you maximize the effectiveness of the resources and the capabilities we have generated in this maneuver force.

So I constantly try to remind the broader set of partners that we work with in and outside the Department to it is more than just this cyber maneuver force here that we need to be thinking about.

General CARDON. Sir, enablers are really important. Often they are in high demand, low density in the Department. There is a lot of structures in place to work to prioritization. But it is truly combined arms. But I don't think we fully understand what we need yet.

And here is what I mean. When I took command, we had two teams. Today we have 25. By summer, we will have 41. The demands are growing. And how to best organize the enablers to meet all the demands that the teams are generating as the teams grow, we are working. We know we need more. To put a finite number on that yet I think is a little premature, but it is not what it is today.

Admiral TIGHE. Chairman, I would say that, from the Navy perspective, we are building the teams just like the other service components at places where I have already got commands. So I have a command structure where we are growing teams, and there are enabling functions associated with growing a large number of military people, you know, personnel, inside of a command, and civilians.

And so some of those kinds of enabling functions have not, you know, really been thought through in terms of how many career counselors do you need, how many SAPR [Sexual Assault Prevention and Response] counselors and victim advocates and those kind of things. And so certainly, when we added the Cyber Mission Force, it was all about that maneuver element.

But, in some cases, we have placed burdens on commands that may not have had sufficient capacity to deal with that growth. And so that is an area that we are definitely looking at, where we go from here in terms of both the enabling and, as Admiral Rogers said, the command and control parts of it.

General O'DONOHUE. Sir, from the Marine perspective, you know, enabling the whole force really is what cyber is. You have a certain amount of expertise represented in the specialized skills. We have folks down here with the ability of the force to train and exercise.

This comes from the resiliency aspect of it and the idea that down to the network operator level or down to the end user, he is able to operate in a contested and degraded environment, in fact, compromised, and every level of command is integrated at cyber less [audio unclear] and not just what is specifically designated as a cyber force.

So one aspect of that is the training exercises that gets a whole force and also provides an enabler to the specialists, who are the catalysts. But it has to be seen as a comprehensive capability across the force and integrated like any other combined arms.

One help for that is a persistent training environment. This helps realistically fight a network without an adversary and enable to test the force and build resiliency. Also, it has another effect in terms of acquisitions, which is another area, not so much money, certainly an acquisition program that is tailored to this new capability that we are developing.

Within the persistent training environment, you can get the collective skills across the force, but also you can test the vulnerabilities of things that we are going to acquire and bring into it in the overall operational context.

General WILSON. Sir, I would just echo a couple of things and add a few.

One is integrated command and control has been key. We have seen that today at the tactical level, if we are able to integrate our command and control elements. That has been a challenge because we have been resourcing the maneuver element. We have not resourced the command and control. So that has been a bit of a challenge. But we see that as a key enabler tactically.

In addition, similar to the Navy, some of the support structure was not put in because of some of the sequestration cuts, if that stays. And so we have got those laid in in our current budget. So if we move back to BCA levels, that may put some stress on the support structure.

The couple things I would add is we see tremendous leverage with a Reserve Component. So our Guard and Reserve partners—they are conducting the mission every day for a couple of reasons.

One, we see tremendous talent and unique skill sets that come in the door that complement the training that we give them and the types of operations we are doing. It also offers our Active Duty members that make a decision to leave the service some options on continuing to serve by wearing a uniform and coming back in the door on a bit limited basis from just a time perspective. But we get to retain that talent and the experience.

So that has been a key enabler for us. We have been doing that for years. But we are seeing that magnified in the CMF, the Cyber Mission Force.

I would echo also we really are going through a culture change. We have a very—it is a contested, degraded, and potentially operational limited environment. And so that culture of having to operate through that kind of environment is different. And so moving the whole force—not just the cyber experts, but everyone—into that and through those training exercises and exposing them to that is key.

And then, finally, I would add it is quickly becoming a commander's business. Just like in industry, we are seeing in a C-suite business—CEOs [Chief Executive Officer], COOs [Chief Operating Officer], et cetera—it is not just the CIO's [Chief Information Officer] problem anymore. This is key. To have mission success, this has got be to a commander's business.

So it is not just the commanders sitting here representing the cyber talent, if you will, in each of the services, but the operational commanders, and getting them involved in the decision process.

What we are seeing in the Air Force is my counterparts in the other combat-numbered Air Forces are very interested and want to understand and want to be part of the solutions. And so we see that as a key enabler.

Mr. WILSON OF SOUTH CAROLINA. Well, I thank each of you.

And we now proceed to Congressman Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

And, again, thanks to our witnesses.

I have got a couple of questions. I am hoping to get to at least a couple of them. I can't get through all of them. So I am going to go as quickly as I can.

But going back to, if I could, retaining and recruiting qualified military and civilian personnel, obviously, it is critical to addressing the threat.

So my question is: What challenges do you face in recruitment and retention? And, more specifically, how are these challenges being addressed? Are special authorities needed?

For example, are enlistment bonuses, civilian hiring authorities, required to address shortfalls in recruitment and retention? And what incentives or methods have been used so far effectively to recruit and retain?

Admiral ROGERS. Let me start and then I will turn it over to my counterparts, because the services actually generate the capability, if you will, the workforce.

When I looked across the entire Cyber Mission Force, the positive side to date is that both accessions, input, if you will, across all the services is meeting target and retention—knock on wood—is actually higher in some ways than we had originally anticipated.

I think that is because—the thing I try to remind people is we are not going to compete on the basis of money. Where we are going to compete is the idea of ethos, culture, that, "You are doing something that matters, that you are doing something in the service of the Nation, and that we are going to give you the opportunity to do some really interesting and amazing things." I think that is how we are going to compete.

And then I would turn it over to my service teammates for the specifics they are running into.

General CARDON. Sir, to echo Admiral Rogers, we have not experienced problems with recruitment. For example, for our high-end operators, we recruited 75 percent of the year in the first quarter with no waivers and no bonuses. So there is a tremendous drive on this.

The challenge will be retention. So if I could go down, officers——

Mr. LANGEVIN. How is that going so far on the retention side, just broadly.

General CARDON. Well, we are headed into our first big bow wave because we started this about 3, 4 years ago and they are entering into the first window. I would say right now it is still unknown.

But a few indicators gave us the idea that we have to manage this as a separate branch, because before we did not count cyber. You were part of another branch and you were selected for promotion or leader development opportunities based on your expertise on that branch, not in cyber. Now you will do this with a cyber focus.

We have also recognized we need this same thing for our civilian workforce. For the civilian workforce, there is no cyber portion of this. So to advance in those, you have to advance where you were hired into as opposed to a cyber focus. So we think those will really help. We have the right tools with bonuses and all that right now to offer them, and the Army is very aggressive on this at this time.

Admiral TIGHE. I would say that the Navy is in a similarly situated position. As it pertains to recruiting, we have not been having any trouble recruiting to the numbers that we needed for all of our cyber-type missions. And on the retention side, we are doing very well, both officer and enlisted, in retaining the talent that we need.

We have the tools that everyone else uses in the Navy to incentivize any particular ratings that are low on numbers, in particular, pay grades and things like that. We use that. But I agree with Admiral Rogers that, in this mission set, it is not about the money. It is about the mission.

And so the best thing that we can do to improve retention in this space is give them the training and the tools and put them on mission because they—you know, what I am seeing in our young people and our workforce is very motivated, enthusiastic for the mission. And getting them on mission is the most important thing we can do.

Mr. LANGEVIN. I am going to hold the—General O'Donohue and General Wilson, if you can perhaps respond in writing, especially if there is something different that you are experiencing. But I wanted to get to the acquisition part.

[The information referred to can be found in the Appendix on page 102.]

Mr. LANGEVIN. Let me ask: Is the current acquisition model adaptive and flexible enough to support cyber technology innovation and rapid utilization of cyberspace capabilities? As you may know, the committee is working on acquisition reform right now. And do you have recommendations on how to ensure the process allows for innovation and rapid acquisition capabilities?

My other question, which you probably won't be able to get to, is going to be for Admiral Rogers. Are you reviewing allocation of resources in terms of—to meet the combatant commanders' requirements? How do you allocate the resources you need for these Cyber Mission Teams? So we can probably do that one for the record. But on acquisition.

[The information referred to can be found in the Appendix on page 101.]

Admiral ROGERS. So let me start on acquisition. The short answer is no. My argument is we have to change the model we are using. The rate of change is such that, within the cyber arena, we have got to account for the fact that, as we are developing and acquiring capabilities in the Department, we have got to build into that process the idea of regular and recurring update and revision, that a set of capabilities that we lock into place and then build to over time—let's say, if you look at what it takes to put a satellite into orbit, if you look at what it takes to build a major warship, for example, I mean, we are talking 5 to 10 years. And the rate of change in the cyber dynamic in 5 to 10 years is just amazing to me.

So we have to build into that program the idea that there will be a recurring refreshment rate required. We don't do that right now in the model at all. That is not the way we do business. But I think we have to get to that.

Mr. LANGEVIN. We are going through acquisition reform right now, and now would be a good time to help us to get this right.

I know my time has expired.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Mr. Langevin.

And we will proceed now to Congressman Ryan Zinke.

Mr. ZINKE. Thank you, Mr. Chairman.

I guess, as I watch the fleet numbers go down, I get concerned. I think we are all concerned. But, also, when the fleet numbers go down, we are asking our fleet to do more with less and it is much easier for our adversaries to target individual platforms.

I guess the bottom line is, if further cuts occur, do you feel that those cuts could, in fact, put our ships and our fleet that are in harm's way at further risk being unable to detect and defend a cyber attack, particularly in the western theater?

Admiral TIGHE. Congressman, I believe that all of our maritime missions, particularly those that are forward, you know, projecting power around the globe, are critically dependent on our cyber capabilities.

And we have spent the last 2 years building programs around closing the gaps in vulnerabilities and increasing our operational capabilities to assure missions around the globe that maritime commanders have to be able to do.

And so certainly what the actual CNO [Chief of Naval Operations] said during his budget testimony is, if we are held at the BCA levels, he would be hard-pressed to recommend to the Secretary that we reduce any of those investments that we have already identified and made as a commitment to our mission assurance based on the cyberspace capabilities.

But I think, as mentioned earlier, another key aspect of that is all of the modernization programs that we have across the board—

aircraft, submarines, ships, all of those modernization programs—tend to upgrade systems that are dependent on operating systems.

And when things like sequestration hits or we have a late budget, you know, getting to our acquisitions system, it ends up throwing a monkey wrench in the modernization plans. Those modernization plans are very critical to closing vulnerabilities.

So even beyond what we would call strict cyber investments, our acquisition process and focus on ensuring that our programs are not delivering vulnerable systems across the board—not just networks, but across the board—is contingent on those modernization programs going forward. So, yes, it certainly puts at risk not just the capability, but the overall mission, command and control, of Navy capabilities around the globe.

Mr. ZINKE. Thank you, Admiral.

Mr. Chairman.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Congressman Zinke.

We now proceed to Congressman Jim Cooper of Tennessee.

Mr. COOPER. Thank you, Mr. Chairman.

Within the last 2 weeks, I think it was publicized that Lenovo computer company shipped laptops already equipped with malware called Spear Phishing or something.

Isn't that kind of amazing, that a brand-new laptop would already be essentially booby-trapped that way?

Admiral ROGERS. Quite frankly, no.

Mr. COOPER. That is not amazing?

Admiral ROGERS. Again, because what I generally find over time is—for example, most of the equipments and the capabilities that we will bring onboard as a Department, we don't automatically assume that it is perfectly secure. We have a series of tests and processes that we go through.

I am not trying to imply it is for nefarious reasons. Many times we will find that, from the time it takes to actually generate and build the capacity to the time it is actually fielded, for example, you will find vulnerabilities.

For example, if you have look at Heartbleed, probably the largest vulnerability we had over the course of the summer, was based on coding from the 1980s. You find these challenges. This is not unique to the nature of the cyber arena, sir.

Mr. COOPER. Someone estimated—and I hope it is unduly pessimistic—that almost 95 percent of government IT [information technology] acquisitions were flawed or deeply flawed in some way.

Are you able at NSA [National Security Agency] to make sure you have clean equipment when you buy it?

Admiral ROGERS. NSA is part of a broader team that helps work information assurance for the Department. Having said that, the service has the overall responsibility for the manned, trained, and equipped functions for their service and broadly for the Department. But we do it as part of a broader team.

Mr. COOPER. But for your own NSA operation, you are able to make sure that all your computers are clean?

Admiral ROGERS. Yes. We spend a lot of time—as every organization does, we spend a lot of time making sure that we don't have

vulnerabilities in the systems that we are counting on to execute our mission.

Mr. COOPER. That would include system administrators like Mr. Snowden?

Admiral ROGERS. Yes. Clearly it is not a perfect system. You will never hear me say that, if that is the point we are trying to make. You will never hear me say that.

Mr. COOPER. What is good enough for government work? What is clean enough to be safe?

Admiral ROGERS. I don't know that there is a particular number that I could give you. It all boils down to what is the level of risk that we are comfortable with, what are the different processes that we can put in place to try to mitigate that. There is no single silver bullet here, as it were.

Mr. COOPER. It is risk for virtually every chip to be made overseas?

Admiral ROGERS. There is clearly an aspect of risk to it. I think that is a fair statement.

Mr. COOPER. Is it worth mitigating that risk by having more domestic manufacturers?

Admiral ROGERS. You know, clearly within the Department, we try to take a look at that. One of the ways we do it is we try to tier some of our systems, if you will. And the standard, for example, that we will use within the nuclear infrastructure is different than the infrastructure we will use for the systems we use for morale, welfare, and recreation functions within the Department.

Mr. COOPER. But a back door can come in from virtually anywhere. The Target hack was mainly the HVAC [heating, ventilation, air conditioning] contractor. Right?

Admiral ROGERS. So is it possible? Yes. There is no doubt about that.

Mr. COOPER. I don't know how many transistors are in a phone like this or chips or whatever like that, but it is surely a large number.

Admiral ROGERS. It is a complex operating system.

Mr. COOPER. So since everyone carries their own supercomputer with them, is anyone smart enough to figure out the hardware/software interface, even assuming that the hardware is perfect and clean and inviolable or——

Admiral ROGERS. Well, the way I put it is, hey, if it is designed by man, man is a flawed individual. And the idea that you are going to create something perfect in which you guarantee that there is no ability to penetrate is highly unlikely, which is why in the Department we do things like defense in depth, multiple looks at the same piece of gear many times.

We try to account for the fact that a single solution—whether it be technical, "Hey, I can create the perfect system," whether it is, "Hey, I can control my workforce and guarantee I am not going to have any issues," we try to use multiple layers.

Mr. COOPER. I guess I am still trying to get at the question of good enough for government work. When are we safe? When have we done enough of that? Do you have to red-team everything? Do you have to practice your operation without using computers? How do we——

Admiral ROGERS. I think the answer is yes, we try to do all of that. You have heard today already we talk about the idea about, for example, how are we going to operate hurt within the Department.

I think the reality of the world around us is, at least on the military dimension, it is not in our best interest to assume we will always have perfect connectivity, that we will never have any issues, we will never have any degradation. Far from it. I think quite the opposite, given the nature of the world that we are dealing with today. We have to think about how we are going to fight through things.

Mr. COOPER. Should the Defense Committee be doing more to help?

Admiral ROGERS. Well, I can use all the partners that we can get in this. Because no one single entity here is going to have all the answers to this, which is one reason why, if you look at the resource piece that the Congress holds here, the legal frameworks that we talk about, you clearly have an important role to play in all this. It won't be just us.

Mr. COOPER. Well, I hope you won't be shy about asking.

Admiral ROGERS. Yes, sir.

Mr. COOPER. Thank you, Mr. Chairman. I see my time has expired.

Mr. WILSON OF SOUTH CAROLINA. Thank you, Mr. Cooper.

As we conclude, I want to thank each of you. And it has to be reassuring to the American people to see such dedicated personnel. So thank you very much for your service on behalf of our country.

We are adjourned.

[Whereupon, at 4:51 p.m., the subcommittee was adjourned.]

A P P E N D I X

MARCH 4, 2015

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MARCH 4, 2015

Chairman Wilson Opening Statement

Hearing: Cyber Operations: Improving the Military Cyber Security Posture in an Uncertain Threat Environment

4 March 2015

Ladies and Gentleman, I call this hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee to order.

I am pleased to welcome everyone here today for this very important hearing on the fiscal year 2016 budget request for cyber operations programs for the Department of Defense. One need only read the headlines of almost any newspaper on almost any day to see the challenges we face as a nation when it comes to hacking and cyber threats. The array of threats from both state and non-state actors pose significant challenges to our military forces, our economic well-being and our diplomatic activities worldwide.

The recent Government Accountability Office report on vulnerabilities to our air traffic control networks vividly illustrate the need to work across departments, agencies and even internationally to ensure our security. We recognize that Department of Defense capabilities will be critical to those efforts, but must be provided the resources and authorities to be effective.

As we look at this budget request, and as the witnesses describe their plans for how they will execute their activities in fiscal year 2016, I ask that you address the following questions:

- What specifically are you requesting in the budget and what major initiatives do you expect to fund?
- If Defense Sequestration caps are enforced in this budget request, what impacts do you expect to see this year?
- How are you measuring or assessing the cyber security posture of Department of Defense networks and what vulnerabilities do you see?

Today, we've invited a panel that represents the top military leadership for cyber operations across the Department of Defense. Our witnesses are:

Admiral Michael Rogers
Commander, U.S. Cyber Command

Lieutenant General Edward C. Cardon
Commander, U.S. Army Cyber Command

Vice Admiral Jan Tighe
Commander, Navy Fleet Cyber Command/10th Fleet (FCC/C10F)

Major General Daniel J. O'Donohue
Commanding General, Marine Forces Cyber

And –

Major General Burke E. Wilson
Commander, 24th Air Force

Now, I'd like to invite my ranking member, Mr. Langevin, to make any comments he might have.

STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

4 MARCH 2015

Chairman Wilson, Representative Langevin, and distinguished members of the Committee, thank you for the opportunity to speak to you today on behalf of the men and women of United States Cyber Command (USCYBERCOM). This is the first time I have had the honor of testifying before this Committee in a posture hearing about our Command's dedicated uniformed and civilian personnel. It gives me not only pride but great pleasure to commend their accomplishments, and I am both grateful for and humbled by the opportunity I have been given to lead them in the important work they are doing in defense of our nation.

USCYBERCOM is a subunified command of U.S. Strategic Command; we are based at Fort Meade, Maryland. Approximately 1,100 people (military, civilians, and contractors) serve at USCYBERCOM, with a Congressionally-appropriated budget for Fiscal Year 2015 of approximately $509 million for Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON). USCYBERCOM also includes its key Service cyber components: Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Our collective missions are to direct the operation and defense of the Department of Defense's information networks while denying adversaries (when authorized) the freedom to maneuver against the United States and its allies in and through cyberspace. On a daily basis, we plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks and the Department's critical infrastructure; and prepare to and, when directed, conduct full-spectrum military cyberspace

operations in order to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace and deny the same to our adversaries.

USCYBERCOM operates with several key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The President's decision to maintain the "dual-hat" arrangement (under which the Commander of USCYBERCOM also serves as the Director of NSA/Chief, CSS) means the partnership of USCYBERCOM and NSA/CSS will continue to benefit our nation. NSA/CSS has unparalleled capabilities for detecting foreign threats, producing intelligence for our warfighters in all domains, analyzing cyber events, and guarding national security information systems. The best, and only, way to meet our nation's needs, to bring the military cyber force to life, to exercise good stewardship of our nation's resources, and to ensure respect for civil liberties and privacy, is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the time nor the resources to re-learn or re-create the capabilities that we tap now by working with our co-located NSA/CSS partners.

Let me also mention another key mission partner and neighbor at Fort Meade, the Defense Information Systems Agency (DISA). DISA is vital to the communications and the efficiency of the entire Department, and its people (especially those supporting the new Joint Force Headquarters-DoD Information Networks) operate in conjunction with us at USCYBERCOM on a constant basis. We also work with other federal government departments and agencies, particularly the Department of Homeland Security (DHS) and the Department of Justice and Federal Bureau of Investigation (FBI). We interact regularly with private industry and key allied nations as they seek to secure their networks, identify adversarial and criminal

actors and intentions, build resiliency for federal and critical infrastructure systems, and investigate the theft and manipulation of data.

Where We Were

This year we will mark the fifth anniversary of USCYBERCOM's activation. The Department authorized the creation of a Cyber Command in 2009, and accelerated its establishment the following year. This initiative was truly reflective of a broad consensus. The highest levels of our government saw potential adversaries militarizing cyberspace, mounting cyber espionage on a world-wide scale and using cyber capabilities to intimidate their neighbors. We also saw cyber efforts against DoD and realized the need to ensure our ability to defend its networks and command and control our own Department's forces and information systems. We in the U.S. military took the step of creating a new warfighting organization for cyberspace because we recognized that our nation's economy, infrastructure, and allies were incurring grave risks from digital disruption, and that potential adversaries were working aggressively to exploit those vulnerabilities. We saw unfriendly states, organized criminals, and even unaffiliated cyber actors stealing American intellectual property and using cyber means for coercion. USCYBERCOM was established to help stop such activities, or at least to minimize their effects on the United States and its allies.

USCYBERCOM confronted serious challenges from the outset. DoD networks had been planned and initially constructed decades earlier in an environment in which redundancy, resiliency, and defensibility were not always primary design characteristics. Operators in USCYBERCOM, not surprisingly, could not even see all of our networks, let alone monitor all the traffic coming into and out of them from the Internet. Our people were and are professionals,

so that issue was rapidly engaged, but nonetheless the sheer volume of work involved in starting a new, subunified command was substantial.

I have been at USCYBERCOM for approximately a year, and thus have had time to form some impressions of the organization and its progress. I knew when I took command that we had a sound foundation and could build upon it with confidence. The organizations had been well scoped and granted the authorities necessary to do our work. The bad news was that USCYBERCOM was built from the ground up by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to build mission capabilities as fast as possible. I was nonetheless pleased by the quality and dedication of the personnel across USCYBERCOM and our Service cyber components. These are professionals, in every sense of the word, and they are determined to put in place military cyber capabilities that will keep the nation safe in cyberspace. For their sake, and even more so for America's, I intend to make our organizations even stronger—and provide my successors the opportunity to do the same.

Where We Are Now

Over the last five years we have built USCYBERCOM to help defend our networks in DoD and the nation. This has not always been a straightforward process. Our Command is growing and operating at the same time, performing a multitude of tasks across a diverse and complex mission set. Of course, every command changes with events in its mission space, adjusts to evolving policies and direction, and adapts with the development of armaments and tactics. I do not want to foster the impression that we are completely unique. It is true, nonetheless, that we are constructing a new command and force while engaged on a 24-hour a day basis, every day of the year, with smart, energetic actors operating in an environment that is

highly dynamic. Some of those actors, I hasten to add, operate with no discernible legal or ethical restraints. At the same time, we are writing doctrine, training people to execute options, and keeping up with the ever-shifting topography of cyberspace. That complexity presents us—and every nation that seeks a military cyber capability—with a set of challenges that are significant.

In essence, USCYBERCOM has been "normalizing" our operations in cyberspace. We seek to afford an operational outlook and attitude to the running of the Department's roughly 7 million networked devices and 15,000 network enclaves. Collectively these represent a weapons system analogous to a carrier strike group or an aircraft strike package, through which we deliver effects. Like conventional weapons systems, our networks enable operations in other domains and distant locations, they demand constant upkeep and skillful handling, and they can be a target themselves for our adversaries. They give us the vital command and control (C2), connectivity, and intelligence for a global, 21st century military. No other nation enjoys such resources—they impart to us formidable advantages over any conceivable adversary. It is for exactly this reason that potential adversaries very much want to map, understand, exploit, and possibly disrupt our global network architecture.

In keeping with that operational mindset, we seek to impress upon commanders that cyber defense is no longer information technology (IT) it is not a mere support function that they can safely delegate to someone on their staff. Cyber is now a central part of their ability to execute their mission. It is commander's business. A successful intrusion, or severance of connectivity, can result in a direct and immediate impact to successful mission accomplishment. We have seen this happen in recent years, and though we have not yet experienced a serious,

sustained disruption to the Department's information systems, it may be only a matter of time before we face one, given the inherent vulnerability of our networks.

The fragility of that legacy architecture motivates our emphasis on deploying the Joint Information Enterprise (JIE) across DoD. We have gained significantly more visibility in our networks, but that is only a stopgap measure while the Department migrates its systems to a cloud architecture that promises to increase security and efficiency while facilitating data sharing across the enterprise. That means that the warfighter at the forward edge of battle benefits from the same data pools as our analysts, operators, and senior decisionmakers here in the United States. While the JIE is being implemented, however, our concerns about our legacy architecture collectively have spurred our formation of our new Joint Force Headquarters to defend the Department's information networks (JFHQ-DoDIN). The JFHQ-DoDIN gained then-Secretary of Defense Hagel's authorization late last year and has recently achieved initial operational capability, working at DISA under my operational control at USCYBERCOM. JFHQ-DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses. Placing the just-established JFHQ-DoDIN under USCYBERCOM gives us a direct lever for operating DoD's information systems in ways that make them easier to defend, and tougher for an adversary to affect. It also gets us closer to being able to manage risk on a system-wide basis across DoD, balancing warfighter needs for access to data and capabilities while maintaining the overall security of the enterprise

USCYBERCOM directs the operation and defense of Department of Defense networks, but it does much more as well, hence its formation of a Cyber Mission Force (CMF) to turn strategy and plans into operational outcomes. The Command's last two annual posture

statements have mentioned the CMF's authorization and initial steps, and I am pleased to report that the Force is very much a reality. With continued support from Congress, the Administration, and the Department, USCYBERCOM and its Service cyber components are now about halfway through the force build for the CMF. Indeed, many of its teams are generating capability today. Three years ago we lacked capacity; we had vision and expertise but were very thin on the ground. Today the new teams are actively guarding DoD networks and prepared, when appropriate and authorized, to help Combatant Commands deny freedom of maneuver to our adversaries in cyberspace. Dozens of teams are now operating; and even though many of them are still filling out their rosters and qualifying their personnel, they are proving their value daily as well as confirming the overall need for such a construct.

The work of building the CMF is not done yet. We have a target of about 6,200 personnel in 133 teams, with the majority achieving at least initial operational capability by the end of FY 2016. I have been working with the Services to accelerate the work we are doing to keep on schedule, but I can promise you that will not be easy. We are already hard pressed to find qualified personnel to man our CMF rosters, to get them cleared, and to get them trained and supported across all 133 teams. To address these gaps, I am working with our Service components, Chief, National Guard Bureau, and Reserve Chiefs to ensure we have considered a total force solution. In several areas, such as critical infrastructure, both USCYBERCOM and the Services have recognized that our Reserve Component brings us unique and valuable skills. In addition, we are charting the proper command and control relationships and structures for these teams, seeking to establish proper headquarters support for them, and giving my commanders insight into their activities so we can ensure the best possible synchronization, deconfliction, and unity of effort across the CMF. There are all sorts of good ideas for doing

this; indeed, we hear no shortage of suggestions. What I tell everyone, however, is that we have admired this issue long enough. For instance, it is time to implement and exercise measures like the objective C2 model that we agreed upon as a Department almost two years ago, even if we believe it may not end up as the permanent solution. Let us see how it works, and then change what needs to be fixed later as we gain insights from operations and the shifting threat.

Where we need help from you is with resources required to hire personnel to fill the team seats as well as necessary operational and strategic headquarters operations, intelligence, and planning staffs, facilities where we can train and employ them, and resources to properly equip them. Everyone involved knows this is a priority for the Department as well as for the Administration writ large. We also know that our Department in particular has a broad range of critical priorities, each of which competes with cyberspace for resources. This is a cold, hard reality—as is the fact that weaknesses in cyberspace have the potential to hold back our successes in every other field where the Department is engaged. Similarly, success in securing our networks and denying adversaries freedom of maneuver in cyberspace can and does bolster our DoD successes in all warfighting domains. That should factor into our resource decisions, particularly as we face the renewed possibility of sequestration—and mandatory, across-the-board eight percent budget cuts—when Fiscal Year 2016 begins a few months from now.

Let me emphasize the value of the intangibles in our work and our environment. Collectively we in USCYBERCOM have gained priceless experience in cyberspace operations, and that experience has given us something even more valuable: insight into how force is and can be employed in cyberspace. We have had the equivalent of a close-in fight with an adversary, which taught us how to maneuver and gain the initiative that means the difference between victory and defeat.

Enhancing such insight is increasingly urgent. Every conflict in the world today has a cyber dimension. Actors with modest conventional military capabilities have shown considerable capacity to harass, disrupt, and distract their adversaries through digital means. This is not, however, some on-line version of a Hobbesian state of nature; it is not a war of all against all. What we are seeing are clear patterns to cyber hostilities, and those patterns have four main trends:

- First, it has to be noted that autocratic governments in several regions view today's open Internet as a lethal threat to their regimes. For example—as President Obama noted last December—North Korea recently turned its cyber capabilities on Sony Pictures Entertainment in revenge for a forthcoming movie. The North Koreans employed unlawful cyber activities to steal and destroy data and property, to intimidate and coerce U.S.-based businesses, to threaten American citizens, and to disrupt free speech within the United States. This is unacceptable. Democracies value Internet freedom and a multi-stakeholder system of governance, in which the Internet is officially neutral with regard to free and open political speech—with clear protection for criticism and debate. We make no apologies for the fact that such neutrality is abhorrent to regimes that fear their own citizens; hence their ubiquitous and determined efforts to redefine "cybersecurity" to mean protection from "dangerous" ideas as well as from malicious activity.
- Second are the ongoing campaigns to steal intellectual property. Massive thefts of personal and institutional information and resources, by states and by criminals, have been observed over the last decade or so. Criminals are mining

personal information for use in identity theft schemes, in a sense committing fraud on an industrial scale. States have turned their much greater resources to theft as well. These intrusions and breaches have drawn comments from the highest levels of the U.S. Government. I would only add here the observation that the most worrisome of these campaigns are state-sponsored, persistent, and world-wide in scope. They are aimed at governments, non-profits, and corporations wherever they might be accruing intellectual capital that the attackers believe could be valuable, whether for re-sale or passage to competing firms and industries.

- The third form of cyber tactic we see is disruption. Once again, the actors, techniques, and targets of these incidents are numerous and varied, ranging from denial-of-service attacks, network traffic manipulation, and employment of destructive malware. We see these used all over the world, particularly in most or all of the conflicts pitting two armed adversaries against one another.
- Finally, we see states developing capabilities and attaining accesses for potential hostilities, perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage. Private security researchers over the last year have reported on numerous malware finds in the industrial control systems of energy sector organizations. As I suggested in my appearance before the House Permanent Select Committee on Intelligence last fall, we believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict.

Despite the spread of cyber attacks and conflicts around the world, we have increasing confidence in our operations-based approach. Though it is still developing and not yet fully implemented, it has nonetheless given us significant advantages in relation to potential adversaries. For instance, I can tell you in some detail how USCYBERCOM and our military partners dealt with the Heartbleed and "Shellshock vulnerabilities that emerged last year. These were unrelated but serious flaws inadvertently left in the software that millions of computers and networks in many nations depend upon; an attacker could exploit those vulnerabilities to steal data or take control of systems. Both of these security holes were discovered by responsible developers who did just what they should have done in response—they kept their findings quiet and worked with trusted colleagues to develop software patches as quickly as possible—allowing systems administrators to gain the jump on bad actors who read the same vulnerability announcements and immediately began devising ways to identify and exploit unpatched computers.

We at USCYBERCOM (and NSA/CSS) learned of Heartbleed and Shellshock at the same time that everyone else did. Our military networks are probed for vulnerabilities thousands of times every hour, so in both cases it was not long before we detected new probes checking our websites and systems for open locks, as it were, at the relevant doors and windows. By this point our mission partners had devised ways to filter such probes before they touched our systems. We were sheltered while we pushed out patches across DoD networks and monitored implementation, directing administrators to start with those systems that were most vulnerable. Very quickly we could determine and report how many systems had been remedied and how many remained at risk. Three years ago, DoD would have required many, many months to

assess the danger and formulate responses to Heartbleed and Shellshock. Thanks to the efforts we have made in recent years, our responses by contrast were comparatively quick, thorough, and effective, and in both cases they helped inform corresponding efforts on the civilian side of the federal government. We also know that other countries, including potential adversaries, struggled to cope with the Heartbleed and Shellshock vulnerabilities. In military affairs it is often relative speed and agility that can make a difference in operations; we demonstrated that in these instances, and in others that we can discuss in another setting.

This operational approach is what we need to be building in many more places. The nation's government and critical infrastructure networks are at risk as well, and we are finding that computer security is really an enterprise-wide project. To cite one example, the U.S. Government is moving toward cloud computing and mobile digital devices across the enterprise, and DoD and the Defense Industrial Base (DIB) are moving with this trend. We are working, moreover, to make our data as secure from insider threats as from external adversaries. This could eventually compel a recapitalization of government systems comparable to the shift toward desktops in the 1980s and local-area networks in the 1990s. In short, a lot of money and many people are involved at all levels. USCYBERCOM is not running this transformation, of course, but we are responsible for defending the DoD systems that will be changed by it.

Neither the U.S. Government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help. We saw in the recent hack of Sony Pictures Entertainment that we have to be prepared to respond to cyber attacks with concerted actions across the whole of government using our nation's unique insights and complete range of capabilities in cooperation with the private sector. This interdependence will only increase in the future. Indeed, the cyber

environment evolves rapidly—making the maturation of our capabilities and their agility in this changing mission space still more imperative for our ability to deter adversaries who might be tempted to test our resolve.

Where We Are Headed

USCYBERCOM has accomplished a great deal, but we still have a long road ahead. Cyberspace is dynamic—it changes constantly with the actions of users and the equipment and software they connect on-line. Compounding that routine volatility are two factors: the rapid evolution of the technology itself, and the changing habits and expectations of users. If current trends hold, then we can expect more nations, and even state-less groups and individuals as well, to develop and employ their own tools and cyber warfare units to cause effects in targeted networks. The cyber strife that we see now in several regions will continue and deepen in sophistication and intensity. In light of our recent experience with the destructive attacks on Sony Pictures Entertainment, we expect state and unaffiliated cyber actors to become bolder and seek more capable means to affect us and our allies. Sadly, we foresee increased tensions in cyberspace.

This is truly a period in history in which we are falling behind if we are merely holding our position in the overall movement to forge new capabilities. We in the U.S. Government and DoD must continue learning and developing new skills and techniques just to tread water, given the rapid pace of change in cyberspace. I liken our historical moment to the situation that confronted the U.S. early in the Cold War, when it became obvious that the Soviet Union and others could build hydrogen bombs and the superpower competition showed worrying signs of instability. We rapidly learned that we needed a nuclear force that was deployed across the three

legs of the riad and underpinned by robust command and control mechanisms, far-reaching intelligence, and policy structures including a declared deterrence posture. Building these nuclear forces and the policy and support structures around them took time and did not cause a nuclear war or make the world less safe. On the contrary, it made deterrence predictable, helped to lower tensions, and ultimately facilitated arms control negotiations. While the analogy to cyberspace is not exact, it seems clear that our nation must continue to commit time, effort, and resources to understanding our historical situation and building cyber military capabilities, along with the "whole-of-nation" structures and partnerships they work among. Just as we fashioned a formidable nuclear capability that served us through the Cold War and beyond, I am confident in our ability to keep pace with adversaries who are determined to control "their" corners of cyberspace, to exfiltrate our intellectual property, and to disrupt the functioning of our institutions. They are every bit as determined, creative, and persistent in these efforts as the Soviet leaders we contained during the Cold War, and unfortunately we see few hints they will act more responsibly in cyberspace. Thus we must commit to the long-term goal of building a truly open, secure cyberspace governed collaboratively by many stakeholders, while we remain prepared for crises and contingencies that can arise along the way—just as we do in every other domain.

I can assure Congress, and the American people, that we are executing and will carry out a well-conceived and systematic plan for doing that. As we train our cyber mission teams, we are inculcating a culture of respect for civil liberties and privacy while learning how to assess their readiness and establishing expectations and an institutional base that will serve to sustain this force, and even to expand it further if that someday becomes necessary. The team members we train today will furnish the leadership of the U.S. military's cyberspace organizations of the

future; they are digital natives, having come up through the ranks thinking about cyber issues. I have no doubt their perspectives will differ from our own, and that they will see solutions to problems that vex us now. Building the capabilities of USCYBERCOM and the CMF is also providing valuable lessons for the reconfiguration of DoD's networked architecture to make it more defensible. When the JIE is completely implemented a few years from now, we will have a far more secure base from which to operate in cyberspace, and all of our capabilities in the other domains will benefit as well from the massive data support they receive from a cloud architecture.

The sophistication of our defenses and operations must grow, of course, in partnership with our allies and as part of a truly whole of nation approach to the problem. Let me reiterate that there is no Department of Defense solution to our cybersecurity dilemmas. The global movement of threat activity in and through cyberspace blurs the U.S. Government's traditional understandings of how to address domestic and foreign military, criminal, and intelligence activities. This is exacerbated further by the speed with which unforeseen threats can impact U.S. interests and the fact that adversaries frequently use (wittingly or unwittingly) U.S.-based resources due to the nation's robust cyber infrastructure. This creates a circumstance in which unity of effort across the U.S. Government is required. DoD's growing capabilities and capacities need to be considered within this broader context. Any plausible solutions will involve multiple actors and stakeholders from within and across several agencies, governments, and economic sectors. Everything we do in USCYBERCOM we do in partnership with other commands, agencies, departments, industries, and countries. As we saw over the last year in our collective response to the Shellshock and Heartbleed vulnerabilities, we must all work together across the U.S. Government, with the states, industry, and allies on a constant basis to ensure we

are ready to surge for incidents and crises and thus provide the necessary assurance for inter-agency and foreign partners.

What does the future hold for USCYBERCOM specifically? I will strongly recommend to anyone who asks that we remain in the dual hat relationship under which the Commander of USCYBERCOM also serves as the Director, NSA/CSS. This is simply the right thing to do for now, as the White House reiterated in late 2013. It might not be a permanent solution, but it is a good one given where we are in this journey as it allows us to build upon the strengths of both organizations to serve our nation's defense.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak, and for all the support that you and this Committee have provided USCYBERCOM. I appreciate our continued partnership as we build our nation's defenses. Our progress has been made possible because of support from all stakeholders, in terms of resources, trust, and impetus. Cyberspace is more than a challenging environment; it is now part of virtually everything we in the U.S. military do in all domains of the battlespace and each of our lines of effort. There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked. We in USCYBERCOM have strived to direct the operation and defense of DoD information systems and to protect and further the nation's interests in cyberspace. We have a great deal of work ahead of us, and thus accelerating USCYBERCOM's growth in capability will remain my focus, and be a continuing emphasis for the Department. We can all be proud of what our efforts, with your help, have accomplished in building USCYBERCOM and positioning its men and women for continued success.

Admiral Michael S. Rogers
Commander, U.S. Cyber Command
Director, National Security Agency
Chief, Central Security Service

Admiral Michael Rogers is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986.

He assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency/Chief, Central Security Service in March 2014.

Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as commander, U.S. Fleet Cyber Command/U.S. 10th Fleet.

Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of commander, Carrier Group 2/John F. Kennedy Carrier Strike Group; and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lasalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.

Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and, has served at Naval Security Group Department; NAVCOMSTA Rota, Spain; Naval Military Personnel Command; Commander in Chief, U.S. Atlantic Fleet; the Bureau of Personnel as the cryptologic junior officer detailer; and, Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander.

Rogers' joint service both afloat and ashore has been extensive and, prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman's Action Group, and a leader of the JCS Joint Strategic Working Group.

Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow; Harvard Senior Executive in National Security alum; and holds a Master of Science in National Security Strategy.

RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL EDWARD C. CARDON
COMMANDING GENERAL
U.S. ARMY CYBER COMMAND AND SECOND ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OPERATIONALIZING CYBERSPACE FOR THE SERVICES

FIRST SESSION 114TH CONGRESS

MARCH 4, 2015

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Introduction

Chairman Wilson, Ranking Member Langevin, and Members of the Subcommittee, thank you for your support of our Soldiers and Civilians, our Army, and our efforts to operationalize cyberspace. It is an honor to address this subcommittee on behalf of the dedicated Soldiers and Army Civilians of U.S. Army Cyber Command (ARCYBER) and Second Army who work every day supporting Joint and Army commanders defending the Nation in cyberspace.

Army Cyber Command and Second Army have gained tremendous momentum building the Army's cyberspace capabilities and capacity. While making significant strides over the past two years, continued progress requires persistent congressional support in three core areas: people, operations, and technology. Put differently, we require resources, appropriate authorities, organizations, and capabilities, which can be synchronized in time and space with singular purpose to accomplish directed missions. This testimony focuses on the actions and activities the Army has underway, or is planning, to support our Title 10 responsibilities to organize, man, train, and equip Army cyber forces for cyberspace.

Mission and Organization

Army Cyber Command and Second Army directs and conducts cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries. To accomplish this mission, the Secretary of the Army and the Army Chief of Staff streamlined the Army's cyberspace command and control structures by placing operational control of all Army operational cyber forces under one commander. The ARCYBER commanding general is responsible for Army and joint cyberspace operations; and is also designated as the Second Army commanding general responsible for all Army network operations (to meet United States Code Titles 40 and 44 requirements as defined by Headquarters, Department of the Army); and is also designated as the Joint Force Headquarters-Cyber (JFHQ-Cyber) commander responsible for cyberspace operations supporting select geographic combatant commands as directed by U.S. Cyber Command (USCYBERCOM). This construct works to enable unity of effort for cyberspace operations. The Secretary of Defense's recent decision to establish Joint Force

Headquarters- Department of Defense Information Networks (DoDIN) better aligned DoDIN operations, and by extension, Army networks, in a joint construct. This decision is essential to realizing the Department's goal of establishing one joint global network that connects Service networks as required for operational missions.

To achieve greater synergy and efficiencies within the Army, we have already established the initial elements of JFHQ-Cyber at Fort Gordon, Georgia, and will collocate the ARCYBER headquarters alongside National Security Agency-Georgia at Fort Gordon by 2020. Army Cyber Command is grateful that the FY16 President's Budget included $90 Million to build a state-of-the-art headquarters and operations facility at Fort Gordon.

Other recent Army decisions include the formation of the Army Cyber Institute at the U.S. Military Academy, West Point, the establishment of the Cyber Center of Excellence (Cyber CoE) at Fort Gordon, Georgia and the transition of the proponent for cyberspace operations from ARCYBER to the Army's Training and Doctrine Command at the Cyber CoE. The Cyber CoE is now the center of gravity for institutionalizing cyberspace, to include the necessary doctrinal, organizational, training, and materiel activities and policies, but it needs more dedicated resources to reach its full potential. The Cyber CoE will also integrate the electronic warfare and cyberspace operations proponents. As a partial solution and in accordance with the Total Army policy with reference to cyberspace, the Cyber CoE is initiating a partnership with the Army National Guard Professional Education Center in Little Rock, Arkansas to increase Cyber training throughput. These decisions have garnered operational and institutional momentum for cyberspace operations across the Army.

Bounding the Impact of Cyberspace on Military Operations

The Army's doctrine, Unified Land Operations, and recently published Army Operating Concept, establish a set of assumptions about conditions of the network and cyber-electromagnetic environment in which our forces are expected to operate. Services and combatant commanders base their plans on the expected Army capabilities, derived from this doctrine. As the current force downsizes, the Army must incorporate additional capability sets to amplify our units' means to operate more effectively in and through cyberspace.

For cyberspace, commanders at all levels will synchronize cyberspace operations into traditional land, sea, air and space activities in time and space and they will simultaneously maneuver with and through networked assets, the electromagnetic spectrum, and kinetic forces in mutually supporting operational constructs to achieve a disproportionate advantage. Achieving operational success also hinges on having the requisite command and control, alignment of authorities with missions, and other key enabling capabilities such as intelligence, information technology and communication activities. Tactical and enterprise networks are converging and future networks and the data they carry will be more contested and challenged — especially in the event of more intense forms of conflict.

The network is a critical enabler and operational capability for cyberspace operations. Congress, recognizing the importance of efficient and effective Information Technology (IT) and Information Assurance (IA) practices, legislated policy standards for both issues in Titles 40 and 44. Information Assurance, now known as Cybersecurity, has evolved into an operational imperative. Army Cyber Command is charged to plan and direct cyberspace operations in support of both Army and USCYBERCOM, and these missions require unity of effort and unity of command.

Now that cybersecurity has to be considered an element of cyberspace operations, where does cybersecurity fit, within the DoD's full-spectrum of cyberspace operations? In other words, where does statutory responsibility for cybersecurity nest with the operational commanders' responsibility to conduct full-spectrum cyberspace operations?

In response to congressional direction, DoD has recently created a new policy position within the Office of the Secretary of Defense, called the Principal Cyber Advisor, to bring an operational focus to all DoD activities affecting cyberspace. In the process, DoD clarified the policy role of the Chief Information Officer (CIO) function within DoD. The policy role of a CIO and the operational focus of a cyberspace operations commander must be mutually supportive to achieve statutory IT and cybersecurity (formerly Information Assurance) mandates. At the same time, operational commanders must assure the effectiveness of DoD networks as warfighting platforms and enablers of DoD operations.

Army leaders and cyber organizations must be capable of ensuring both freedom of maneuver in cyberspace, and integrating interactions between cyberspace operations and our traditional military activities, that are increasingly reliant on networks and network-dependent enablers. This requires an agile and adaptive network that does not exist in the Army today. The Army recognizes it must collapse its vast array of disparate networks, enclaves, and nodes at both tactical and enterprise levels to improve security, effectiveness and efficiency through network modernization. In his recent testimony, the Army's Chief Information Officer, LTG Robert Ferrell, described how the Army will address this issue.

Recruiting, Retaining and Maintaining Cyberspace Operations Personnel

The Army's first priority is to grow the Cyber Mission Force (CMF). We have grown its capacity exponentially since September 2013 with 25 of 41 teams at initial operating capability. We are on track to have all 41 CMF teams established and operating by the end of FY 16. However, they will not all be fully operationally capable until FY17.

Nothing is more important and vital to the growth of cyber capabilities than our ability to attract and retain the best people. As such, the Army views people as the centerpiece to cyberspace characterized by high degrees of competence and character. After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills. The Secretary of the Army established a cyber branch on September 1, 2014, and discussions are ongoing to determine how to better manage civilians supporting cyberspace operations. In addition, the Army has also created an "E4" additional skill identifier to better track personnel who have served in cyber and cyber related assignments as we build the branch and the force.

The Army has enjoyed success with in-Service recruiting into the growing cyber force, and is actively working to expand access to high-quality recruits. We have increased recruiting aptitude scores, visibly expanded our marketing efforts, and started work on a Cyber CoE-led initiative to encourage Science Technology Engineering and Mathematics cadets from both United States Military Academy (USMA) and the Reserve Officers' Training Corps (ROTC). We will commission the first 30 Cyber branch officers from both USMA and ROTC programs this summer. Once assessed

into the cyber branch, officers are managed by the U.S. Army Human Resources Command's Cyber Management Branch.

The Cyber CoE, in collaboration with ARCYBER and other stakeholders is working to implement a cyber Career Management Field for enlisted personnel that will encompass accessions, career management, and retention this fiscal year. The Army recently approved Special Duty Assignment Pay, Assignment Incentive Pay, and bonuses for Soldiers serving in operational cyber assignments. We have also expanded cyber educational programs, including training with industry, fellowships, civilian graduate education, and utilization of inter-service education programs (e.g., Air Force Institute of Technology and the Naval Postgraduate School). We are confident these will serve as additional incentives to retain the best personnel for this highly technical field.

Additionally, as part of our Total Force efforts, we have worked with the Reserve Components on key retention initiatives, including bonuses for critical skill Service members transitioning from active duty service into the Reserve Components; and accession bonuses for commissioned and warrant officers upon award of their duty qualifying military occupational specialties. Appropriate Special Duty and Assignment Incentive Pays should be considered for each of the Reserve Components' cyber Soldiers.

Recruiting and retaining Army Civilian cyber talent is challenging given internal federal employment constraints regarding compensation and a comparatively slow hiring process. Current efforts to attract and retain top civilian talent include extensive marketing efforts, and leveraging existing programs and initiatives run by the National Security Agency, Office of Personnel Management, and National Science Foundation.

The targeted and enhanced use of recruiting, relocation and retention bonuses, and repayment of student loans will improve efforts to attract, develop and retain an effective cyber civilian workforce. These authorities exist but require consistent and predictable long-term funding. Retaining highly skilled cyber professionals will continue to be a significant challenge that needs to be addressed.

Training

Training is critical to building and retaining our cyberspace force. Individual and collective cyber training has four components: training the CMF; integration of cyber into

unified land operations at echelon; training other cyber forces and enablers; and training to achieve basic cybersecurity awareness across the Total Army.

The Department of Defense provided resources to fund joint training requirements through USCYBERCOM for the CMF build for all the Services through FY16. This training allotment was only for Active Component Soldiers and Civilians. Training and sustainment resourcing after FY16 will become a Service responsibility, which the Army must fund beginning in 2017. The Army Cyber CoE recently conducted a Joint Cyber Training Forum in conjunction with USCYBERCOM and representatives from other Services and agencies to determine the way ahead for the transition to Service responsibility. The forum established that the Services are best positioned to develop the common core individual training and will re-evaluate the feeder school training model with regards to specific CMF operator work roles.

Both ARCYBER and the Cyber CoE are developing robust collective training methods that include both simulated, virtual, and real-world operational events on ranges and production networks that stress individual and team capabilities. We now require dedicated training facilities, support infrastructure and cyberspace live fire facilities consistent with joint range requirements at the Service and joint levels. These persistent training environments with dedicated facilities and resources will enable training innovations and further growth in capability and capacity available to combatant and Army commanders.

Army Cyber Command works closely with Army Training and Doctrine Command to ensure the continuum of cyberspace leader development, education, and training remains current and relevant despite the high rates of technological change. The Cyber CoE is explicitly charged with incorporating joint standards into existing programs of instruction in Military Occupational Specialty schools and the Combined Arms Center is incorporating cyber operations planning into their training scenarios. The Army must place equal attention toward the training of our cyber network defense service providers, our computer emergency response teams, and our information technology professionals. Finally, we must continue to improve the effectiveness of training on user practices for the Total Army. This also requires a culture change.

To ensure synergy between Army and joint training, the Army fully participates in the design and conduct of USCYBERCOM-sponsored and executed training and

exercise events. Army Cyber Command has also incorporated cyberspace operations into multiple operational plans and major exercises — building a cadre of cyberspace planners now supporting the joint force and Army commanders. The Army recognizes that cyber capabilities should also extend and be executed at the tactical edge to provide our forces a winning advantage across warfighting functions; therefore, the Army is working hard to define cyber requirements, including training requirements, for cyber support to our Corps and below formations with pilot programs planned for this year. We continue to expand our professional cyberspace opposing force, to more effectively train organizations and individuals on how to better protect and defend themselves against cyber attacks and how to operate in a degraded cyberspace environment during operational training events, such as major exercises and training center rotations.

Reserve Components Integration

Army Cyber Command is a total multi-component force of Active and Reserve Components which are fully integrated into the cyberspace force mix. Building the U.S. Army Reserve (USAR) and Army National Guard (ARNG) cyber forces is a high priority for the Army and ARCYBER. Our Reserve Components integration strategy was reflected in the Army's response to Section 933 of the FY14 National Defense Authorization Act, titled "Cyber Mission Analysis for Cyber Operations of the Department of Defense," which requested an analysis of the Reserve Components' role in cyberspace operations and is focused along several lines of effort, including: building an operational reserve in the USAR and ARNG for cyberspace crisis response; seeking opportunities to provide dual-use capability in support of Military and Homeland Defense and Defense Support of Civil Authorities missions; organizing cyber units to match CMF structure; aligning ARNG and USAR cyber forces under ARCYBER training and readiness authority; leveraging industry connected skills and using the Reserve Components' retention advantages for the Total Force.

The Army and ARCYBER will create a Total multi-component Army cyber force that includes 21 Reserve Component Cyber Protection Teams trained to the same standards as the Active Component cyber force. The civilian acquired skills and experience of Reserve Component Soldiers should be leveraged to provide equivalency for cyber training, enabling faster integration of the Reserve Components' capability into

the cyberspace force mix. In October 2014, in coordination with the Director of the Army National Guard, the Army activated one Army National Guard Cyber Protection Team in a Title 10 status supporting ARCYBER and Second Army.

Army Guard and Reserve forces routinely augment our headquarters now for cyberspace operations even as we work to build additional capability and capacity in the Guard and Reserve. Our Reserve Components' contributions include supporting Operation ENDURING FREEDOM, current operations in Southwest Asia, the Defense Information Systems Agency, USCYBERCOM, the standup of JFHQ-Cyber, and the defense of Army networks. As we move forward with the ARNG and USAR to build the Total Army cyber force, we will continue to train and integrate 429 ARNG and 469 USAR Soldiers into the Army's cyberspace operations.

Authorities are a complex problem. While the 933 report was an excellent start for defining the critical role our Reserve Components must play in cyberspace operations, authorities remain a challenge. While Title 10 authorities are clear, Title 32 and State active duty require the application of varied State constitutional, legislative, and executive authorities and coordination with state agencies and officials. While every State is different, there is merit in developing a common approach for authorities and capabilities to facilitate rapid and effective response in cyberspace.

Equipping the Army's Cyberspace Operations Force

As cyberspace grows more complex, and increasingly contested with sophisticated threats able to exploit known and unknown vulnerabilities, cyberspace operations and cybersecurity are exceptionally critical to national security. Sophisticated software is readily available that almost anyone can operate to achieve altruistic or nefarious ends. Aided by the proliferation of dual-use technologies, cyber actors of all types continue to exercise distinct advantages in cyberspace, especially when acting as an aggressor, as illustrated by the recent attacks on Sony Pictures Entertainment and Anthem health insurance. Electronic devices are increasingly embedded in everything from vehicles to guided missiles, and are often integrated into systems which are difficult and costly to update or upgrade as new threats or vulnerabilities are identified with increasing speed and widely ranging tempo. These factors represent malefactors impacting our warfighting systems.

In conjunction with our joint partners, the Army is aggressively improving its defensive posture beginning with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing but ever-critical perimeter defense capability. Notably, the Joint Regional Security Stack (JRSS) initiative, a component of the Joint Information Environment (JIE), will consolidate and improve the security of currently disparate networks, and provide foundational elements for enhanced situational awareness. Recent intrusions plainly underscore the extent to which DoD lacks sufficient situational awareness, putting operations and sensitive data at grave risk. With the proliferation of cyberspace capabilities globally, situational awareness also depends upon analysis of unprecedented quantities of data across friendly, enemy, and neutral space. Essential data elements are created throughout all phases of cyber attacks, which potentially originate deep within adversary space, and span our entire defense in depth. All of these separate data sources must be captured, aggregated, and correlated in near real-time to discover ever-evolving and diverse threats, including insider threats. Accordingly, we are aggressively pursuing foundational big data analytic capabilities required to deliver complete cyber situational awareness across all cyberspace operations. We have to modernize and get to the JIE as quickly as possible for improved mission effectiveness, enhanced security, and to increase efficiency — an imperative to protecting the DoDIN. Coupled with architecture modernization, these efforts align directly with JIE standards and its Single Security Architecture construct. In parallel, we are pursuing several advanced technologies to include network mapping, cloud and virtualization, and cyber infrastructure, platforms and tools, all of which are also fully integrated with USCYBERCOM's Unified Platform initiative. Additionally, we are also an active partner with Defense Advanced Research Projects Agency on its PLAN X cyberwarfare program that is developing foundational platforms for the planning and execution of cyber operations.

Given the pace of technological change, we must address distinct requirements, resourcing and acquisition processes. Together, they influence the entire spectrum of research, development, testing, evaluation, fielding, and sustainment. Dynamic and agile institutional processes are crucial to building and maintaining our decisive technological advantage. Recent updates to policy instructions for the Joint Capabilities Integration and Development System and the Defense Acquisition System provide a

foundation for requirements and acquisition governance and management rooted in agility, flexibility, and accountability with the objective to rapidly deliver cyberspace capabilities. The Army is also establishing the requisite fiscal structures and governance construct for investments and appropriations against urgent requirements. We must capitalize on the cumulative innovative power of industry, academia, and our National Laboratories to develop, test, and pilot promising technology and concepts. This requires a willingness to engage in iterative development and operations, for which success is measured by rapidly validating assumptions, failing cheaply, early, and often to ensure resources are liberated from non-performing programs and applied to those demonstrating promise, as well as delivering new or enhanced cyberspace capabilities in weeks or months instead of months or years.

In recognition of the unique demands of cyberspace, the Army has designated a cyber focal point at the office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, and designated initial cyber materiel development roles across our Program Executive Offices. The Army is deeply focused on improving the security posture and resilience of its critical weapons and business platforms, ensuring cyber threats and vulnerabilities are considered both in the design phase and throughout production and sustainment. Remaining focused on DoD and USCYBERCOM guidance and directives we will ensure Army capabilities are presented in alignment with joint requirements and are interoperable within the joint community so that we optimize our collective investments across DoD. As we work to ensure current processes evolve to capitalize on innovative technologies, ultimately, new programming and acquisition authorities can provide greater flexibility to developing and fielding the infrastructure, platforms, and tools needed by our operational cyber forces.

Conclusion

Despite cyberspace operations' central role in current defense strategy, funding for core requirements remains uncertain. Cyber professionals – resourced with the right infrastructure, platforms and tools – are the key to dominance in cyberspace. Army Cyber Command, Second Army, and JFHQ-Cyber have made tremendous progress operationalizing cyberspace for the Army. Army networks are better defended and our cyber forces are better manned, trained and equipped. Recent institutional changes are helping recruit, retain, and continuously develop competent and disciplined cyber

professionals. This is a journey and congressional support is essential to ensure the Army has the required resources and authorities, and the right people, processes, and technologies to provide our combatant commanders and national decision makers with a ready, capable, and superior operational cyber force.

With your support, we can provide national leaders and military commanders with an expanded set of options in support of national security objectives. We will deliver.

Lieutenant General Edward C. Cardon

Biography ★★★

Lieutenant General Edward C. Cardon was born in Texas, raised in California and was commissioned as an Engineer Officer from the United States Military Academy in 1982. His company grade assignments include: Platoon Leader and Battalion Maintenance Officer with the 17th Engineer Battalion (Combat), 2nd Armored Division, Fort Hood, Texas; Training Officer with the 130th Engineer Brigade, V Corps; Brigade Engineer for 3rd Brigade, 3rd Armored Division; Company Commander, C Company, 23rd Engineer Battalion, 3rd Armored Division; Staff Officer and Engineer Company Trainer for the Live Fire Team, Operations Group, National Training Center; and Instructor, United States Army Engineer School. After graduation from the Naval Command and Staff College, he served as the Assistant Division Engineer, 3rd Infantry Division (Mechanized); Executive Officer, 82nd Engineer Battalion, 1st Infantry Division (Mechanized); Staff Geographic Officer for Land Forces Central Europe, NATO; Chief Geographic Officer, IFOR/SFOR Bosnia- Herzegovina; Chief of the Initiatives Group for the Commander, Stabilization Force (SFOR); Battalion Commander of the 588th Engineer Battalion, 4th Infantry Division (1998-2000); and as Special Assistant (Strategy) for the Army Chief of Staff, Pentagon (2000-2002).

After graduation from the National War College; he assumed command of the Engineer Brigade, 3rd Infantry Division (2003-2004) in Iraq, and later served as the first Commander of the 4th Brigade Combat Team, 3rd Infantry Division (2004-2006) including a deployment to Iraq. Upon selection for Brigadier General, he was assigned as the Deputy Commanding General (Support), 3rd Infantry Division (2006-2008) including a deployment to Iraq (2007-2008).

Upon his return from Iraq, he served as the Deputy Commandant, US Army Command and General Staff College, and the Deputy Commanding General, Leader Development and Education -- US Army Combined Arms Center, Ft. Leavenworth, Kansas (2008-2010). Lieutenant General Cardon then served as the Deputy Commanding General for Support, United States Forces – Iraq (2010-2011). Most recently, he served as the Commanding General of 2nd Infantry Division (2011-2013).

Among his awards are the Distinguished Service Medal, Defense Superior Service Medal, the Legion of Merit (with 5 Oak Leaf Clusters), the Bronze Star (with Oak Leaf Cluster), Defense Meritorious Service Medal, Meritorious Service Medal (with 3 Oak Leaf Clusters), Joint Service Commendation Medal (with Oak Leaf Cluster), Army Commendation Medal (with 5 Oak Leaf Clusters), Army Achievement Medal (with 2 Oak Leaf Clusters), Combat Action Badge, Parachutist Badge and the Army Staff Identification Badge.

Lieutenant General Cardon has earned a Bachelor of Science Degree from the United States Military Academy, and Master's Degrees from the National War College and the United States Naval Command and Staff College, both in National Security and Strategic Studies. His military education includes the Engineer Officer Basic and Advanced Courses, Combined Arms and Services Staff School, United States Naval Command and Staff College, the Armed Forces Staff College, and the National War College.

NOT FOR PUBLICATION UNTIL RELEASED
BY THE HOUSE ARMED SERVICES
COMMITTEE SUBCOMMITTEE ON
EMERGING THREATS AND CAPABILITIES

STATEMENT

OF

VICE ADMIRAL JAN E. TIGHE
COMMANDER, U.S. FLEET CYBER COMMAND/U.S. TENTH FLEET

BEFORE THE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OF THE

HOUSE ARMED SERVICES COMMITTEE

ON

CYBER OPERATIONS: IMPROVING THE MILITARY CYBER SECURITY POSTURE IN AN UNCERTAIN THREAT ENVIRONMENT

March 4, 2015

NOT FOR PUBLICATION UNTIL RELEASED BY THE
HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Chairman Wilson, Ranking Member Langevin and distinguished members of the Subcommittee, thank you for your support to our military and the opportunity to appear before you today along with my military service component counterparts and partners.

Mr. Chairman, I have been in command of U.S. Fleet Cyber Command and U.S. TENTH Fleet for just under one year. U.S. Fleet Cyber Command reports directly to the Chief of Naval Operations as an Echelon II command and is responsible for Navy Networks, Cryptology, Signals Intelligence, Information Operations, Electronic Warfare, Cyber, and Space. As such, U.S. Fleet Cyber Command serves as the Navy Component Command to U.S. Strategic Command and U.S. Cyber Command, and the Navy's Service Cryptologic Component Commander under the National Security Agency/Central Security Service, exercising operational control of U.S. Fleet Cyber Command operational forces through TENTH Fleet. Specifically, we conduct cyberspace operations to ensure Navy and Joint or Combined forces' freedom of action while denying the same to our adversaries.

The commissioning of U.S. Fleet Cyber Command and reestablishment of U.S. TENTH Fleet on January 29, 2010 closely followed the Navy's 2009 acknowledgement of information's centrality to maritime warfighting, known as Information Dominance. Information Dominance is defined as the operational advantage gained from fully integrating the Navy's information functions, capabilities, and resources to optimize decision making and maximize warfighting effects. The three pillars of Information Dominance are assured command and control (C2), battlespace awareness, and integrated fires. U.S. Fleet Cyber Command is a key warfighting element in delivering on missions across those three pillars.

Since my U.S. Fleet Cyber Command predecessor ADM Michael S. Rogers last testified before this Subcommittee in July 2012, the Department of Defense (DoD), U.S. Cyber Command, and the Service Components have significantly matured cyber operations and enhanced cyber operational capabilities. I appreciate the opportunity to outline the Navy's progress over the past two years, where we are headed to address an ever increasing threat, and how budgetary uncertainty is likely to impact our operations.

Cyber Operations, Posture, and Future Investments

U.S. Fleet Cyber Command directs operations to secure, operate, and defend Navy networks within the Department of Defense Information Networks (DoDIN). We operate the Navy Networking Environment as a warfighting platform, which must be aggressively defended from intrusion, exploitation and attack. The Navy Networking Environment consists of more than 500,000 end user devices; an estimated 75,000 network devices (servers, domain controllers); and approximately 45,000 applications and systems across three security enclaves.

Operations during the past two years led to a fundamental shift in how we operate and defend in cyberspace. Specifically, late summer 2013 we fought through an adversary intrusion into the Navy's unclassified network. Under a named operation, known as OPERATION ROLLING TIDE, U.S. Fleet Cyber Command drove out the intruder through exceptional collaboration with affected Navy leaders, U.S. Cyber Command, National Security Agency, Defense Information Systems Agency (DISA), and our fellow service cyber components. Although any intrusion upon our networks is troubling, this operation also served as a learning opportunity that has both matured the way we operate and defend our networks in cyberspace, and simultaneously highlighted gaps in both our cybersecurity posture and defensive operational capabilities. As a result of this operation and other cybersecurity initiatives, the Navy has already made or proposed (through FY20) a nearly 1 billion dollar investment that reduce the risk of successful cyberspace operations against the Navy Networking Environment. Of course these investments are built on the premise that our future year budgets will not be drastically reduced by sequestration. Specifically, if budget uncertainty continues, we will have an increasingly difficult time addressing this very real and present danger to our national security and maritime warfighting capability.

The Navy's future cybersecurity investments are being informed by the Navy's Task Force Cyber Awakening, which was chartered by the Chief of Naval Operations and the Assistant Secretary of the Navy for Research, Development and Acquisition to gain a holistic view of cybersecurity risk across the Navy, and beyond just our corporate navy networks to include

combat and industrial control systems. The FY16 Proposed Budget (PB16) includes Task Force Cyber Awakening -recommended investments amounting to $248M for FY16 and $721M across the Future Years Defense Plan (FYDP). Task Force Cyber Awakening will make additional recommendations on how to organize and resource capabilities to mitigate that risk.

Concomitant with the Task Force Cyber Awakening outcomes is the migration to a single defensible Cyber architecture, which is vital to the continued success of Navy's worldwide operations. The Navy recognizes that the Joint Information Environment (JIE) is an operational imperative and endorses that vision, including the implementation of a single security architecture (SSA). The Department of the Navy intends for the Navy and Marine Corps Intranet (NMCI) to serve as the primary onramps into JIE, incorporating JIE technical standards through our network technical refreshment processes as those standards are defined. Through delivery of these enterprise environments, the Navy will achieve the tenets of JIE's framework of standards and architecture consistency.

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 as outlined below.

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 with counterfeit devices from untrusted sources. Operationally, we think of these opportunities in terms of the network intrusion attack surface presented to malicious cyber actors. The greater the attack surface, the greater the risk to the Navy mission. The attack surface grows larger 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. Furthermore, we are bolstering our ability to manage cyber security risks in our networks through our certification and accreditation process, and through cyber security inspections across the Navy. Additionally, the Navy is reducing the attack surface with significant investments and consolidation of our ashore and afloat networks with modernization upgrades to the Next Generation Enterprise Network (NGEN) and the Consolidated Afloat Networks and Enterprise Services (CANES), respectively. Finally, the Navy is executing a Data Consolidation Center (DCC) strategy, which will reduce the number and variance of information systems at the same time allow for a centralized approach towards managing the confidentiality, integrity and availability of our data.

For long term success in cyber security, the Navy is working on improved acquisition and system sustainment processes. Specifically, we will design in resiliency by generating a common set of standards and protocols for programs to use as guiding principles during procurement, implementation, and the configuration of solutions, which will improve our cyber posture by driving down variance.

The Navy recognizes that all hands (users, operators, program managers, systems commands…) have an impact (for better or worse) on the magnitude of the Navy's attack surface and the mission risk associated with it. U.S. Fleet Cyber Command must defend this attack surface, regardless of size, using defense in depth capabilities described below.

Defense in Depth

The Navy is working closely with U.S. Cyber Command, NSA/CSS, our Cyber Service Partners, DISA, Interagency 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.

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 include reputation-based and heuristic capabilities), and improving our ability to detect new and unknown malware.

JIE Joint Regional Security Stacks are also integral to our future defense in depth capabilities. As described above, the Navy has already consolidated our networks behind defensive sensors and countermeasures. We expect that JIE Joint Regional Security Stacks (JRSS) v2.0 will be the first increment to bring equal or greater capability to Navy Defense in Depth. 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.

Cyber Situational Awareness

Success in cyberspace requires vigilance: it requires that we constantly monitor and analyze Navy Networking Environment. We must understand both its availability and vulnerabilities. Furthermore we must be able to detect, analyze, report, and mitigate any suspicious or malicious activity in our Networks. The Navy is planning to expand our current capabilities to include a more robust, globally populated and mission-tailorable cyber common operating picture (COP). Additionally, with improved network sensor information across the DoD, however, comes the need for a single dedicated data strategy and big data analytics for all DoD network operations and defense data. This will allow for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of big data analytics to harness existing knowledge rapidly.

U.S. Fleet Cyber Command Operational Forces

U.S. Fleet Cyber Command's operational force comprises nearly 15,000 Active and Reserve sailors and civilians organized into 22 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. Approximately 35 percent of U.S. Fleet Cyber Command 's operational forces are aligned with the cyber mission.

Status of the Cyber Mission Force

As you may recall, during a hearing before the Senate Committee on Armed Services on March 12, 2013, General Keith Alexander briefed the Cyber Mission Force model, which DoD endorsed in December 2012. 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 personnel assigned for all 40 Navy-sourced Cyber Mission Force Teams in 2016 with full operational capability in the following year. As of 1 March 2015, we had 22 teams at initial operating capability (IOC) and 2 teams at full operational capability (FOC). We are in the process of manning, training, and equipping our FY15 teams to meet IOC standards by the end of FY15. Additionally, between now and 2018, 298 cyber reserve billets will also augment the Cyber Force manning plan as described below.

U.S. Fleet Cyber Command has also been designated as the Joint Force Headquarters-Cyber by U.S. Cyber Command to support U.S. Pacific Command and U.S. Southern Command in the development, oversight, planning and command and control of full spectrum cyberspace operations that are executed through attached Combat Mission and Support Teams. In 2014,

Navy's Joint Force Headquarters-Cyber was certified and declared to have achieved Full Operational Capability. This capability was attained without additional U.S. Fleet Cyber Command resources. As the Cyber Mission and Support Teams continue to grow and mature, additional resources to operationally control and manage these teams in support of Combatant Command Priorities will be required.

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' skill sets and expertise to maximize the Reserve Component's support to the full spectrum of cyber mission areas. Within this strategy, the 298 Reserve billets, which are phasing into service from FY15 through FY18, will be individually aligned to Active Duty Cyber Mission Force teams and the Joint Force Headquarters-Cyber. Accordingly, the Joint Force Headquarters-Cyber and each Navy-sourced team will maximize its assigned Reserve Sailors' particular expertise and skill sets to augment each team's mission capabilities. As our Reserve Cyber Mission billets come online and are manned 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.

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 and as we refine our needs to holistically address the challenges being informed by Task Force Cyber Awakening. 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 Navy Information Dominance Force (NAVIDFOR) in 2014 as a Type Commander will go a long way in generating readiness for cyber mission requirements. NAVIDFOR will work closely with the Man, Train, and Equip organizations

across the Navy to ensure that U.S. Fleet Cyber Command and other Information Dominance operational commands achieve proper readiness to meet mission requirements.

Recruit and Retain

There are many young Americans with the skill sets we need who want to serve their country. I am very encouraged by the dedication and commitment I see entering our ranks. I am awed by their dedication and growing expertise every day. We must consistently recruit and retain this technically proficient group of diverse professionals for the cyber mission to sustain this momentum.

In FY2014, the Navy met officer and enlisted cyber accession goals, and is on track to meet accession goals in FY2015. 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.

Cyber-related officer communities are also meeting retention goals. While both Information Warfare (IW) and Information Professional (IP) communities experienced growth associated with increased cyber missions, we are retaining officers in these communities at 93 percent overall. Both IW 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 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.

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. 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 Information Warfare Officers, Information Professional Officers, or Intelligence Officers within the Information Dominance Corps.

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, 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.

Declining Budgets

While the overall Navy budget has been impacted by financial constraints and sequestration, the Navy has done a good job in terms of minimizing the budgetary impact on U.S. Fleet Cyber Command and the capabilities it employs to conduct its operations. Should this circumstance change and future budgets decline, however, there will be an impact to the capability and capacity to conduct operations in cyberspace. The scope and magnitude of such impacts would be driven by the scope and magnitude of a budget decline.

It is, however, possible to speak in broad terms regarding the potential areas of impact. Operations in cyberspace are highly dependent on people - to a certain extent our people are part of the warfighting platform in cyberspace. Budgetary declines impacting our ability to attract and retain the numbers of people with the requisite skills and experience would negatively impact the Navy's ability to conduct operations in cyberspace. Additionally, declining budgets affecting the ability of the Navy to implement initiatives described above that reduce the network intrusion attack surface, enhance defense in depth and cyber situational awareness, or modernize/migrate to the Joint Information Environment greatly jeopardizes the Navy's ability to accomplish all missions, since all Navy mission accomplishment depends on having an available and secure network.

Summary

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace. To ensure operational success in the maritime and other warfighting domains, defense of Navy and DoD networks and information is essential and cannot be separated from the overall maritime operational level of war.

In order to continue to progress in cyberspace operations, we must have sufficient resources to ensure we close any identified cybersecurity gaps and provide our workforce with the right capabilities to maintain our warfighting advantage. We must be prepared – both technologically and with skilled operators, civilian and uniformed - and remain innovative. The threat in cyberspace will only continue to grow despite our budgetary challenges. 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.

I thank you for this opportunity to share U.S. Navy and U.S. Fleet Cyber Command operations and initiatives in cyberspace.

Vice Admiral Jan Tighe

Commander, U.S. Fleet Cyber Command
Commander, U.S. 10th Fleet

Vice Adm. Tighe was born in Bowling Green, Ky., and raised in Plantation, Fla. In April 2014, she assumed duties as the Commander, U.S. Fleet Cyber Command / U.S. 10th Fleet.

Tighe's previous tours include duty with Naval Security Group Activities in Florida, Virginia, Japan, VQ-1 and Naval Information Warfare Activity. She also had staff assignments on the Headquarters of the Pacific Fleet, Naval Security Group, Naval Network Warfare Command, and served as Executive Assistant to Commander, U.S. Cyber Command. Tighe commanded more than 2,800 multi- service and multi-agency personnel at the National Security Agency/Central Security Service Hawaii in Kunia. As a Flag Officer, Tighe served as U.S. Cyber Command Deputy J3; OPNAV N2N6 Director, Decision Superiority; Naval Postgraduate School Interim President; and Deputy Commander, U.S. Fleet Cyber Command / U.S. 10th Fleet.

Tighe is a graduate of the U.S. Naval Academy and was commissioned as an ensign (special duty cryptology) in 1984. She attended the Defense Language Institute in Monterey, California, where she studied Russian. She also attended the Naval Postgraduate School, Monterey, Calif., and in 2001 was awarded a Ph.D. in Electrical Engineering and a M.S. in Applied Mathematics.

Tighe wears both the Information Dominance Warfare pin and Naval Aviation Observer wings, earned while deployed as an airborne special evaluator aboard VQ-1 EP-3E aircraft in the Persian Gulf during Operation Desert Shield/Storm. She is also a member of the Acquisition Professionals Community and holds a Level III Defense Acquisition Workforce Improvement Act (DAWIA) certification in Program Management.

Tighe has been awarded the Defense Superior Service Medal, Legion of Merit, Defense Meritorious Service Medal, Meritorious Service Medal (second award), the Strike/Flight Air Medal, the Navy and Marine Corps Commendation Medal (fourth award), and the Navy and Marine Corps Achievement Medal.

Updated: 21 April 2014

MARFORCYBER RECORD VERSION

STATEMENT BY

MAJOR GENERAL DANIEL J. O'DONOHUE
COMMANDING GENERAL
MARINE FORCES CYBERSPACE COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OPERATIONALIZING CYBERSPACE FOR THE SERVICES

FIRST SESSION 114TH CONGRESS
MARCH 4, 2015

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Introduction

Chairman Wilson, Ranking Member Langevin, and distinguished members of this subcommittee, it is an honor to appear before you today. On behalf of all Marines, our civilian workforce, and their families, I thank you for your continued support. I appreciate the opportunity to discuss the Marine Corps' cyberspace operations posture.

The Marine Corps is the nation's expeditionary force-in-readiness. We are forward deployed, forward engaged, and prepared for crisis response. For generations, your Marines have been victorious against our nation's foes by remaining agile and adaptable to dynamic environments and evolving threats. As the force that is 'the most ready when the nation is least ready,' we are prepared to defend against adversaries who operate across multiple domains to include cyberspace.

Our current operating environment is volatile, complex, and distinguished by increasingly sophisticated threats that seek asymmetric advantage through cyberspace. Our cyberspace posture guards against these threats while simultaneously exploiting our competitive advantage in employing combined arms to include closely integrated cyberspace operations.

Our joint cyberspace mission builds on the Marine Corps institutional focus as a global crisis response force with strong naval, inter-agency, COCOM, SOF, cross-service and coalition partnerships. 2015 is a key transitional year as we deploy rapidly maturing cyber capabilities and make them central to Marine Air Ground Task Force, COCOM and coalition training, planning and operations. Activities in cyberspace increasingly influence all our warfighting functions.

Marine Forces Cyberspace Command (MARFORCYBER) is engaging in ongoing cyberspace operations, making strong progress with the force build, achieving operational outcomes, and building capacity for tomorrow's opportunities and challenges. Our priorities are to operate and defend our networks, support designated COCOMs with full spectrum cyber operations, organize for the fight, train and equip the cyber workforce, develop workforce

lifecycle management, and to ensure mission readiness through joint and service capabilities integration.

Mission and Organization

As the service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum Cyberspace Operations to ensure freedom of action in and through cyberspace, and deny the same to our adversaries. The operations include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (DCO) within the MCEN and Department of Defense Information Networks (DODIN), and - when directed - conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. MARFORCYBER is also designated at the Joint Force Headquarters – Cyber (JFHQ – CYBER) as directed by USCYBERCOM.

Operationalizing Cyber

MARFORCYBER is in its sixth year of operation. Our focus remains developing ready cyberspace capability for the naval, joint and coalition force. Consistent with our Commandant's guidance, we are developing tactical cyber capacity as an organic aspect of how we fight.

Further, in conjunction with joint and interagency partners, we intend to pursue the development of an integrated and unified platform for cyberspace operations that will enable centralized command and control, real time situational awareness, and decision support. We are accomplishing this through close coordination with industry partners, and aligned with DoD and USCYBERCOM priorities in support of the Joint Information Environment.

Train and Equip

In this presumably automated and system driven arena, our most valuable resource is our people. Just as the Marine Corps remains dedicated to the notion that there is no more

dangerous weapon than a Marine and his rifle, we believe the solutions to our shared problems in cyberspace revolve around our people, and not systems. However, we must provide our workforce the training, tools, and resources they need to defend our nation. Our ability to acquire tools and technology more rapidly than our adversaries is paramount to mission success.

MARFORCYBER's approach to training and developing the cyber work force has a singular vision—to train as we fight. Specifically, MARFORCYBER will adapt a persistent training environment to support training and exercises of cyber units that are assigned to conduct military cyber operations. This training environment will be designed to enhance military occupational skills (MOS) proficiency, test and development of next generation solutions, host remote training and education of Marine Corps Operating Forces, and refine tactics, techniques, and procedures (TTPs) to increase effectiveness of cyberspace operations. Additionally, we are developing a web based training environment hosted by Carnegie Mellon University Software Engineering Institute (CMU-SEI), a Federally Funded Research and Development Center (FFRDC). This environment combines extensive research and innovative technology to offer a new solution to cyberspace operations workforce development. The focus of this collaboration is to help practitioners and their teams build knowledge, skills, and experience in a continuous cycle of professional development. The combined effect of this approach is for cyberspace operations workforce to train individually and collectively. This initiative will support the future development and certification of Cyber National Mission Forces (CNMF) training requirements.

The training pipeline to build these teams is extensive and often depends on joint schoolhouses that serve all the cyber service components. There are simply not enough school seats to meet the demand from the joint force. Compounding this problem are slowdowns in the clearance process, as technically qualified personnel from our communications or data job fields still require high level security clearances. Often these personnel come from distant and austere duty stations that lack investigators who can complete their clearances prior to arrival at MARFORCYBER. These personnel often wait months at the command prior to starting work due to long wait times for clearance adjudication.

We have dramatically increased cyber integration into the training cycle by leading, supporting, or participating in over 31 combined, joint, and Marine Corps exercises in the past year. Commanders across our Marine Corps are asking for cyber capabilities both in real world operations and in training to ensure their Marines are ready to face the challenges presented by a shifting complex landscape.

Workforce Life-Cycle Management

We have seen substantial increases in capacity and capability. Such achievements are significant but they have not been easy, and MARFORCYBER's success grows from the hard work of its people. Marines and Civilians have shown a sharp interest in pursuing a cyber career.

Since MARFORCYBER last appeared before this committee in 2012, we have dramatically increased our workforce—with an authorized strength of almost 1000 Marines and civil servants today. By the end of fiscal year 2016, MARFORCYBER's authorized strength will increase to over 1300 personnel, which is in line with previous projections. The majority of these new personnel are allocated to support the cyber mission force as directed by the Secretary of Defense.

In order to attract and retain the best people, the Marine Corps has followed multiple lines of effort. To improve continuity and reap greater return-on-investment in the lowest density highest demand military occupational specialties (MOS), we have coordinated with our Service to extend standard assignments to four years. Additionally, the number of feeder MOS available to lateral move into critical cyber related specialties has been increased in order to obtain a larger talent pool of qualified and experienced Marines. We are currently accessing sixteen feeder occupational specialties from the communications, signals intelligence, electronic warfare, data, and aviation specialty fields to meet the personnel demands of cyber occupational field. The largest reenlistment or lateral move bonus offered in the past year of $60,750 dollars was offered to Sergeants who move into the Cyber Security Technician specialty. To drive home the point of how seriously the Marine Corps takes its cyber talent

management, this bonus consumed 16% of the retention bonus budget for the last fiscal year. Furthermore, to ensure we have the right metrics, we are leveraging academia and industry to understand how to better attract and retain talent. In the future, our focus will broaden to include generating a sustainable force generation model that retains a unique, skilled expertise within the larger contexts of cyber ready MAGTFs.

Readiness

MARFORCYBER is leading the effort to take cyberspace operations mainstream across the Marine Corps so as not to be outpaced in an evolving and complex battlespace. Initial teams are being operationally employed as they achieve IOC. As we support the DoD and USCYBERCOM efforts to implement a unified cyberspace architecture of the JIE, we continue to improve the operational readiness of our existing enterprise network (MCEN). We have assumed full control of the MCEN, which was previously contractor-managed, and have decreased our legacy network footprint.

In conjunction with joint, interagency, and private partners, we intend to improve our operational readiness and our ability to measure it. In this context, our staff is working and collaborating with our partners to develop rapid acquisition of tools, training environment, and development of procedures that will allow us to train as we fight.

Last June, USCYBERCOM certified our first Cyber Mission Team (CMT) as fully operational (FOC) and simultaneously, our first national Cyber Protection Team (CPT) and the second Cyber Mission Team (CMT) reached initial operational capability (IOC). MARFORCYBER is on track to have over 75% of its CMT, CPT, and CST teams resourced by the end of fiscal year 2015.

In order to fulfill the requirements of USCYBERCOM, we have been actively engaged in building and sourcing our national and combat mission, protection, and support teams (CMT, CPT, CST). With one CMT currently certified, the plan going forward is to have MARFORCYBER's second CMT certified early in calendar year 2015. We have one operational CPT working from the MCNOSC, which is our service wide network operations and security center. Our second

CPT, which will be in support of national missions, is in the process of certification now. In addition, we stood up our Joint Forces Headquarters-Cyber (JFHQ-C), now at Full Operational Capability (FOC), which directs and coordinates the actions of cyber forces in support of directed missions. The current glide slope for team build-out is to have two (2) CMTs, three (3) CPTs, and one (1) CST at either IOC or FOC by the end of fiscal year 2015. No later than the end of FY17 all teams will be FOC, meaning the Marine Corps will furnish one (1) NMT, three (3) CMTs with one (1) CST in support, and eight (8) CPTs. Three of those CPTs will be dedicated to Marine Corps' specific needs. All other teams will function in support of joint requirements from unified and sub-unified combatant commands.

Conclusion

Over the past six years, MARFORCYBER experienced both the increased risk and opportunity presented by a world that grows more connected. These experiences reinforced the need to remain focused on our priorities of developing our organization and cyber work force, refining our service support to MAGTF operations and joint cyber forces, and securing our networks to yield results for commanders worldwide. Although I am pleased to report that our growth is increasing our capacity, capability, and integration with warfighters, I must reiterate the opportunities and challenges that lie ahead are great. While global technology advances rapidly, the Marine Corps faces challenges in adapting its acquisitions to operate at the speed required of cyberspace. Critically, in this domain characterized by human activity, people remain our center of gravity. Resourcing and sustaining this most valuable asset also remains a difficult task. These are difficult challenges, but through your continued support and leadership, we can count such difficulties among the many that Marines have overcome in the defense of this great nation.

Thank you for this opportunity to appear before you today. Thank you for your continued support of our Marines and Civilians and I look forward to answering your questions.

Major General Daniel J. O'Donohue

Commander, Marine Forces Cyber Command

Brigadier General O'Donohue graduated from the College of William and Mary with a Bachelor of Arts in History and was commissioned in 1984. He is a distinguished graduate of the Amphibious Warfare School, the School of Advanced Warfighting, the National War College, and the Naval Postgraduate School. He has Masters of Science Degrees in National Security Strategy and Manpower Management.

Brigadier General O'Donohue's command assignments include: Commanding Officer, Charlie Company, 1st Battalion, 2nd Marines (1993-1995), Commanding Officer, 2nd Battalion 5th Marines (2002-2004), Commanding Officer, 1st Marine Regiment (2009-2010).

Brigadier General O'Donohue's staff assignments include: Ground Structure Planner, Headquarters Marine Corps (1988-1992); 8th Marines Operations Officer (1995); Operations Officer for Joint Task Force and Special Purpose Marine Air-Ground Task Force Liberia (1996); Tactics Instructor and Expeditionary Operations Program Director at the Amphibious Warfare School (1997-2000); Operations Officer, 1st Marine Division (2001-2002); Assistant Chief of Staff G-7 I Division Combat Assessment Officer (2004); Deputy Branch Head for the Secretary of the Defense's Office of Force Transformation (2005-2007); Branch Head, Ground Combat Element Branch, Plans, Policies and Operations, Headquarters Marine Corps (2007-2008); Assistant Chief of Staff G-3 for 1st Marine Division (2008-2009); Director, Capabilities Development Directorate (2010-).

PRESENTATION TO THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

UNITED STATES HOUSE OF REPRESENTATIVES

SUBJECT: Cyber Operations: Improving the Military Cyber Security Posture in Uncertain Threat Environment

STATEMENT OF: Major General Burke E. Wilson
Commander, Air Forces Cyber and
Commander, 24th Air Force

March 4, 2015

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE
HOUSE COMMITTEE ON ARMED SERVICES
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITES
U.S. HOUSE OF REPRESENTATIVES

Introduction

Chairman Wilson, Ranking Member Langevin, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today, with my counterparts from the other military Services, to discuss Air Forces Cyber's contributions to joint operations in cyberspace. We have made significant strides towards normalizing the Air Force's cyber operations since Major General Vautrinot had the privilege of speaking to the committee in August 2012. Air Forces Cyber (24th Air Force) is one of four Service Cyber Components established to support U.S. Cyber Command; our headquarters is at Joint Base San Antonio-Lackland, Texas and we have ongoing cyber operations around the world. The outstanding men and women of Air Forces Cyber have been diligently working to increase our capacity and capability to build, operate, defend and engage across the full spectrum of cyberspace capabilities in, through and from cyberspace in support of joint warfighters. I'm extremely proud of the work they do each and every day in support of military operations around the world, while at the same time, innovating and mastering new and emerging technologies within cyberspace to project global military power.

Cyberspace is an inherently global domain that impacts nearly every function of our Joint Force, which is increasingly dependent upon cyber capabilities to conduct modern military operations. To that end, today's capabilities enable streamlined command, control and execution of joint operations through the rapid collection, fusion and transmission of information at unprecedented speed, capacity and precision.

However, the pace of threats continues to grow in scope, intensity and sophistication. Recent attacks such as the Sony Pictures Entertainment incident that resulted in physical damage demonstrate that no industry or sector is immune to this growing threat. State-sponsored actors, non-state-sponsored actors, criminals, and terrorists operating in the cyberspace domain will continue their attempts to penetrate Department of Defense networks and mission systems. We must remain vigilant and not falter in our commitment to properly prioritize our support to cyber missions, even with the strain of diminishing resources across the Department.

In response to these growing threats, Air Forces Cyber remains committed to delivering innovative and cost-effective solutions for the joint warfighter with unwavering focus on delivering mission success. Air Forces Cyber's priorities are as follows: employ cyber capabilities in support of Combatant and Air Force Commanders; develop and empower our Airmen and take care of their families; lead through teamwork, partnerships and a strong warfighting narrative; and equip the force through rapid, innovative fielding of cyber capabilities. In this dynamic environment, resource stability will be critical to our ability to protect our networks, provide the needed cyber forces, protect critical information, and provide full spectrum cyber capabilities in support of Combatant and Air Component Commanders around the world.

Employing Cyber Capabilities

Air Forces Cyber has placed significant emphasis on normalizing cyber operations. We continue to transform our organization to an operational Component Number Air Force providing ready cyber forces and capabilities to Combatant and Air Force Commanders. Our operational level command and control center has made incredible gains towards our ability to effectively integrate the full spectrum of cyber operations and capabilities in support of joint and air component operations.

We cannot stand still in this environment and must continue to build our capability and capacity. Working closely with Air Force Space Command, 25th Air Force (formerly Air Force Intelligence, Surveillance and Reconnaissance Agency), and the Air Staff we have established cyber forces in support of the DoD's approved strategy. In full coordination with our Total Force partners in the Air National Guard and Air Force Reserves, these new cyber teams are providing U.S. Cyber Command with capabilities to defend the nation, support Combatant Commanders, and defend the DoD Information Network. We have reorganized our units to meet the training and equipment requirements to build a ready force of approximately 1,700 mission-ready personnel. In concert with the Air Force's basing process, we have identified Joint Base San Antonio-Lackland, Texas, as well as Scott Air Force Base, Illinois, as primary locations for our Cyber Protection Teams. The remaining cyber forces will operate at the National Security

Agency's regional operating centers. Today, Air Forces Cyber has seventeen operational cyber mission teams -- two fully operational teams and an additional fifteen teams that have achieved initial operational status. Our Joint-Forces Headquarters-Cyber also declared initial operational status in October 2013 and continues to work toward achieving full operational status.

In 2014, the Air Force designated seven cyberspace systems as weapons systems directly supporting our lines of effort. This designation has been critical to our ability to operationalize and integrate cyber capabilities through a normalized budget, sustainment and support process. Since we last briefed this subcommittee, the Air Force has completed the migration of its portion of the DoD Information Network (e.g. the Air Force Information Network or "AFIN") into a single, centrally-managed and defended architecture. Transitioning over 644,000 users across more than 250 geographic locations to a single network has enabled Air Forces Cyber (24^{th} Air Force) to operate, maintain and defend a standardized network using centralized control and decentralized execution with more optimally employed resources. Additionally, we've worked tirelessly to collapse over 100 internet access points into a more streamlined and manageable 16 gateways for the Air Force. The end result has been critical to achieving a more effective, efficient and defensible network.

Finally, our operations center is leveraging a combat-proven joint planning and execution process to command and control our cyber forces. Air Forces Cyber is employing small defensive cyber maneuver forces to complement our enterprise defensive capabilities to identify, assess and mitigate vulnerabilities and adversary actions within our networks. This new approach has proven truly effective in a number of operations over the past year and we continue to make strides in the planning, command, control and execution of cyberspace operations.

Develop and Empower Our Airmen and Take Care of Their Families

Our innovative Airmen are the centerpiece to our Air Forces Cyber capabilities. Therefore, we continue to be wholly committed to recruiting, training, developing and retaining the right cyber talent. Whether a military or civilian candidate, the Air Force begins by recruiting highly-qualified individuals with demonstrated competency and character.

To meet the growing requirements of the Department of Defense's Cyber Mission Force, the Air Force has restructured and expanded its initial training and force development programs. These changes are yielding significant results and put us on pace to nearly quadruple the rate at which cyberspace operators will be qualified to join Air Force cyber teams in support of the Cyber Mission Force since we last briefed the subcommittee in 2012.

Realizing the need to operationalize our training, we have also mirrored our cyber operations training based on lessons from our counterparts in air and space operations. Specifically, we have leveraged the mission qualifications process to ensure our cyber operators meet mission-ready status. Additionally, our cyber operators now participate in U.S. Cyber Command and Air Force Warfare Center events such as CYBER FLAG and RED FLAG to better hone their skills through real-world force-on-force exercises that provide the ability to integrate cyber capabilities with other domains in a live training environment. Air Forces Cyber's participation in simulated live-fire environments is accelerating the development and fielding of new tactics, techniques and procedures. These cyber warrior's experiences are further magnified when participants bring hard won lessons back to their home units.

Air Forces Cyber's participation in a wide array of Combatant Command, Joint and Service exercises also complements our efforts to integrate cyber effects with both kinetic and non-kinetic operations across multiple warfighting domains. While demanding in terms of time and resources, these exercises have become integral to effectively developing our Airmen into a ready cyber force capable of operating in joint and coalition environments.

To better develop our forces, the Air Force has also instituted a new cyberspace officer career field specific to Cyberspace Warfare Operations to develop Airmen with the requisite skills and expertise to meet our nation's emerging needs. In addition, a Cyber Intermediate Leadership program has been developed to ensure cyber operators and appropriate intelligence officers are provided the right professional growth opportunities in key command and operational positions. The first Air Force board recently convened to review and competitively select officers for these unique leadership positions. In an effort to retain our highly skilled

enlisted force, the Air Force offers a selective reenlistment bonus that provides additional incentive to continue to serve our nation in this emerging mission.

Lead Through Teamwork, Partnerships and a Strong Warfighting Narrative

Conducting successful operations in cyberspace requires seamless integration with a host of mission partners. In many ways, cyber is a "team sport" and Air Forces Cyber (24th Air Force) is wholly committed to strengthening our relationships with other Air Force partners, our sister Services and interagency counterparts, Combatant Commanders, coalition allies, as well as civilian and 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 Jack Shanahan, has been a steadfast supporter throughout the standup of the Cyber Mission Forces.

U.S. Cyber Command serves as the focal point for all Department of Defense cyber operations. As one of the four Service Cyber Components, we provide an array of cyber forces and capabilities in order to defend DoD Information Networks (DoDIN), support Combatant Commanders, and strengthen our nation's ability to withstand and respond to cyber events. The recent stand-up of the Joint Force Headquarters DoDIN under the leadership of Lieutenant General Hawkins and the Defense Information Systems Agency (DISA) was a major milestone in normalizing the command and control of network defensive operations.

As already highlighted, we partner closely with the Air Reserve Component in day-to-day cyber operations. Through a compliment of Traditional Reservists, Air Reserve Technicians and Air National Guardsmen, our Air Force's cyber units are a striking example of Total Force Integration in action. These total force professionals bring a unique blend of experience and expertise to the full spectrum of cyber missions. Many work in prominent civilian positions within the Information Technology industry, which bolsters our mission effectiveness through their willingness to serve the nation. Likewise, we are often able to retain unique skillsets gained by investment in our Airmen by supporting their continued service in the Air Force Reserves or

Air National Guard. These partnerships will be vital to our future operations as the Air Reserve Component continues to provide integrated support of the DoD's Cyber Mission Force.

Air Forces Cyber 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 industry leaders such as Symantec, AT&T, USAA, Northrop Grumman and 21 other partners 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.

We also enjoy strong relationships with other DoD Components. As an example, the Air Force recently aligned with the Army and the Defense Information Systems Agency (DISA) to support the development and fielding of a key technology in the transition to a Joint Information Environment (JIE). Together we are implementing Joint Regional Security Stacks (JRSS) and making enhancements to our networks with Multi-Protocol Label Switching (MPLS) as part of the single security architecture. Through this teamwork, the first JRSS "security stack" was fielded at Joint Base San Antonio-Lackland, Texas, in line with one of the sixteen Air Force Gateways. Additional "security stacks" are being installed at other AF and DoD sites as part of the JIE. These efforts [JRSS, MPLS] benefit the entire DoD by reducing attack surface of our networks and threat vectors – allowing for more standardized security of our networks and by providing increased network capacity to support defense missions.

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. The community leadership also understands that encouraging our younger generation to gain the needed cyber skills will be essential to our nation's success in this arena. By partnering together, Air Forces Cyber (24th Air Force) supports a broad array of programs

designed to touch young students. 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 over 9,000 high school and middle school students. Another example is our "Troops for Teens" program at a local high school focused on reaching over a hundred at-risk students through exposure to military values, heritage and way of life.

Equip the Force Through Rapid, Innovative Fielding of Cyber Capabilities

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" and "Real Time Operations and Innovation" initiatives. These efforts have resulted in the fielding of capabilities that have thwarted the exploit 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 developed and fielded in weeks to months.

Similarly, Air Forces Cyber (24th Air Force) is working closely with 25th Air Force to improve our development, fielding and employment of multi-domain capabilities that leverage the Air Force's unique strengths in cyber, electronic warfare and intelligence, surveillance and reconnaissance. The collaboration is enabling Airmen to drive innovative solutions to many of our most challenging operational challenges. It also harnesses the subject matter expertise in other Air Force organizations such as the Air Force Research Laboratory, Air Force Institute of Technology, National Air and Space Intelligence Center, Air University, Air Force Academy, as well as academia and industry to meet growing joint warfighter needs.

Conclusion

We are proud of the tremendous strides made by Air Forces Cyber (24th Air Force) to operationalize cyber capabilities in support of joint warfighters and defense of the nation. Despite the challenge of growing and operating across a 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 nation'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 has been essential to the 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. Finally, resource stability will 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.

MAJOR GENERAL BURKE E. "ED" WILSON

Maj. Gen. Burke E. "Ed" Wilson is the Commander, 24th Air Force and Commander, Air Forces Cyber, Joint Base San Antonio-Lackland, Texas. General Wilson is responsible for the Air Force's component numbered air force providing combatant commanders with trained and ready cyber forces which plan and conduct cyberspace operations. Twenty-fourth Air Force personnel extend, maintain and defend the Air Force portion of the Department of Defense global network. The general directs the activities of two cyberspace wings, the 624th Operations Center, and the Joint Force Headquarters – Cyber, all headquartered at JBSA-Lackland, as well as the 5th Combat Communications Group at Robins Air Force Base, Georgia.

General Wilson entered the Air Force in 1985 as a graduate of the U.S. Air Force Academy after earning a Bachelor of Science degree in electrical engineering. He has served in various assignments, including space and cyber operations, planning, strategy, policy, acquisition and combat support. The general has commanded at the squadron, group and wing levels, as well as served on the staffs of Air Force Space Command, 24th Air Force, the National Reconnaissance Office, North American Aerospace Defense Command, and the former U.S. Space Command. Prior to his current assignment, General Wilson served as the Director, Space Operations, Deputy Chief of Staff for Operations, Plans and Requirements, Headquarters U.S. Air Force, Washington, D.C.

EDUCATION
1985 Bachelor of Science degree in electrical engineering, U.S. Air Force Academy, Colorado Springs, Colo.
1986 Squadron Officer School, by correspondence
1990 Master of Science degree in electrical/computer engineering, Northeastern University, Boston, Mass.
1990 Distinguished Graduate, Squadron Officer School, Maxwell AFB, Ala.
1998 Air Command and Staff College, Maxwell AFB, Ala.
1999 Master of Airpower Art and Science, School of Advanced Airpower Studies, Maxwell AFB, Ala.
2004 Air War College, by correspondence
2004 Back to Basics, Executive Business Training, Darden Graduate School of Business, University of Virginia, Charlottesville, Va.
2005 Secretary of Defense Corporate Fellowship, Cisco Systems, San Jose, Calif.
2006 Joint Forces Staff College, Norfolk, Va.
2009 U.S. Air Force Enterprise Leadership Course, Darden School of Business, University of Virginia, Charlottesville, Va.

ASSIGNMENTS
1. July 1985 – May 1988, design engineer, Space Defense Operations Center; Chief, SPADOC Systems Engineering Branch, Electrical Systems Division, Hanscom AFB, Mass.
2. June 1988 – June 1990, Military Strategic and Tactical Relay systems engineer; program manager, MILSTAR Transportable Terminal, Electronic Systems Division, Hanscom AFB, Mass.
3. July 1990 – June 1994, Operations Director; Flight Director; Chief, Advanced Satellite Planning Division; Chief, Advanced Satellite Management Division, Operational
Detachment 4, Onizuka AFB, Calif.
4. July 1994 – December 1995, Mission Director; Chief, Support to Military Operations Division, Overhead Collection Management Center, Fort George G. Meade, Md.
5. January 1996 – February 1997, executive officer, Deputy Director, National Reconnaissance Office, Chantilly, Va.
6. March 1997 – July 1997, military assistant, Assistant Secretary of the Air Force, the Pentagon, Washington, D.C.
7. July 1997 – June 1998, student, Air Command and Staff College, Air University, Maxwell AFB, Ala.
8. July 1998 – June 1999, student, School of Advanced Airpower Studies, Air University, Maxwell AFB, Ala.
9. July 1999 – June 2000, plans and programs officer; Chief, Plans and Programs Branch, U.S. Space Command, Peterson AFB, Colo.
10. July 2000 – June 2002, Deputy Director, Commander in Chief's Action Group, North American Aerospace Defense Command/U.S. Space Command, Peterson AFB, Colo.
11. July 2002 – July 2003, Commander, 1st Space Operations Squadron, 50th Space Wing, Schriever AFB, Colo.
12. July 2003 – July 2004, Deputy Commander, 50th Operations Group, 50th Space Wing, Schriever AFB, Colo.
13. August 2004 – May 2005, Secretary of Defense corporate fellow, Cisco Systems, San Jose, Calif.
14. June 2005 – June 2006, Director, Commander's Action Group, Air Force Space Command, Peterson AFB, Colo.
15. June 2006 – September 2006, student, Joint Forces Staff College, Norfolk, Va.
16. September 2006 – April 2008, Commander, Space Operations Group, Aerospace Defense Facility – East, Fort Belvoir, Va.
17. April 2008 – February 2010, Commander, Space Development and Test Wing, Kirtland AFB, N.M.
18. February 2010 – August 2011, Commander, 45th Space Wing, Patrick AFB, Fla.
19. September 2011 – June 2013, Deputy Commander, Air Forces Cyber (AFCYBER/24th Air Force), Fort George G. Meade, Md.
20. June 2013 – July 2014, Director of Space Operations, Deputy Chief of Staff for Operations, Plans and Requirements, Headquarters, U.S. Air Force, Washington, D.C.

21. July 2014 - present, Commander, 24th Air Force and Commander, Air Forces Cyber, Joint Base San Antonio - Lackland, Texas

SUMMARY OF JOINT ASSIGNMENTS
1. July 1999 – June 2000, plans and programs officer; Chief, Plans and Programs Branch, U.S. Space Command, Peterson AFB, Colo., as a major
2. July 2000 – June 2002, deputy director/member, Commander in Chief's Action Group, North American Aerospace Defense Command/U.S. Space Command, Peterson
AFB, Colo., as a major and a lieutenant colonel
3. September 2006 – April 2008, Commander, Space Operations Group, as a colonel

BADGES AND RATINGS Command Space Badge
Senior Cyberspace Operator Badge
Basic Parachutist Badge
Basic Acquisition and Financial Management Badge
Certified Acquisition Professional: Program Management (Level III) System Planning, Research and Development (Level III)
Test and Evaluation (Level I)

MAJOR AWARDS AND DECORATIONS Defense Superior Service Medal
Legion of Merit with oak leaf cluster
Defense Meritorious Service Medal with two oak leaf clusters
Meritorious Service Medal with oak leaf cluster
Joint Service Commendation Medal with oak leaf cluster
Air Force Commendation Medal with oak leaf cluster
Air Force Achievement Medal
National Reconnaissance Office's Distinguished Service Medal
National Reconnaissance Office's Superior Service Medal

EFFECTIVE DATES OF PROMOTION Second Lieutenant May 28, 1985
First Lieutenant May 28, 1987
Captain May 28, 1989
Major Jan. 1, 1997
Lieutenant Colonel May 1, 2001
Colonel March 1, 2006
Brigadier General Dec. 17, 2010
Major General April 2, 2014 (Current as of August 2014)

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

MARCH 4, 2015

RESPONSES TO QUESTIONS SUBMITTED BY MR. LANGEVIN

Admiral ROGERS. In December 2012, the Department determined its initial set of resources required to man, train and equip of Cyber Mission Forces (CMF) based on operational requirements defined by the Joint Staff in coordination with the Combatant Commands and U. S. Cyber Command (USCYBERCOM). Based on those requirements, the Department of Defense (DOD) initiated a major investment in its cyber personnel and technologies for the Cyber Mission Force in 2013.

From the initial 2012 assessment, the Services were required to meet the man, train and equip 133 teams with various levels of involvement using the traditional equitable allocation model (Army 30%, Air Force 30%, Navy 30%, Marine Corps 10%) with all teams being fully resourced by Fiscal Year (FY) 2016 Specifically, Army is to provide 41 teams, Air Force is to provide 39 teams, Navy is to provide 40 teams, and Marine Corps is to provide 13 teams. The Department also included integration of Reserve and National Guard personnel in the Cyber Mission Force (primarily as protection forces and surge support) as described in its August 29, 2014 report to Congress in response to FY14 NDAA Section 933 (d). USCYBERCOM looks forward to completion of the Department's effort to fully resource the required command and control structure approved in 2013 by the Chairman, Joint Chiefs of Staff.

Based on Combatant Commanders' requirements expressed in approved plans and prioritized effects lists, the initial mission assessment included distribution of combat mission teams to Combatant Commands (CCMDs) under each of the Service allocations. The initial distribution was re-examined in late 2013 and an alignment adjustment was made to two teams to account for certain increased cyber activity within the 133 team ceiling. Current plans are to complete the build out of the CMF and, once the 133 teams have reached full operational capability (FOC), reassess the force structure to determine what (if anything) should be adjusted based on lessons learned. Additionally, as described in The DOD Cyber Strategy, USCYBERCOM continues to work with Joint Staff to integrate cyber requirements into combatant command plans and may reassess allocation of the CMF based on the results of these activities.

With regards to training, USCYBERCOM published the joint training and certification standards for the Services to follow to ensure consistent training of individuals and teams. While the Department works to develop an enduring Persistent Training Environment (PTE) for the cyber force, USCYBERCOM expanded its joint training exercises (e.g. Cyber Knight, Cyber Guard, and Cyber Flag) to increase certain capability and capacity to help Service personnel and teams obtain the training required and complete the exercises needed for teams to reach FOC. USCYBERCOM will continue to monitor the readiness of the Cyber Mission Force as the Department integrates the CMF into its overall planning and force development activities to recruit, retain, and provide appropriately trained cyber personnel.

When it comes to equipping the force, CMF team needs are based on operational requirements that were initially established at the beginning of the team build outs and continue to evolve or expand as current real world involvement dictates. As described in The DOD Cyber Strategy, USCYBERCOM is working with the Department to develop a Unified Platform that will integrate and establish interoperability between disparate platforms. The Unified Platform will enable the CMF to conduct full-spectrum cyberspace operations in support of national requirements. As cyberspace requirements evolve and expand, the pace to equip the CMF is constrained by the deliberate processes within the acquisition system. The speed in which USCYBERCOM needs the CMF to be equipped with certain capabilities continues to stress the Department's acquisition system built primarily to reduce risks in developing aircraft, ships, and land vehicles and/or oversee major enterprise-wide Information Technology programs where acquisitions occur over a period of years. The pace in which cyber events unfold and adversaries adapt their cyber actions require an agile acquisition system and related acquisition authorities that enable rapid development and fielding of military cyberspace capabilities where USCYBERCOM and combatant command requirements are met in a period of days, weeks, or months. [See page 24.]

General O'DONOHUE. The Air Force continues to meet all accession requirements within the cyber community with highly qualified individuals. To assist with recruiting highly qualified candidates within the cyber community, the Air Force offers Initial Enlistment Bonuses for members enlisting in one of four cyber specialty fields. The member must possess Security+ and/or A+ certification prior to enlistment and enlist for 6 years to be eligible for the bonus and receive an advance promotion to Airman First Class upon completion of specialty training.

In terms of retention, our legacy enlisted cyber support specialties retain slightly better than the Air Force average. However, given the relative infancy of some of our core cyber operations specialties (half of our enlisted specialties are less than five years old and we created a separate officer sub-specialty within the past year), we lack sufficient retention history in cyber operations. As first tour enlistments continue to expire over the next couple of years, we will have a better understanding of longer-term Airmen retention behavior.

Regardless of retention, we continue to be challenged in our newer cyber specialties due to the rapid growth in requirements, which exceeds our trained personnel inventory. It is crucial that we retain our cyber professionals to help close the current manning gaps. As noted, on the enlisted side, we have made concerted efforts to increase accessions and pay retention bonuses where these challenges are most acute. For officers, we are currently exploring how we can leverage the Critical Skills Retention Bonus to retain cyber leaders. Continued Congressional support for all of our special and incentive pays aimed at recruiting and retaining cyber operations airmen is appreciated. We will continue to monitor and assess but it is clear that retaining these professionals is essential. [See page 23.]

General WILSON. Currently, we are not experiencing any major issues in recruiting or retention. While we are competing within DOD, as well as within industry, for top talent, we have a number of advantages. Some of these advantages will only appeal to a small segment of people, but that is all we need. Each Service, or industry for that matter, has advantages and many of these will only appeal to certain people, and that diversity helps us all. Our civilian salary and annual bonuses may not measure up to what industry can offer for a more skilled and highly trained individual. For the civilian Information Technology (IT) personnel, we have limited monetary incentives that can be offered. What we see more than often is our cyber civilian positions offer a way for talented Marines that have trained and grown up in this domain, with hands on experience, but are leaving the service for various reasons; from family, to career, to retirement, a way to stay associated with the Marine Corps. They continue to be a part of the Marine Corps team and gain the stability (in terms of position and PCS moves) or flexibility that can be offered by a civilian position, and so these Marines apply for and earn these positions. We have a number of civilian personnel from other services as well, they too leave their service for some of the same reasons and apply to our civilian positions for similar reasons, and they are still associated with the military, but get to choose where they live and work. Sometimes our applicants have a desire to serve the military, but for various reasons were unable to in the past or now cannot be in the active duty component, so they apply to our positions. As for the Active Duty Marines, especially some of our younger Marines, see cyberspace as a new and exciting domain. We generally have more Marines wanting to come to MARFORCYBER than we have space. The younger Marines have been raised in this domain more than the past generations and for them, continuing to fight our enemies in a domain they are already comfortable with is something they are seeking. Additionally, once they arrive, they receive advanced training and the hands on experience that goes with work. The Marines see cyberspace as the future and want to be a part of it. Some will decide to get out, and as we stated above, some will get out but want to come back on as a civilian. Some go to industry and wish to keep that link to the Marine Corps, so they transition to the reserve component, bringing their industry experience back to the Marine Corps when it is needed and continue to build that knowledge and experience in both realms. Others will stay as long as the service allows them to continue to see this domain grow and mature. [See page 23.]

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MARCH 4, 2015

QUESTIONS SUBMITTED BY MR. WILSON

Mr. WILSON. Several of you mentioned in your testimony something called Unified Platform? What is Unified Platform, and what capabilities will it provide for you? Will there be service-unique capabilities that you believe will be integrated in? From an acquisition perspective, how do you plan to proceed? Do you need any special acquisition authority or a special acquisition process in order to develop Unified Platform in a timeframe that will be useful for the cyber mission forces? How are you working with your service laboratories and program offices to develop the capabilities you will need as part of this initiative?

Admiral ROGERS. [No answer was available at the time of printing.]

Mr. WILSON. What role, if any, do you see the Cyber Threat Intelligence Integration Center playing in your day to day operations?

Admiral ROGERS. [The information referred to is for official use only and retained in the committee files.]

Mr. WILSON. Do you have adequate all-source and multi-intelligence fusion and analysis capabilities for cyber to support the cyber mission teams we are building?

Admiral ROGERS. [No answer was available at the time of printing.]

Mr. WILSON. Several of you mentioned in your testimony something called Unified Platform? What is Unified Platform, and what capabilities will it provide for you? Will there be service-unique capabilities that you believe will be integrated in? How are you working with your service laboratories and program offices to develop the capabilities you will need as part of this initiative? From an acquisition perspective, how do you plan to proceed? Do you need any special acquisition authority or a special acquisition process in order to develop Unified Platform in a timeframe that will be useful for the cyber mission forces?

General CARDON. The Unified Platform (UP) is USCYBERCOM's joint, unifying vision for full-spectrum cyberspace operations that in concept will provide the Cyber Mission Force the ability to seamlessly integrate defensive and offensive operations. In its essence UP is a network of computers, servers, data storage, and analytic capabilities leveraged to maneuver in and out of red space (adversary assets), and an access capability to enter the desired red space. It provides a suite of capabilities to actively defend our network and to project power in and through cyberspace if called upon to do so. While inherently Joint, the intent is that Service presented capabilities can be integrated into a common framework for Joint C2 and execution. While USCYBERCOM's UP vision is driving current and future investments within the service laboratories and program offices, several ongoing pilot efforts are further refining the development of specific requirements. Additionally, through the distribution of a small amount of USCC RDT&E funding we have been able to further the development of emerging technologies and concepts critical to what the Army would present in a Unified Platform construct. These efforts are informing the development of requirements in line with the agile requirements validation and acquisition models currently afforded by updated JCIDS and Defense Acquisition System.

Mr. WILSON. Several of you mentioned in your testimony something called Unified Platform? What is Unified Platform, and what capabilities will it provide for you? Will there be service-unique capabilities that you believe will be integrated in? From an acquisition perspective, how do you plan to proceed? Do you need any special acquisition authority or a special acquisition process in order to develop Unified Platform in a timeframe that will be useful for the cyber mission forces? How are you working with your service laboratories and program offices to develop the capabilities you will need as part of this initiative?

Admiral TIGHE. The Unified Platform is a planned Department of Defense cyberspace operations platform that will enable the Cyber Mission Force to conduct full spectrum Cyberspace operations. The Unified Platform is important in enabling Cyberspace operations approved by the President and directed by the Secretary of Defense to support National and Department of Defense policy objectives in disrupting and denying adversary operations that threaten U.S. interests. It will provide the Navy Cyber Mission Forces an integrated capability that is synchronized with Joint combat operations across multiple geographic Combatant Commanders' AORs. Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet, through its re-

search and development arm, the Navy Cyber Warfare Development Group, is coordinating development and acquisition with service laboratories, industry, and Commander, U.S. Cyber Command.

Mr. WILSON. Several of you mentioned in your testimony something called Unified Platform? What is Unified Platform, and what capabilities will it provide for you? Will there be service-unique capabilities that you believe will be integrated in? From an acquisition perspective, how do you plan to proceed? Do you need any special acquisition authority or a special acquisition process in order to develop Unified Platform in a timeframe that will be useful for the cyber mission forces? How are you working with your service laboratories and program offices to develop the capabilities you will need as part of this initiative?

General O'DONOHUE. Unified Platform is expected to be an operationally responsive infrastructure designed to improve information fusion into an effective, integrated approach that leverages developing cohesive solutions, a single architecture, and reduced infrastructure.

A more detailed explanation will be provided to the Committee by separate correspondence.

Mr. WILSON. Several of you mentioned in your testimony something called Unified Platform? What is Unified Platform, and what capabilities will it provide for you? Will there be service-unique capabilities that you believe will be integrated in? From an acquisition perspective, how do you plan to proceed? Do you need any special acquisition authority or a special acquisition process in order to develop Unified Platform in a timeframe that will be useful for the cyber mission forces? How are you working with your service laboratories and program offices to develop the capabilities you will need as part of this initiative?

General WILSON. [No answer was available at the time of printing.]

QUESTIONS SUBMITTED BY MR. ASHFORD

Mr. ASHFORD. Is there a role for USCYBERCOM in combating Islamic extremist propaganda and online recruiting?

Admiral ROGERS. [No answer was available at the time of printing.]

Mr. ASHFORD. What role does the Reserve Component have in CYBERCOM's manning construct?

Admiral ROGERS. As part of its USCYBERCOM Cyber Mission Force (CMF), in addition to Air Force Reserve Cyber Personnel that support various staffs and units, the Air Force has tasked the Air National Guard to fulfill the requirements for two full time Cyber Protection Teams and the cyber operations element of one National Mission Team. These teams will be mobilized from fifteen Cyber Operations Squadrons either already in existence or being stood up. The Navy and Marine Reserves participation is based on individual augmentation to shortfalls in their parent service. Army Reserve Component teams are being built to support Army Service capability apart from USCYBERCOM's CMF.

Mr. ASHFORD. Do we need more cyber capacity in Guard and Reserve units? Do you believe we need to have cyber-focused units in each of the States?

Admiral ROGERS.The question of whether or not to have capability within each State is a resourcing issue. The current resources allocated to USCYBERCOM require them to continue to be focused on training the nearly 6,200 Cyber warriors assigned to the Cyber Mission Force. Cyber Security is a team effort. Although it might be beneficial to have a DOD Cyber trained capability within each State, in today's fiscal environment, difficult fiscal conditions have USCYBERCOM focusing on building the approved 133 teams.

Mr. ASHFORD. What role does the Reserve Component have in CYBERCOM's manning construct?

General CARDON. The Army and Army Cyber Command, as the Army's service component to U.S. Cyber Command, continue to build a Total Army approach for our cyber forces that will include 21 Reserve Component Cyber Protection Teams. These teams will be trained to the same joint standards as the Active Component cyber force. The Army's plan includes one Army National Guard cyber protection team currently serving on Active Status, 10 Army National Guard cyber protection teams and 10 United States Army Reserve cyber protection teams that are essential components of the Total Army cyber force.

The Army Reserve Cyber Operations Group conducts Defensive Cyberspace Operations support and provides Department of Defense Information Network operations and Computer Network Defense Service Provider support to the Southwest Asia Cyber Center.

United States Army Reserve provides U.S. Cyber Command with cyberspace planners, an intelligence fusion cell, and joint personnel.

The Virginia Army National Guard Data Processing Unit conducts cyberspace operations in support of U.S. Cyber Command.

The United States Army Reserve Military Intelligence Readiness Command, which will transition to the Army Reserve Intelligence Support to Cyberspace Operations Element, provides intelligence support and analysis products to U.S. Cyber Command.

United States Army Reserve personnel serve within the Army's Joint Force Headquarters-Cyber to execute joint cyberspace operations for U.S. Cyber Command.

The United States Army Reserve and the Army National Guard are integral to the Total Army approach to cyberspace operations.

Mr. ASHFORD. Do we need more cyber capacity in Guard and Reserve units? Do you believe we need to have cyber-focused units in each of the States?

General CARDON. Approximately 2,000 Army National Guard (ARNG) and United States Army Reserve (USAR) personnel are or will be trained and equipped to the same joint standards as the Active Component cyber force. Army Cyber Command and Second Army assess that the plan for 11 Army National Guard and 10 United States Army Cyber Protection Teams, and the current and planned additional Reserve Component Cyber elements (which include the Army Reserve cyber Operations Group, Military Intelligence Readiness Command/Army Reserve Intelligence Support to Cyberspace Operations Element, Virginia Army National Guard Data Processing Unit, U.S. Cyber Command Army Reserve Element, and the Army Joint Force Headquarters-Cyber Reserve Component augmentation) do and will provide adequate Cyberspace capacity to the Total Cyber force through FY 2018.

As these United States Army Reserve and Army National Guard units become fully manned, trained, and equipped, we will continue our assessment to determine the right number and mix of cyber capacity for the United States Army Reserve, Army National Guard, and Active units.

Mr. ASHFORD. What role does the Reserve Component have in CYBERCOM's manning construct?

Admiral TIGHE. Navy has realigned 298 enlisted Reserve billets that will be phased in between FY2015 and FY2018 to directly support Navy Cyber Mission Forces. Of the 298 billets, 280 are assigned seven each to the Navy's 40 CMF teams, with the remaining 18 assigned directly to the Joint Forces Headquarters-Fleet Cyber staff at U.S. Fleet Cyber Command. The seven billets assigned to each team serve in an augmentation role allowing the teams to capitalize on the specific cyber-related expertise of individuals in these billets. Under this construct, the Navy CMF teams are afforded an opportunity to maximize their operational capabilities through the employment of Reserve cyber experts, many of whom possess very specific skillsets and knowledge via their civilian careers and training. This "augmentation" construct further allows the Navy to efficiently secure a highly proficient and flexible CMF cadre irrespective of budgetary limits and the constraints of the normal Active Component CMF training pipeline.

Seven enlisted Reserve billets have been realigned to Navy Information Dominance Forces (NAVIDFOR) Command to support its cyber inspection requirements.

Mr. ASHFORD. Do we need more cyber capacity in Guard and Reserve units? Do you believe we need to have cyber-focused units in each of the States?

Admiral TIGHE. Through ongoing mission analysis of the Navy Total Force Integration Strategy, we developed a Reserve Cyber Mission Force (CMF) Integration Strategy that leverages our Reserve Sailors' skill sets and expertise to maximize the Reserve Component's support to the full spectrum of Cyber mission areas. Within this strategy, the 298 Reserve billets, which are phasing into service from FY15 through FY18, will be individually aligned to Active Duty CMF teams and the Joint Force Headquarters-Cyber (JFHQ–C). Accordingly, each Navy Reservist assigned to a CMF billet provides operational support to the team's respective operational commander, including Fleet Commanders, US Pacific Command, US Southern Command, US Cyber Command, and DOD/Defense Information Security Agency. As the Navy builds its Reserve CMF support structure, Fleet Cyber Command and TENTH Fleet conduct ongoing assessments to maximize the Reserve Force's support to CMF operational objectives.

These ongoing assessments look at both the size as well as the location within the Navy's geographic footprint. Navy Reserve cyber assets (CMF billets), which are governed under Title 10 authorities, are located with their respective Active Component team. They are currently assigned to eight of the Navy Information Operations Command (NIOC) centers, which are located in Maryland, Norfolk, Georgia, Florida, Texas, California, Hawaii and Japan. (The Navy does not possess any Title 32 authorities or personnel.)

Mr. ASHFORD. What role does the Reserve Component have in CYBERCOM's manning construct?

General O'DONOHUE. For the Marine Corps we currently provide reserve component augmentation to the MARFORCYBER headquarters and to the Marine Corps Network Operations and Support Center. There is the potential to use the reserve component in less time-sensitive roles to augment the active component. We do not currently have plans for a reserve component role in the cyber mission force in the near term. We are reviewing options for individual augmentation where appropriate; however few in the reserve component possess the required high demand/low density military occupational specialties which limits options for any degree of incorporation into the teams.

Mr. ASHFORD. Do we need more cyber capacity in Guard and Reserve units? Do you believe we need to have cyber-focused units in each of the States?

General O'DONOHUE. The Marine Corps has not identified a surge capacity required for the role of reserve augmentation to the active component beyond the current augmentation levels. Additionally, maintaining the required skills that are required would be difficult given the limited time to train available to the reserve component. We do not provide Guard units.

Mr. ASHFORD. What role does the Reserve Component have in CYBERCOM's manning construct?

General WILSON. The reserve component manning within USCYBERCOM is currently limited to Individual Mobilization Augmentees (IMAs) in support of the sub-unified command mission.

AFCYBER/24 AF/JFHQ–C is has fully partnered with the Air Reserve Component as part of its current and future build-up of cyber operations, to support the Air Force's cyber mission and the DOD's Cyber Mission Force (CMF).

From the outset, the Air Reserve Component, in support of AFCYBER, has been integrated into the Cyber Mission Force build-up of 39 teams. To meet the demand signal of the CMF construct, the Air Force Reserve Command (AFRC) is standing up one Classic Associate Unit in FY16, integrating into a Regular Air Force Cyber Protection Team (CPT) squadron, providing steady-state capacity of one CPT or 30% day-to-day mission share. If mobilized, it will be able to provide manning for three CPTs in a surge capacity.

In addition to the team build in the CMF, the AFRC supports numerous other cyber missions under the 960th Cyberspace Operations Group. The 960 CyOG is comprised of nine squadrons. These units defend the Air Force Networks and key mission systems, train personnel, develop new weapon systems and tools, and provide command and control of cyber operations. In addition to the 960 CyOG, there are Individual Mobilization Augmentees (IMAs) under the AFCYBER/24 AF/JFHQ–C that support various cyber missions.

Between FY16–FY18, the Air National Guard (ANG) is building 12 unit-equipped squadrons to sustain two steady-state CPTs, with each organized into the 30/70 full-time/part-time ratio. The ANG is also standing up a National Mission Team (NMT) unit in FY16. These units will align under two ANG Cyberspace Operations Groups.

In addition to the build-up within the CMF Teams, the Air National Guard support to cyber operations includes five cyber units. These units support Defensive Cyber Operations and Command & Control. Additionally, the Air Guard has one of only three of the Network Operations Squadrons in the Air Force.

Finally, the Air Reserve Component plays a significant role in our Engineering and Installation and Combat Communications. There are 38 AFRC and ANG units supporting these missions and in the last 2 years the Air Reserve Component deployed over 800 personnel supporting the warfighter with these capabilities.

Mr. ASHFORD. Do we need more cyber capacity in Guard and Reserve units? Do you believe we need to have cyber-focused units in each of the States?

General WILSON. TThe Air Force is wholly committed to Total Force Integration across the full spectrum of cyberspace operations. The Air Reserve Component is a full partner in the Cyber Mission Force build in addition to our other day-to-day cyber operations. We are leveraging Traditional Reservists, Air Reserve Technicians and Air National Guardsmen throughout the command to meet our warfighting commitments. Whether it's commanding and controlling cyber forces from one of our operations centers, deploying as part of our Combat Communications team, installing cyber infrastructure around the world, or any other task, each of our Total Force members meets the same demanding standards and serve alongside their Active Duty counterparts.

Today, the Air Reserve Component provides approximately 9,000 personnel to support the Air Force's cyber missions. The majority of the personnel support the Combat Communications and Engineering & Installation missions. An additional 1,300 will be added to support the DOD's Cyber Mission Force. We believe growth

in the Air Reserve Component is an effective and efficient option to reduce risk and meet Combatant and Air Component Commander's requirements as the demand for cyber capabilities increases.

It's important to remember operations in the cyberspace domain are not constrained by physical geography. Similar to traditional air operations, the Air Force has few needs that demand a force distribution model across the 54 states and territories. Cyber missions are a case in point. We understand the National Guard Bureau is also considering the cyber requirement for each of the Governors. One of the force structure strategies under consideration is the alignment of Army and Air National Guard units by FEMA region with the appropriate inter-state support agreements.

○