S. HRG. 115–837

JOINT HEARING TO RECEIVE TESTIMONY ON THE CYBER OPERATIONAL READINESS OF THE DEPARTMENT OF DEFENSE (OPEN SESSION)

HEARING

BEFORE THE

SUBCOMMITTEE ON
CYBERSECURITY

AND THE

SUBCOMMITTEE ON
PERSONNEL

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 26, 2018

Printed for the use of the Committee on Armed Services

Available via http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
40–883 PDF WASHINGTON : 2020

COMMITTEE ON ARMED SERVICES

JAMES M. INHOFE, Oklahoma, *Chairman*

ROGER F. WICKER, Mississippi	JACK REED, Rhode Island
DEB FISCHER, Nebraska	BILL NELSON, Florida
TOM COTTON, Arkansas	CLAIRE MCCASKILL, Missouri
MIKE ROUNDS, South Dakota	JEANNE SHAHEEN, New Hampshire
JONI ERNST, Iowa	KIRSTEN E. GILLIBRAND, New York
THOM TILLIS, North Carolina	RICHARD BLUMENTHAL, Connecticut
DAN SULLIVAN, Alaska	JOE DONNELLY, Indiana
DAVID PERDUE, Georgia	MAZIE K. HIRONO, Hawaii
TED CRUZ, Texas	TIM KAINE, Virginia
LINDSEY GRAHAM, South Carolina	ANGUS S. KING, JR., Maine
BEN SASSE, Nebraska	MARTIN HEINRICH, New Mexico
TIM SCOTT, South Carolina	ELIZABETH WARREN, Massachusetts
JON KYL, Arizona	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY

MIKE ROUNDS, South Dakota, Chairman

DEB FISCHER, Nebraska	BILL NELSON, Florida
DAVID PERDUE, Georgia	CLAIRE MCCASKILL, Missouri
LINDSEY GRAHAM, South Carolina	KIRSTEN E. GILLIBRAND, New York
BEN SASSE, Nebraska	RICHARD BLUMENTHAL, Connecticut

SUBCOMMITTEE ON PERSONNEL

THOM TILLIS, North Carolina, *Chairman*

JONI ERNST, Iowa	KIRSTEN E. GILLIBRAND, New York
LINDSEY GRAHAM, South Carolina	CLAIRE MCCASKILL, Missouri
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts

CONTENTS

SEPTEMBER 26, 2018

JOINT HEARING TO RECEIVE TESTIMONY ON THE CYBER OPERATIONAL READINESS OF THE DEPARTMENT OF DEFENSE (OPEN SESSION)

WEDNESDAY, SEPTEMBER 26, 2018

UNITED STATES SENATE,
SUBCOMMITTEE ON CYBERSECURITY
AND SUBCOMMITTEE ON PERSONNEL,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The Subcommittees met, pursuant to notice, at 2:43 p.m. in Room SD–106, Dirksen Senate Office Building, Senator Mike Rounds (Chairman of the Subcommittee on Cybersecurity) and Senator Thom Tillis (Chairman of the Subcommittee on Personnel).

Members present: Senators Rounds and Tillis, presiding, Wicker, Fischer, Nelson, Gillibrand, McCaskill, and Warren.

OPENING STATEMENT OF SENATOR MIKE ROUNDS

Senator ROUNDS. The Cybersecurity and Personnel Subcommittees meet this afternoon to receive testimony on the cyber operational readiness of the Department of Defense.

Our witnesses are Brigadier General Dennis Crall, Principal Deputy Cyber Advisor and Senior Military Advisor for Cyber Policy; Ms. Essye Miller, Principal Deputy, Department of Defense Chief Information Officer; Lieutenant General Stephen Fogarty, Commander, U.S. Army Cyber Command; and Lieutenant General Vincent Stewart, Deputy Commander, United States Cyber Command.

Welcome.

This hearing will commence in open session in which Senators Tillis, Nelson, and Gillibrand will all make a few opening remarks. At the conclusion of Senator Gillibrand's comments, we will ask our witnesses to make their opening remarks. After that, we will all have our round of questions and answers. We will then transition to SVC–217, the Office of Senate Security, and recommence in closed session. Each of the witnesses may provide additional context and testimony that they were not able to provide in an open setting, and we will then close with another round of Q&A. I encourage members and staff to stay through the closed session, given the gravity of the topic at hand.

The administration recently issued a new policy document, known as National Security Presidential Memorandum 13. The new policy entailed by NSPM–13 replaces that of PPD, or Presi-

dential Policy Directive, 20, which virtually paralyzed the conduct of offensive operations by U.S. Cyber Command outside of armed conflict. I look forward to a Department of Defense briefing on the new policy in the near future. I am hopeful this new policy will enable the Department of Defense to act more nimbly and effectively to counter and deter our adversaries' ongoing cyberattacks on the United States, attacks conducted with virtual impunity.

However, no such policy, however well crafted, will succeed unless U.S. Cyber Command develops and maintains the high level of cyber operational readiness required to implement it.

With the elevation of Cyber Command to status as fully unified command and the Cyber Missions Force's achieving full operational capability in May, the Department's cyber forces appear to have moved beyond adolescence. It is now vital that the current capability and operational readiness of the Command fulfill the requirements entailed by these designations. I invited Senator Tillis and Senator Gillibrand, along with the remainder of the Personnel Subcommittee, because these shortfalls are not limited to traditional readiness measures of equipment and training. Indeed, a great deal of the Department's cyber readiness issues resolve around the shortage of skilled cyber-capable personnel. These shortfalls will only be aggravated if the Cyber Mission Force needs to be expanded in the future. I am concerned that the current recruitment, pay, retention, and career pathway structures in place are not equipped to manage this problem. I am, thus, eager to hear the service or tactical-level perspective from General Fogarty, the operational Cyber Command's perspective from General Steward, the more strategic and governance perspective from General Crall in OSD [Office of the Secretary of Defense], and the CIO [Chief Information Officer] and civilian personnel perspective from Ms. Miller. I am also eager to explore the Department's plans to correct these shortfalls with the Senators of the Personnel Subcommittee today. I am grateful to have their expertise at this table.

An ongoing concern of the subcommittee, which I am sure the Department shares, is that we preempt a hollow cyber force and that we have a cyber force that is adequately staffed and equipped and has the necessary tools, targeting capability, and development capability to respond to operational needs. In particular, Cyber Command needs the indigenous capability, without over-reliance on NSA [National Security Agency], to surveil adversary networks for zero-day vulnerabilities, produce malware to exploit these vulnerabilities, and implant this malware within a reasonable and realistic timeline. Such capabilities are necessary, not only for its own DODIN [Department of Defense Information Network] defense and national missions, but also for those conducted in support of the combatant commands. I am eager to hear about CYBERCOM's [Cyber Command] current capability and activity to assist EUCOM's [European Command], PACOM's [Pacific Command], and CENTCOM's [Central Command] operations.

Each of our witnesses have an important role to play in this space. General Stewart, as Deputy Commander of the Cyber Command, is most directly responsible for the readiness of Cyber Mission Force. General Crall's role in defining DOD [Department of Defense] cyber policy shapes, and is shaped by, the capabilities of-

fered by the Cyber Mission Force. General Fogarty, as Commander of the Army Cyber Command, is the executive agent for the persistent cyber training environment and must man, train, and equip the Army's cyber teams. Ms. Miller and the CIO's office generally retain responsibility for the cyber infrastructure, including that on which the Cyber Mission Force will fight and test their malware across the Department.

I will close by thanking our witnesses for their service and for their willingness to appear today before the subcommittee.

Senator Tillis.

STATEMENT OF SENATOR THOM TILLIS

Senator TILLIS. Thank you, Mr. Chairman.

I'm glad our two committees were able to put together this joint hearing. I think it represents an opportunity to examine an important topic, but also to share information that's instructive to our independent roles on committees. We should do more of them.

Success in the cyber domain is uniquely reliant on highly qualified personnel. Where aircraft carriers, stealth technology, and smart weapons have given the United States a discernible advantage in traditional warfighting domains, the U.S. military doesn't have similar technological edges when it comes to cyberspace. Rather, we must rely on intelligence, creativity, and cunning of our people if we are to be successful in this rapidly changing environment. Since operating in cyberspace is so heavily dependent on access to talented people, we look forward to asking questions on the proper cyber workforce mix, the status of Cyber-Excepted Service, and the larger personnel management issues within the Cyber Mission Force.

I thank all of the witness for your willingness to be here today, and I look forward to the following questions.

Senator ROUNDS. Senator Nelson.

STATEMENT OF SENATOR BILL NELSON

Senator NELSON. In the interest of time, the questions I'll be asking are: "Are the forces the right size? Are they getting the right training? Are they a good match for their mission? Do they have the tools and infrastructure they need? Are we recruiting the right people? How are we retaining them and managing their careers?"

Thanks.

Senator ROUNDS. Senator Gillibrand.

Senator GILLIBRAND. Thank you. I look forward to your statements.

Senator ROUNDS. At this time, I would ask—Ms. Miller, would you like to begin, or did you have planned sequence that you would like to deliver these remarks today?

Ms. MILLER. Mr. Chairman, if you don't mind, we do have a planned sequence.

Senator ROUNDS. Okay.

Ms. MILLER. We'll start with General Crall.

Senator ROUNDS. Very good.

General Crall, begin.

Thank you.

STATEMENT OF BRIGADIER GENERAL DENNIS A. CRALL, USMC, PRINCIPAL DEPUTY CYBER ADVISOR AND SENIOR MILITARY ADVISOR FOR CYBER POLICY

Brigadier General CRALL. I think the sequence should start with the junior person, so I'll certainly oblige, sir.

First, I'd like to thank the committee members for a couple of things. One, for my invite to talk about a matter that's clearly important to the Department and the Nation, but also your continued interest and investment in improving these things that we're about to discuss today. So, I certainly thank you for that.

In your openings, it's very clear that we all understand the challenges we have. We keep talking about competitive spaces in cyberspace, particularly in how we're going to see information contested in our current and future wars that we fight. But, we also have an interesting dynamic, as you've pointed out. We have competition in the recruitment, retention, the training aspect, and development of the cyber workforce. We understand that, in our competition, if you look at it that way—these are really partnerships, but, when it comes down to resources, each of these communities handles these differently, and they all have their own unique allures. For private industry, we know that it's difficult to match some of the compensation packages. It's also difficult to match the speed with which they hire and onboard and start individuals and clear them for some very sensitive projects. On the military or the civilian side for the Department of Defense, we have our own allures, as well: service to the Nation, the ability to perform very unique mission sets you can't do anywhere else, and also the exposure to a wide array of technology that really pulls individuals in. So, we need to understand that, and understand it well.

So, what I'd like to do is cover a couple items very briefly in my opening, and that is to really set the stage for how we—enhancements that we're looking at on how we recruit, how we keep the folks that we recruit, and how we develop or train them. On the closed session, I'd like to use some of that time to talk about the governance structure, as it is classified, tied to our recently published Cybersecurity Strategy, and going into some of those details require that setting.

So, to really get to the meat of what I will present today is in the Cyber-Excepted Service. These are authorities and funding that Congress gave the Department back in fiscal year 2016, and the rollout of that started in 2017. A couple of these incentives are already in place. I'll cover a couple of them, with a few that are being onboarded here really starting in the next 30 days, the first of which is this idea of moving between competitive service and noncompetitive service. The idea of how we take title 5 and title 10, blend them together, and move individuals and attract them to the Cyber-Excepted Service without penalty or loss of grade or seniority. Certainly an attractant. The other is the idea of building qualifications and advancements based on competencies, where you can be rewarded, compensated, and advanced because of the unique training that you have. Finally, increased pay scale. We know that the general service or competitive pay scales stop at the pay band of 10, where the Cyber-Excepted Service, we've expanded that to include pay bands 11 and 12, which offers a little more flexibility

for that professional worker who would have no other place to go or no other incentive to offer. Those are in place today, albeit in a modest fashion. I'll explain the numbers in a minute. But, they are in play.

What we're proposing are a few other items that will, again, start, here, hopefully in the next few months. One of them is the idea of a targeted market compensation. We know that it's difficult to recruit competent quality that we're looking for in every part of the country. In some cases, it's due to high-demand, low-density assets. There's just really a strict competition. In other place, they just don't exist, writ large, where we need them. So, that targeted compensation package will allow us to apply that particular solution to that target set.

We also are looking at the idea of retention bonuses. Current pay caps prevented us from applying these, meaning they were available, but they couldn't be used in other combinations. You've given us the authority to move out, where it makes sense, to apply them, again, to our most gifted workforce.

Finally, the piece the Department has to solve is its long security clearance process. We certainly don't want to compromise the end result. We want to ensure that we understand who we're employing. But, we certainly recognize that we've got to cut down the timeframe. You've asked us to do that. We're—certainly have ways and means in front of us to do just that.

From the total-force side that we're looking at, we're looking at the development and training aspects of this, enterprise and joint training standards. We're just finishing a coding initiative so that we can understand what a Military Occupational Specialty means in language to a civilian hire that we have. Right now, we—every service uses different descriptions. It's difficult to understand how to move an individual from one spot to another. When you're trading spaces and looking at benefits of training, manpower reallocation, and rightsizing the force, you have to start with a common lexicon. That coding effort is largely complete. Goes a long way to making sure that we can develop.

Also, finally, I would say, putting on a career path. What right looks like in a workforce management to ensure that we don't pyramid out; where we have a lot of competent people that are stuck in certain places, but we have either the rotation that they need to go to to continue those skillsets or the advancement opportunities there in front of them. More work to do on that front. Definitely not there yet, but certainly putting brainpower to that.

On the military side, I'd let the generals on the panel discuss the efficiency of some of the things that they're working on, but direct commissioning, we've been given the authority to increase both our rates and the levels in which we do that, very similar to the way that we onboard doctors, lawyers, and chaplains, bringing in those specialists at higher grades initially. Also, the constructive credit, how we can take people who are coming from the workforce and actually give them the credit due for the job skills they've had previously, whether that be in the service or in private industry. So, those two are available for our military side, as well.

Looking at how we phase these, phase 1 was a very modest rollout. We had roughly 363, I believe, slots that we created in Cyber-

Excepted Service, and we targeted U.S. Cyber Command with that initiative to begin with. Almost 70 percent of those billets were filled in relatively short order, which means I think we've got part of the cocktail correct, that the recipe may be right. That's only with half the enhancement packages onboard. But, given the size of our workforce, that's a very small number. Starting this year, we've—we're going to expand that to about 8300 slots, and we're going to target a few others—DISA [Defense Information Systems Agency] and the service cyber components—again, rolling out the full package to see if we can get that mix right.

Some areas that I would tell the committee that I believe we need to improve, and in full transparency, we need to understand our market better. I think we use too much anecdotal evidence and experience to describe what attracts people and why people leave. While I would say that most of it sounds right, and we do have a few studies that look at it, from, you know, doing a couple of recruiting tours, market analysis is key, and we've got to make sure we're dialed in and we're not focusing on a goal that's maybe a year or two old.

We may need to take a look at how we recruit. I think our message is slow to get out. Not everyone knows what our message is. On the military side, I would say the campaign is a little easier, far stronger, and we find that our audiences are more informed. Very few understand what we offer in the Federal Government side that would be an attractant, as well. We've got to do better there.

I attended a ribbon-cutting ceremony with Senator Nelson a few years back at the Cyber Center in Tampa, sir. In both your public remarks and remarks to me privately, you stressed the importance of internships and making sure that we stay connected to academia, that we can build the kind of force we need if they come out of the schoolhouse equipped and right-set for us to put them to work. Neat environment in Tampa, with U.S. Central Command and Special Ops Command right there. I'll tell you, I think our efforts are still too modest. I don't think we've come close to leveraging that requirement and that opportunity. Our intelligence community does that well. They groom very early. They have recruiters at the universities. They teach classes, they stay very connected to that workforce, and we could learn something from that. So, we have the means. They're in front of us. We've got to execute better to get after that. We're a bit slow.

Lastly, I would say we need to ensure that we have a solid baseline and assessment mechanism so, when we come back here and talk to you about what's working and what's not working and how we've spent money, we can do so with the right kind of accountability. We've got to be careful with all these incentives—and you've charged us to be careful with those—to ensure we just don't simply throw money at a problem without making sure that these are targeted, and they're targeted very specifically, and the outcomes are examined so we can keep that machine refined and moving in the right direction.

So, hopefully, with an opener, I'll leave it at that, and either take questions or pass it on for opening.

Thank you.

[The prepared statement of General Crall follows:]

[Deleted.]

Senator ROUNDS. Thank you.

Who would you like to have move next?

Ms. MILLER. Well, Mr. Chairman, had I known General Crall would cover the world——

[Laughter.]

Senator ROUNDS. Okay.

Well, that's okay, because what we're going to do is, we'll take all of your full remarks for the record, but then I'd ask that each of you limit your opening remarks to about 5 minutes, and we'll kind of move from there.

STATEMENT OF ESSYE B. MILLER, PRINCIPAL DEPUTY, DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER

Ms. MILLER. So——

Senator ROUNDS. Ms. Miller, would you like to go next?

Ms. MILLER. So, given that General Crall——

Senator ROUNDS. Very good.

Ms. MILLER.—has done a great job of laying out where we are with policy and governance and how we are looking at the environment, writ large—and I'd like to just add that the Department does face workforce challenges that we need to address—most of the job losses that we've seen here over the last year or so total about 4,000 civilian cyber-related personnel losses. We're going to have to, to his point, work the recruiting piece of this such that we are postured and we know what that industry should look like, what the objectives and the outcomes of those hiring positions should be, and how we manage the force, in terms of career paths. But, keep in mind, too, this is—encompasses more than your traditional IT [information technology] intel role. It also includes some our health occupations, criminal investigation, and other occupational series that we need to keep in mind such that we take a holistic approach to how we execute the mission with our cyber forces and drive effect and outcome.

So, with that, sir, I look forward to your questions. I really appreciate the opportunity to have this discussion with you today.

[The prepared statement of Ms. Miller follows:]

PREPARED STATEMENT BY ESSYE B. MILLER

INTRODUCTION

Good afternoon Mr. Chairman, Ranking Member, and distinguished Members of both Subcommittees. Thank you for this opportunity to testify before the Subcommittees today on the cyber operational readiness of the Department of Defense. I am Essye B. Miller, Department of Defense (DOD) Principal Deputy Chief Information Officer (PDCIO). I am the principal deputy advisor to the Secretary of Defense for information management, Information Technology (IT), cybersecurity, communications, positioning, navigation, and timing (PNT), spectrum management, and senior leadership and nuclear command, control, and communications (NC3) matters. These latter responsibilities are clearly unique to the DOD, and my imperative, on behalf of the DOD CIO in managing this broad and diverse set of functions, is to ensure that the Department has the information and communications technology capabilities needed to support the broad set of Department missions. This includes supporting our deployed forces, cyber mission forces, as well as those providing mission and business support functions. I would like to provide you with an overview of the current state of the Department's cyber workforce policies and programs, as

well as provide you with an update on the Department's implementation of the Cyber Excepted Service (CES) Personnel System.

DEPARTMENT OF DEFENSE CYBER WORKFORCE OVERVIEW

The DOD cyber workforce is currently comprised of four workforce categories. The Office of the DOD CIO is responsible for the policy oversight of two categories, Cyber (IT) and Cybersecurity. The Principal Cyber Advisor (PCA) leads the Cyber Effects category, while the Under Secretary of Defense for Intelligence (USD(I)) is responsible for the Intelligence (Cyber) category. Together, the DOD CIO, PCA, and the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) tri-chair a Cyber Workforce Management Board that works with USCYBERCOM, the Military Departments, Joint Staff, OUSD(I), and other select DOD Components to provide oversight over the management of the DOD civilian and military cyber workforce. Additionally, the Office of the DOD CIO also acts as the Functional Community Manager for 18 civilian occupational series, composed of approximately 52,000 individuals, working with USD (P&R) and the DOD Components to sustain the health and capabilities of each occupation.

Over the past several months, DOD Components have been coding civilian cyber positions, per the Federal Cybersecurity Workforce Assessment Act. In addition to the typical or traditional cyber occupations, DOD also has some individuals performing cyber responsibilities in acquisition and engineering, financial management, health care occupations, as well as criminal investigation and physical security.

The Department does face some cyber workforce challenges. DOD has seen over 4,000 civilian cyber-related personnel losses across our enterprise each year that we seek to replace due to normal job turnover. Most of these job losses fall within the IT Management and Computer Science occupations, but we also have cyber professionals within key engineering occupations such as Electronics Engineering and Computer Engineering. We need individuals across a wide variety of cyber work roles, including: software developers and secure software assessors, system administrators and network operations specialists, data analysts, systems security analysts, and system test and evaluators. Specific to the Cyber Mission Forces, their personnel needs center on planning, coding, forensics, malware, data science, linguists, and cybersecurity professionals.

Congress has been a strong partner in this area. Specifically, through a number of key pieces of legislation, Congress has enabled: the startup of a new personnel management system for cyber, the Cyber Excepted Service; Direct Hire Authority and Advanced-In-Hire Authority for Cyber Workforce positions; other compensation flexibilities; new term appointment authority; and funding for the DOD Cyber Scholarship Program. Each has aided the Department in establishing and maintaining the readiness of our cyber warriors.

We also work closely with other federal stakeholders, through the Federal CIO Council and the National Initiative for Cybersecurity Education (NICE). We share the same concerns on the challenges to find highly qualified job candidates and retain cyber professionals in a hyper competitive job market. Enhanced management practices, such as the implementation of the National Cybersecurity Workforce Framework, will provide greater capabilities to identify personnel requirements and target effective solutions.

CYBER EXCEPTED SERVICE (CES) PERSONNEL SYSTEM

The Cyber Excepted Service is an enterprise-wide approach for managing civilian cyber professionals across the Department. By fostering a culture based upon mission requirements and employee capabilities, Cyber Excepted Service will enhance the effectiveness of the Department's cyber defensive and offensive mission. This personnel system will provide DOD with the needed agility and flexibility for the recruitment, retention and development of high quality cyber professionals. Specifically, the CES will help DOD to streamline its hiring procedures to quickly fill vacant mission-critical cyber positions across the Enterprise. CES lets DOD Hiring Managers recruit candidates from any source and offer more competitive market-based compensation packages.

The Office of the DOD CIO has successfully designed, developed, and implemented the new personnel system for U.S. Cyber Command, Joint Force Headquarters DOD Information Networks, and the Deputy CIO for Cybersecurity. To date, 403 positions have been converted to the CES. We are currently partnering with the DOD Components to begin implementing CES for 8,305 positions across the Defense Information Systems Agency and the Service Cyber Components.

CONCLUSION

DOD recognizes the importance of growing and maintaining the cyber workforce. The recent authorities provided by Congress have allowed the Department to adjust existing personnel policies and to implement new policies that account for this dynamic need in an increasingly important mission area. The Department appreciates the support of both Subcommittees on this important matter. Thank you for the opportunity to testify today and I look forward to your questions.

Senator ROUNDS. Thank you.

General Stewart.

STATEMENT OF LIEUTENANT GENERAL VINCENT R. STEWART, USMC, DEPUTY COMMANDER, UNITED STATES CYBER COMMAND

Lieutenant General STEWART. Yeah. Mr. Chairman, Ranking Members, members of the committee, first of all, thanks for the opportunity to do this. I think the support that we've gotten—that we've received from the committee that's driven us to think about the policy, think about the strategy, think about the readiness of the force, has pushed us in the right direction. So, I thank you for the opportunity to be here.

But, more than that, I thank you for the opportunity to be able to speak about the men and women who make up this cyber force, extraordinary men and women who today are on mission against a threat that's operating—that's pervasive in this space. I look forward to the opportunity to talk about that, and I certainly look forward to the opportunity to discuss that in closed session.

Among the things that we've learned over the last year or so is that success in cyberspace requires—in fact, it demands—persistent engagement, it demands persistent presence, and it demands a persistent innovative spirit. Failure to do that means that we will never compete against near-peer competitors in this space. So, we're thinking our way now through how we move from growing this force to how we persistently engage, persistently have presence and we innovate in this space.

We have shifted from building out those teams to how we build a force that is operationally relevant and is able to deliver outcomes, as necessary, from the Chairman—from the national authorities, all the way through the Chairman.

We've shifted a little bit from building capacity—we think about just personnel and their training readiness—to the capabilities. Those capabilities requirements speaks to our necessity for the right tools or the munitions that we need in order to be successful in this space, the access that we need, the authorities we need, the infrastructure we need, and the intelligence necessary to support operation of a relevant force.

So, we're now melding—in order to get a better sense of readiness, we're melding both capability and capacity against the problem sets that we've been assigned. So, as we look forward, we realize that the future requires us to be continually engaged in order to compete in cyberspace. We're building a combatant command that will be postured for success. We couldn't have built that without—or accomplished what we have for this Nation without your dedicated support that we receive from the committee. The language you included in the Fiscal Year 2019 NDAA [National Defense Authorization Act] was especially helpful, and we thank you

for your continued advocacy and support, and we look forward to your questions.

[The prepared statement of General Stewart follows:]

PREPARED STATEMENT BY LIEUTENANT GENERAL VINCENT R. STEWART

U.S. CYBER COMMAND (USCYBERCOM) STATEMENT FOR THE RECORD

USCYBERCOM's mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national security interests in collaboration with domestic and international partners. Success in cyberspace requires persistent engagement, persistent presence, and persistent innovation. To support the Nation's priorities as a combatant command, USCYBERCOM's focus has shifted from building a cyber force to focusing on readiness, partnerships and building the ethos of a new Command.

USCYBERCOM is diligently working to build a more robust fighting force for the future. We are embracing innovative ways to develop and strengthen our workforce. If we are to maintain our strategic advantage in cyberspace, we must invest heavily in the talent of our people and the resources they need.

USCYBERCOM is acutely aware of the challenges that result from being in persistent contact with the adversary in cyberspace. Our adversaries continue to adapt and evolve . . . so must we.

OPERATIONAL READINESS

One component of our evolution is our approach to measuring readiness. As a command, we have evolved from a model focused on building a force to a model that ensures the sustained readiness of the force we've built. Early in our development as a combatant command, we measured readiness based on number of people and the status of their training. Now that we have matured, previously used readiness metrics are not sufficient to provide a holistic readiness picture. The sustained readiness approach we are developing merges capability metrics with capacity metrics to provide a more complete readiness picture. In other words, our new approach assesses readiness in terms of both "capacity" (people and training), as well as "capability/' (tools, access, authorities, infrastructure, and intelligence).

WORKFORCE

As a trailblazer for DOD's Cyber Excepted Service (CES) personnel system, USCYBERCOM is using new, fast and flexible hiring authorities to tackle civilian vacancies and recruit talent necessary to build our Combatant Command. Outside the confines of the traditional DOD hiring process, USCYBERCOM is pushing past the norms of laborious, slow hiring by actively recruiting talent through job fairs and hiring events where our teams screen resumes and conduct on-site interviews leading to the best candidates receiving intent-to-hire job offers.

For our military workforce, like the other Combatant Commands, USCYBERCOM relies on the Services to recruit and retain the talent we need to deliver joint force objectives for the Nation. We applaud the diligent efforts of the Services to organize, train and equip cyber operations forces, including fully leveraging recruitment and retention incentives and creating talent management programs that grow a robust cyber workforce.

CONCLUSION

Whether civilian or military, the men and women of USCYBERCOM are committed to being part of something bigger than themselves. Our men and women want to make a difference for this Nation, and they do—everyday.

USCYBERCOM is a learning organization continuing to innovate and adapt as we posture our force for success in the cyberspace domain. With the sustained support of Congress, USCYBERCOM will build upon our momentum and continue to defend and advance our Nation's national security interests in cyberspace.

Senator ROUNDS. Thank you, General.

General Fogarty.

STATEMENT OF LIEUTENANT GENERAL STEPHEN G. FOGARTY, USA, COMMANDER, U.S. ARMY CYBER COMMAND

Lieutenant General FOGARTY. Chairman Rounds, Chairman Tillis, Ranking Members, and members of the subcommittee, I want to thank you for the support, from both committees, which is vitally important to Army Cyber Command's continued progress and the critical missions of our dedicated and talented soldiers, Army civilians, contractors, and Reserve and Army National Guardsmen carry out every day on behalf of the Army and the Nation.

The Army's philosophy for training is to train as you fight. For the Army's teams within the DOD Cyber Mission Force, training to a joint standard is predicated on a culture of adaptive learning for operations and form, training at every level. A "train as you fight" philosophy in cyberspace also depends on employing realistic, dynamic, and complex range environments against simulated peer and near-peer adaptive adversaries. Cyber Mission Force training must be tough, realistic, relevant, and holistic, just like it is for the rest of our forces. With the achievement of full operational capabilities for the Army's CMF [Cyber Mission Force] last year, the Army and joint forces are shifting focus to measuring and sustaining CMF readiness. While achieving full operational capabilities of these teams was an important milestone, it is certainly not an end state and doesn't tell the complex story of the Army and joint force's overall readiness to fight and win.

Readiness is a combination of the CMF's ability to conduct cyberspace operations, reflects a team's ability to plan, develop access, report, and maneuver in cyberspace, hold targets at risk, and deliver capabilities based on assigned missions. This is the standard we use for operations, and it must be the standard we use for training. This includes a focus on nonstandard access methodologies, title 10 operator training, and integration with mission partners to improve mission readiness. Again, training as we fight.

Army Cyber Command's mission success rests on our people. We must recruit, retain, and reward the most talented people. As such, we put tremendous focus on talent management. Thanks to your support, Army talent management initiatives continue to show increased results in civilian hiring and military recruiting. But, we do have a challenge with retaining the core skills that we need. We have a superb recruitment pool that we draw from. I think the training is outstanding. They get on the mission. But, our challenge, as the other witnesses have already mentioned, is the compensation to keep that trained force. You know, the average interactive online operator, it takes about 2 and a half years of training to be able to conduct operations. In a 6-year enlistment, you get about 3, maybe 3½ years of useful work out of that individual. So, it's absolutely critical that we roll out, really, the incentives we need to maintain that force.

Now, readiness of the total force requires that our investment in cyber ensure that Active and Reserve and Guard forces are trained and equipped to one standard. We also continue to make progress toward fully integrating the Army's Reserve and National Guard into the Cyber Mission Force. We're already benefiting from the

critical skills the Reserve component brings to bear and look forward to their full integration.

The Reserve component is approved to build and maintain 21 Cyber Protection Teams, 11 in the Army National Guard and 10 in the U.S. Army Reserve. One Army National Guard and two Army Reserve CPTs [Cyber Protection Terms] have already achieved initial operational capabilities. The Army National Guard is scheduled to have all 11 CPTs at full operational capability by fiscal year 2022. In the Army Reserves, 10 CPTs will be fully operational-capable by fiscal year 2024, trained and equipped to the same standards as the Active component. I'll discuss PCT [Persistant Cyber Training] at detail to answer your questions.

One of the things I did want highlight is, my command is getting ready to move from Fort Belvoir down to Fort Gordon, Georgia. We'll do that in about 18 months. That is a significant investment, almost $1.3 billion, that the Army has placed in Army Cyber Command and the Army Cyber Center of Excellence, which is our premier schoolhouse. We train Active, we train civilians, and then we train Army National Guard and Reserve forces. For the Army, this is important, because we'll have the operational headquarters, the operational platform, and the schoolhouse all on the same location. We think that's going to give us the ability to take operators that are in Active missions to be able to move over and instruct, realtime, in the classroom. It also gives a stability for our workforce. You can have an entire career at Fort Gordon, Georgia, if you decide that you wanted to have your family there.

The soldiers, civilians, and contractors from Army Cyber Command are persistently engaged against a wide range of adversaries and competitors in the cyber domain. We remain committed to preserving U.S. superiority in cyberspace and defending the Nation. Furthermore, we are committed to working with our interagency partners, international allies and partners, the defense industrial base, and defense critical infrastructure partners to secure that critical infrastructure. It's worth stating that operations in the cyber domain require problem-solving in ways never employed before by the U.S. Army. But, creativity, aggressive problem-solving, and rapid mastery of new fighting methods are not just possible for the Army, they are, in fact, qualities that lie at the core of our service. I'm confident that, with your continued support, we will continue to make progress and continue to achieve mission success.

I thank you for the opportunity to testify today and look forward to answering your questions.

[The prepared statement of General Fogarty follows:]

PREPARED STATEMENT BY LIEUTENANT GENERAL STEPHEN G. FOGARTY

Chairman Rounds, Chairman Tillis; Ranking Members Nelson and Gillibrand; and Members of the Subcommittees on Cybersecurity and Personnel, thank you for your continued support of the dedicated soldiers and Army civilians of U.S. Army Cyber Command (ARCYBER) and the entire Army Cyber Enterprise. It's an honor to represent the Army's Cyber Team, alongside my colleagues from the Department of Defense and U.S. Cyber Command, to discuss the critical issues associated with sustaining a ready Cyber Mission Force (CMF). My testimony addresses the following topics as requested by the Subcommittees: retaining and maintaining the Army's cyber talent; individual and unit level training of the Army's CMF; integration of the Army's Reserve Component into the CMF; and the development of the National Cyber Range Complex and Persistent Training Environment.

RETAINING AND MAINTAINING THE ARMY'S CYBER TALENT

Army Cyber Command's mission success rests with recruiting, retaining, and rewarding talented people, and as such we put tremendous focus on talent management. Thanks to congressional support, Army talent management initiatives continue to show increased results in civilian hiring and military recruiting. The Army is on pace to man, train, and equip Total Army cyber forces to meet current and future threats. Readiness of the total force requires that our investments in cyber ensure that Active and Reserve forces are trained and equipped to one joint standard. We have established innovative and tech-centric recruiting cells; are exercising our direct hiring authority for cyber professionals supported by Fiscal Year 2017 National Defense Authorization Act; and using internships, scholarship programs, and talent management initiatives focused on attracting, employing, developing and retaining technical people, including our Cyber Officer Direct Commissioning Pilot supported by Fiscal Year 2017 National Defense Authorization Act. The first two 1st Lieutenants under the Direct Commissioning Program are now training and we are assessing the next accessions from hundreds of applicants. With the expanded constructive service credit (up to O6 (Colonel) level) included in the Fiscal Year 2019 National Defense Authorization Act, we intend to attract candidates from a wider pool of applicants in the coming months.

To help the Army resolve some of our toughest talent management and technical challenges, we have partnered with the Pentagon's Defense Digital Service (DDS) to bring technically-gifted soldiers together with interns and top private sector civilian talent to rapidly develop immediate-need cyber capabilities. We have also partnered with DDS on a Civilian Hiring as a Service Pilot to streamline the hiring process for technical talent and better leverage hiring authorities and incentives. We are working with DDS and the State of Georgia to expand this program to Fort Gordon and the region surrounding Augusta, Georgia, the Army's center of gravity for cyber operations and training. This innovative partnership is solving problems and serving as a powerful retention and recruitment tool. Additionally, in partnership with DDS, ARCYBER and the Cyber Center of Excellence launched a training pilot in January 2018 to compress and streamline joint cyber training courses.

INDIVIDUAL AND UNIT LEVEL TRAINING OF THE ARMY CYBER MISSION FORCE

The Army's philosophy for training is to "Train as you fight!" For the Army's teams within the DOD's Cyber Mission Force (CMF), training to a joint standard is predicated on a culture of adaptive learning, where operations inform training at every level. A "train as you fight" philosophy in cyberspace also depends on employing realistic, dynamic, and complex cyber range environments against simulated peer and near-peer adaptive adversaries. Cyber Mission Force training is tough, realistic, relevant, and holistic.

With the achievement of Full Operational Capability of the Army CMF, the Army and Joint Force are shifting focus to measuring and sustaining CMF readiness. Readiness of the CMF's ability to conduct cyberspace operations reflects a teams' ability to plan; develop access; report and maneuver in cyberspace; hold targets at risk; and deliver capabilities based on assigned missions; this is the standard we use for training. This includes a focus on non-standard access methodologies, title 10 operator training, and integration with mission partners to improve mission readiness.

The readiness of our defensive teams is tested daily, during remediation of routine incidents; proactive defensive cyberspace operations; and during contingency operations. Training programs must constantly sharpen our edge to adapt faster than our adversaries. Mission rehearsals, simulating complex conditions, are necessary to ensure sufficient procedures are in place, while real-world operations grow our understanding of our adversaries' capabilities and add a decisive edge to our collective training.

The Army's Cyber Protection Brigade has taken the lead in Cyber Protection Team (CPT) training by developing a concise training manual, known as "Cyber Gunnery Tables," that defines the tasks individuals, crews, and mission elements must master. These tables provide foundational training for individuals and teams and serve as training and readiness validation events, certifying that a crew has the required knowledge, skills, and abilities to participate in collective exercises as part of a mission element. They also provide a metrics-based assessment to determine individual and crew readiness.

The Army's Cyber Electro-Magnetic Activities Support to Corps and Below (CSCB) initiative provides another venue to improve team readiness levels. Teams are integrated into the Combat Training Center rotations, War Fighter Exercises, and senior leader developmental exercises and events that train and challenge supported

units and keep teams proficient on individual and collective skills. Army Cyber Command has built real-time reach-back links between Corps and Below level forces at the National Training Center and cyber operators at Fort Meade, Maryland and Fort Gordon, Georgia, that further enhance training capabilities for the Army's Brigade Combat Teams as well as our cyber forces. Based on lessons learned from the CSCB initiative, the Army will start building a Cyber Warfare Support Battalion (CWSB) in fiscal year 2019, dedicated to integrating tactical operations with strategic cyber capabilities, and supporting Electronic Warfare and cyber planning and integration.

Training is critical for operators and teams, but the CMF also needs infrastructure, tool development, and mission alignment of these ready teams. In 2017 the Army completed the second of two joint mission operations centers for offensive cyberspace operations, located at Forts Meade and Gordon. The Army has also established tool development workspaces at three locations and aligned talented personnel to innovate the creation of these in-house tools. To support this effort, the Army is developing a sustainable career map for tool developer Officers and Warrant Officers.

The Army is also leading the way with broadly-scaled multi-domain exercises for the Active, Reserve, and National Guard components. These exercises take place at existing CTCs and purpose-built environments like Muscatatuck, Indiana's "Cybertropolis" facility. In September, 2018 the Army exercise "Cyber Blitz" based out of Joint Base McGuire-Dix-Lakehurst, New Jersey will allow Total Army forces to synchronize new technologies and define how the information warfare capabilities can be employed in the Multi-Domain fight. Specifically, the Army is looking at how Cyber Operations, Information Operations and Electronic Warfare can be synchronized with maneuver warfare and precision fires to bring effects to bear against adversaries.

THE ARMY'S INVESTMENT IN FORT GORDON, GA AS A POWER PROJECTION PLATFORM

Thanks to congressional support and over $1 billion in cumulative construction and modernization projects, Fort Gordon, Georgia will be the Army's focal point for cyberspace operations and training for responsive and enhanced support to the Army and the Joint forces. The ARCYBER headquarters will relocate to Fort Gordon beginning in 2020. The new purpose-built, modern headquarters will support more than 1,300 new cyber soldiers and civilian employees at Fort Gordon, is projected to be ready for occupation in summer 2020 and fully operational by 2022. The co-location of Army cyber operational and institutional forces will enable collaboration, flow of instructors, and speed up requirements development and acquisition.

Additionally, the transformative modernization project of the Army Cyber Center of Excellence (Cyber CoE) at Fort Gordon will break ground in fiscal year 2019. This will increase training capacity and provide modern training and workspaces to gain efficiencies across the installation. The Cyber CoE continues to make significant progress growing the cyber, electronic warfare and signal workforce. The Cyber CoE is the Army's principal organization for future cyberspace, EW and signal innovation, providing capability through concepts, design and experimentation, across Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy. In addition to training, the Cyber CoE provides force modernization, capabilities and career management for Signal, Cyber and Electronic Warfare forces.

The Cyber CoE trained over 13,000 students in fiscal year 2018. This includes students from the Cyber School, Signal School and the Non-commissioned Officer Academy. The Cyber School trains officers, warrant officers, and enlisted soldiers from all three force components (Active, Guard, and Reserve), provides training across the joint forces, and offers two industry certifications tied to training.

The Signal School provides trained soldiers to the operational force to conduct Department of Defense Information Network (DODIN) operations and cybersecurity, training 17 military occupational specialties and providing 42 industry certifications tied to training. Signal soldiers install, operate, and maintain the Army's portion of the DODIN. The Signal School provides a common foundation in networking fundamentals in support of DODIN Operations to all new Signal soldiers.

INTEGRATION OF THE ARMY'S RESERVE COMPONENT INTO THE CMF

The Reserve Component (RC) is approved to build and maintain 21 CPTs; 11 in the Army National Guard (ARNG) and 10 in the U.S. Army Reserve (USAR). One ARNG and two USAR CPTs have already achieved Initial Operational Capability, the ARNG is scheduled to have all 11 CPTs at Full Operational Capability (FOC)

by fiscal year 2022, and the USAR's 10 CPTs will be FOC by f24; trained and equipped to the same standards as the Active Component.

Beyond the build of these teams, soldiers from the Army's Reserve and National Guard are trained, ready, and on-mission today, performing critical and unique support and effects-delivery roles for Army and Joint cyber missions. The 91st Cyber Brigade was initiated in September, 2017, as the Army National Guard's first cyber brigade. In August, 2017, the all-National Guard Task Force Echo was launched to engineer, install, operate, and maintain critical networks for U.S. Cyber Command.

Our RC cyber soldiers bring critical skills that are a force multiplier. Continued support from Congress for programs to attract soldiers, such as Direct Commissions, Special Duty and Assignment Pay, and Cyber Affiliation Bonuses will assist in recruiting and retaining RC cyber talent.

THE NATIONAL CYBER RANGE COMPLEX AND PERSISTENT CYBER TRAINING ENVIRONMENT

Currently, DOD operates four Cyber Training and Test Ranges: the DOD Cyber Security Range; the Joint Information Operations Range; the National Cyber Range Complex; and the C5 Assessments Division range. The Persistent Cyber Training Environment (PCTE) is a material solution that provides the total cyber force a training platform to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks. PCTE will use resources from all four of the DOD ranges, as well as resources from other existing cyber training facilities.

Headquarters, Department of the Army is the DOD's Executive Agent for Cyber Training Ranges, a responsibility led by the Army's Deputy Chief of Staff, G–3/5/7. Army Cyber Command is in support as a primary advisor to the G–3/5/7, with the Army's Program Executive Office for Simulation, Training, and Instrumentation (PEO–STRI) serving as the lead for acquisition, prototyping, and deployment of PCTE. The entire PCTE effort is governed by a board that includes Army Cyber Command, the DOD's Principal Cyber Advisor, and the Undersecretaries of Defense for Personnel & Readiness and Acquisition, Technology, & Logistics, as well as U.S. Cyber Command's J7, through which the Joint Cyber Service Components take part in shaping the PCTE to meet current joint operational needs.

The PCTE v1.0 prototype was delivered 31 July 2018, just one year after the Army received initial funding for the project, and is currently undergoing limited user assessment, with feedback informing the next prototype, PCTE v2.0. Follow-on capability drops are projected to occur every six months (v2.0 in January 2019; v3.0 in July 2019; etc.). To meet the requirements for individual and lower-level collective training, the Army is also using a commercially available cyber range product. To meet higher collective training tasks, the Army is evaluating another commercial platform used by the U.S. Navy, which provides a broader collective training environment. All Services are currently using, or considering, both platforms to meet training requirements. These tools will be a bridging effort until the PCTE is fully operational.

CONCLUSION

Thank you again for inviting me to appear before you today representing the Army Cyber Enterprise. Your support has been enormously important to the maturation of Army Cyber Command, the Army Cyber Enterprise, and the critical mission our dedicated and talented soldiers and Army civilians conduct for the Army and the Nation. The Army Cyber Enterprise has made tremendous progress during the last eight years—building a cyber branch, schoolhouse, cyber infrastructure, and a Total Army cyber force. Although much remains to be done, I am confident that with your sustained support we will continue to make progress and achieve mission success. The tasks before us are great, however the talent and drive of our people is greater.

Senator ROUNDS. Thank you, General.

This group in front of us as a team has a huge responsibility. Cyberspace, this new domain, requires personnel. The reason that we're doing a program like this with both subcommittees, Personnel and Cyber, together is because we recognize the seriousness of the situation at hand.

General Fogarty, the Army faces significant manning gaps in the roles of tool developers and interactive on-network operators, or, I

think, as we call them, IONs. While the Army needs about 150 operators, for example, it has about half of its requirements. Part of the problem is that the Army has only about 14 spots in the RIOT training, which is Remote Interactive Operational Training, which is provided by the NSA. About half of these personnel will fail the training, meaning that the Army might only see seven graduate to the Cyber Mission Force as capable operators for any given RIOT course. This could leave the Army below the replacement level, given promotions and retirements, and yields a major capability gap. The Air Force has noted to us that the NSA has facilitated—they're obtaining more spots in training, as required, and that, because they send their operators to training later, they are less likely to fail, leaving them without the shortfalls that afflict the Army.

My specific question is, What is the impact of the resulting gaps—in particular, in infrastructure, IONs, and tool developers—on your operations?

Lieutenant General FOGARTY. So, Senator, we have identified three critical missions for—or critical work roles for the offensive force. So, the IONs, the exploitation analysts, and the tool developers. Each one is really—for the Army, is in a different point. So, you've aptly described our challenge with IONs. There are two things that we're doing about this. First of all, as we conduct more and more operations off of title 10 infrastructure—and the Army is really—we were the service that had title 10 infrastructure first, we've got the most robust capability—what we recognize is, not every ION has to be RIOT qualified. We have a title 10 operators course that allows our IONs to actually operate off the title 10 infrastructure. That gives us the opportunity to observe them as they start to act, conduct reps. Then we can identify better those star athletes that we need to send to RIOT. What we're hoping is, we can identify someone who has better aptitude, a better likelihood of actually graduating, and that would essentially double our numbers if we can get that straight, per——

Senator ROUNDS. Excuse me. You don't——

Lieutenant General FOGARTY.—per year.

Senator ROUNDS.—you don't quite have it straight yet, so what is that doing to your operational timelines today?

Lieutenant General FOGARTY. So, what happens, sir, is, with the current limit of 15 per year—and I would say, for the Air Force, we actually gave up slots, both for EAs [exploitation analysts] and IONs, so they could actually get fully operational-capable and meet their timelines. So, we took a little bit of hit there. But, I think the big thing is, we weren't selecting people that were making it all the way through the course. So, by getting them in the title 10 operators course, we get them actually on mission much sooner than we do if we send them through RIOT training. That allows us to determine the best athletes that would then allow us to get them into RIOT, have a much better chance of graduating. So, we think that will increase graduation.

We've also talked to General Nakasone. We think, ultimately, we're going to have to expand the throughput of the RIOT course. So, we think that's going to be necessary to meet our ultimate requirements.

But, we think success, for us, is a number of RIOT-trained operators, and then a larger number, actually, of title 10 operators. Because, again, as you said very eloquently, we've got to get off of the NSA platform, become more independent. The title 10 infrastructure with title 10 IONs actually allows us to achieve that goal.

Senator ROUNDS. One thing that I'm going to ask, for the record, of both you, General Fogarty, and also for you, General Crall, is a timeline for actually meeting the guidelines necessary to make that happen.

[The information referred to follows:]

Lieutenant General FOGARTY. Since the standup of the Cyber Mission Force (CMF) in 2012, the work roles presenting the greatest training and retention challenges for the Army are Interactive on-Network Operator (ION) and Tool Developer (TD). Both are high demand, low density work roles requiring personnel with advanced technical aptitude, training and certification. Since 2012, changing mission requirements, organic platform developments, and programmatic changes necessitated a revised model for Army's training of IONs. The Army developed our own interactive cyber operator course external to NSA's training pipeline with a curriculum informed by and more directly supporting the evolving USCYBERCOM mission. Since the Army's development of this course in 2017, as of January 2019, 73 Army students have graduated, and over 21 individuals have been Joint Qualification Reviewed (JQR)-certified and are on-mission supporting USCYBERCOM operations. The remainder are fulfilling JQR requirements. The Army plan going forward is to hand-pick the high performing graduates of this course and select them for the RIOT course. We project this will increase graduation rates, and help close the ION gap. Tool Developers (TD), much like IONs, fill a critical role in the execution of cyberspace missions by building software and hardware capabilities to enable a variety of operations. To better serve the TD mission, the Army built a developer environment that enables the rapid production and delivery of cyberspace capabilities to our operational force. Our experience indicates officers and civilians are the best equipped to fill the TD work role, often arriving with computer science, electrical engineering, or computer engineering degrees. As a result, the Army developed the Tool Developer Qualification Course (TDQC) in partnership with the University of Maryland Baltimore County (UMBC) Training Center. The 11-month course provides students with the basic fundamentals of computer science and programming. The average class size is 14, with a graduation rate of approximately 75 percent. The high pass rate is directly attributed to the strong emphasis placed on identifying and assessing the best candidates for the course. Since 2016, the Army has successfully graduated 64 soldiers. The Army executes assessment tests and selection panels to identify the best qualified TD and ION candidates. The most experienced in the force administer the assessments and oversee the selection panels, ensuring the prospective candidates understand the rigors and challenges ahead of them. Once a candidate is selected, (e.g. IONs for RIOT), a mentor is assigned to them to ensure help is available should the need arise. However, the aptitudes and talent required for ION and TD roles come from the same population. As we improve recruiting and training, we must also improve retention of our Cyber force. The attrition rate of trained IONs and TDs equals or exceeds the production rate of new personnel. Part of the challenge with this highly technical force is compensating trained and experienced IONs and TDs at an appropriate level. Currently HQDA has authorized the maximum Selective Retention Bonus it can provide ($72,000 for a 6-year re-enlistment) for enlisted soldiers serving as IONs, TDs, and Exploitation Analysts (EA). HQDA has also implemented a Written Bonus Agreement that will have a maximum of $100,000 for an additional four years of service for our most experienced senior Non-Commissioned Officers, and has approved Assignment Incentive Pay ranging from $200–$500 a month and Special Duty Assignment Pay ranging from $150–$300 per month for personnel trained and serving in these key work roles. ARCYBER leadership continues to work with HQDA to maximize the benefits that can be provided to these soldiers by law, in order to reduce the compensation gap that can be offered by the private sector, or even other governmental agencies.

Senator ROUNDS. General Crall, I'm out of time, but the same questions that I've asked of General Fogarty I will be asking of you for the record, as well.

[The information referred to follows:]

Brigadier General CRALL. [Deleted.]

Senator ROUNDS. Thank you.

With that, Senator Tillis.

Senator TILLIS. Thank you, Mr. Chair.

Again, thank you all for being here.

General Crall, thank you for, I think, covering good landscape in your opening comments.

Ms. Miller, my first question is for you. I believe you chair the Cyber Workforce Management Board. Is that correct?

Ms. MILLER. Yes, sir, along with——

Senator TILLIS. And P&R [Personnel and Readiness] co-chairs, right?

Ms. MILLER.—P&R, exactly.

Senator TILLIS. Tell me a little bit about how that relationship works, and how the roles are playing out right now.

Ms. MILLER. Well, actually, sir, we're very well aligned. The board was charted to manage the health and welfare maturity of the force, both civilian and military, so we have an opportunity to oversee and assess the use of the force, how we are doing on the recruiting and attracting, as General Crall talked about. Predominantly, efforts have been focused on Phase 1 and how we code the positions, identifying the work roles and understanding where our shortfalls are and where we need to focus our efforts. But, I think it's pretty safe to say, the relationship between the three organizations are very closely aligned. We meet on a regular basis, and our staffs are joined at working the issues, be it with the coding or with the hiring-and-retention piece.

Senator TILLIS. This question is probably for all of you. I spent virtually all of my professional career in technology, first in research and development, then architecture definition, deployment, and then project execution. Sometimes I worked at Pricewaterhouse, so sometimes we would acquire another firm, or at IBM we would acquire another firm, and it would be standing alone, but it really didn't make sense to have it stand alone for long. In most of your mission sets, I can see a very rational basis for—the mission of the Marines has its own kind of training, tools, tactics, it's separate from the Army, the Navy, the Air Force. But, in this domain, I'm struggling—except at the atomic level, maybe equipment that you need to a service line—I'm struggling to understand why we're not looking at a more innovative way to leverage—you know, we had matrixed organizations, where we have the silos of the service lines now, or we had market domains or technology domains—but the common platform that we're talking about, can you explain to me the rationale for having—and the risk of having duplicative systems and environments and potentially sub-optimizing some of the cross-learning? I'm not saying that any one service should own it, but I'm wondering whether or not we should be looking at a very different structure than the current trajectory.

Lieutenant General STEWART. Let me take the first shot at this one. In fact, what we've designed and what we've put forward, Senator, is what we call the Joint Cyber Warfighting Architecture. It is an integrated architecture. It includes building common firing

platforms, common set of tools, common infrastructure, common cockpit for command and control. Now, none of the services will do that by themselves, but we will designate a specific service to build one element of that Joint Cyber Warfighting Architecture.

Senator TILLIS. So, a center-of-excellence sort of capability.

Lieutenant General STEWART. So, for the training component, the Army will take that persistent common training environment. so, they will bring that into a common architecture, where U.S. Cyber Command will set the standards, set the information exchange protocols, and then each of the elements within our subordinate elements within Cyber Command will build those pieces and those components to a common standard. So, we get the idea that we don't want each of the services build their own unique tools, build their own training environment, build it on—and so, now we've put that all together, and we structured that into what we call the Joint Cyber Warfighting Architecture.

Senator TILLIS. And the government——

Lieutenant General STEWART. So, we're moving in that——

Senator TILLIS. Okay.

Lieutenant General STEWART.—direction.

Senator TILLIS. Because I'm going to be limited on time—I have to step out briefly to go to a VA [Veterans Affairs] Committee—I think that the—with respect to something that General Fogarty and I talked about, and as Chair of the Personnel Subcommittee, we have provided some authorizations that, hopefully, are helping you be a little bit more competitive recruiting and retaining resources. But, you can expect that we'll have a hearing in Personnel to talk about what more we can do.

General Crall, you made a very important point. If we're giving you these authorities to use to be more competitive, but we're also going to be expecting seeing how they've been used and what the results are. We'll discuss those in the—we'll discuss those in the hearing or in meetings that we'll have in my office.

For many of you, I've got a lot of questions, and I know—I'm looking forward to getting back so we can go to the closed session, but I'll probably have a number of questions that are structural in nature that'll be instructive to some of the work we'll be doing on the Personnel Subcommittee.

Thank you, Mr. Chair.

Senator ROUNDS. Thank you.

Senator Nelson.

Senator NELSON. General Stewart, how are we going to objectively measure the readiness of Cyber Mission Force to execute their mission?

Lieutenant General STEWART. So, we know we have a standard now that the Chairman measures: personnel readiness, number of folks that the services are providing, the level of their training. So, we have a standard approach for measuring that. Now, what we have to do is—in U.S. Cyber Command, is clearly define the mission essential task and the joint mission essential task that says, "When a team is presented to us, here are the things that we need them to do against a particular target set." That is more than just the personnel. That's easy objective measurement. The services are either providing them at a certain level or they're not, they're ei-

ther trained to a certain level or not. Quite frankly, the services are doing a remarkable job in presenting personnel.

Senator NELSON. Will the combatant commanders understand this so-called meaningful set of metrics that you're talking about, a standard?

Lieutenant General STEWART. There is no doubt in my mind that we've identified intelligence requirements that are essential for delivering capabilities, we've identified access requirements that are important, we've identified tools and munitions that are important, we've identified architecture that's important to get to the target. Those are things that I think any combatant commanders would understand, "In order for me to have an operational effect, here are the things that I must have in order to deliver those outcomes." So, we think that's pretty well-defined, and we'll continue to refine that over time.

Senator NELSON. So, how are you going to make sure that the services are giving you what you need in their training and standards?

Lieutenant General STEWART. We've now mandated or laid out the requirements for 1,000–2,000 level. That's the basic entry-level training. The services are building capability and capacity. We were just down in Georgia, had an opportunity to see the things that the Army was doing. All of the services understand the requirements. Quite frankly, Senator, I think they're delivering a fairly capable—and I say that, "fairly capable," because we now have to take them, when they come to Cyber Command, and take them from the journeymen and the apprentice level to the mastery level. I think the services are doing a remarkable job, and we have to—to go back to the question on ION's, for instance, we have to now define whether or not we have the right number of ION's on the teams. We started with a number, based on our best guess of how we would operate in the space. The reality is, we may not need as many ION's, and that will change the training requirements and allow us to do some things that are more creative to get our workforce from journeyman, from apprentice, to a mastery level. I—we're working to refine those as we speak.

Senator NELSON. General Fogarty, the Secretary assigned to you the job of building a cyber range and training system. Why aren't all of these separate ranges being consolidated and moving to a cloud?

Lieutenant General FOGARTY. Senator, currently, there are so many ranges—there are so many ranges. I'm the executive agent for the training ranges. There are a whole series of test-and-evaluation ranges that TRMC [Test Resource Management Center] is the executive agent for.

Services have built ranges. So, what we're trying to do at this point is start to move these ranges, connect them. The objective actually is to move them into the cloud. So, that's the direction we believe we need to be at.

But, it's—I think it's similar to many challenges. Over a long period of time, you had organizations that built their own capability because they had an immediate need for it. We're at the point now where we're—we've inventoried those. We know what the advantages and disadvantages of the different ranges are, how to better

connect them. There are certain ranges that, frankly, we'll probably have very limited interest in. It doesn't mean there's not a requirement, but it's not for the Cyber Mission Force. There's others that are very robust. We don't want to duplicate that. We actually want to connect to those ranges.

Senator NELSON. Can I assume that what you're saying is that you're going to move to the cloud so that you don't have to constantly upgrade the in-house computing infrastructure?

Lieutenant General FOGARTY. Senator, that's actually a succinct way of saying that, but we're——

Senator NELSON. Okay.

Lieutenant General FOGARTY.—we're not there yet——

Senator NELSON. Let me——

Lieutenant General FOGARTY.—for sure.

Senator NELSON. Let me ask General Crall. Cyber Command, created in 2009, but it wasn't until 2013 that we actually started to build the mission force. So, a number of years, we had a command with no forces. It took another couple of years for the Department to start the acquisition process for command and control, network, infrastructure, weapons, and so forth. Why the delays?

Brigadier General CRALL. Sir, that's probably a question that I'll have to go back and do some forensics to give you an adequate answer. I can give you a few answers that I think apply generally, and certainly not making excuses. But, understanding what rightsizing looks like, I've learned the challenges of moving anything quickly in the Department. Matching resources, at the time they're available, with the need and the planning that we're trying to execute has also been a challenge. You could ask the same question on our infrastructure, writ large. We've been modernizing our IT infrastructure for 10 years, at least, in a holistic fashion. Change has been difficult, but I think we're looking at the problem set in a new way. And, in the closed session, we're going to lay out a placemat for you to consider the "eaches" of how we're trying to do this in a way that makes some sense. But, I'll tell you, sir, one of the areas that we're making improvements on, General Stewart has already covered. We've allowed too much of unique building. Lack of standards, allowing each person to do what's right in their own eyes in the process, and not holding individuals or services accountable for a common standard, I believe, have all been contributors, and significant contributors, to delays.

Senator NELSON. Thanks.

Senator ROUNDS. Senator Gillibrand.

Senator GILLIBRAND. General Stewart, I appreciate that your authority is focused on addressing foreign cyberactivities and you're constrained in working on domestic matters. However, I'm very concerned that foreign adversaries have abused the borderless nature of the Internet to stage cyberattacks on our domestic critical infrastructure, such as our election system. How do you coordinate with domestic Federal agencies, as well as local and State agencies, where much of our election security is entrusted?

Lieutenant General STEWART. Well, we're generally not, Senator, directly interfacing with the State and local levels. We are, in fact, working closely with the Department of Homeland Security. We've had a series of engagements to ensure that they understand the

threats as we see the threats, that we've asked them to pass those indicators of compromises down to the States so they can also see the threats. So, we're working this, to borrow a phrase, by, with, and through DHS [Department of Homeland Security] to get the insights that we have, both from Cyber Command and from our NSA partners, turn those into real indicators, and pushing those out to the State and local level. Beyond that, we have limited authority to go to the State and local levels.

So, if I were going to use this platform to send a message, I suspect the message would be: As we move indicators of compromise from DHS down to the State levels, how do we make sure the States are loading those indicators of compromise onto the appropriate sensors and then passing them back up through DHS so that we can be proactive in going after the adversary in gray and red space?

Senator GILLIBRAND. It also sounds, though, that your limited authority is limiting for you. I'm concerned that, you know, you have a mission to protect this country and our critical infrastructure. That's part of Department of Defense mission. But, you've not been given all the authorities you need, in fact, to prevent or stop or respond to cyberattacks to critical infrastructure if it has to do with the electoral system. I think that's a mistake. So, one thing that I hope you will do is seek the authorities that you think you need from this committee, because, regardless of what the administration believes, I believe that better coordination, more holistic coordination, through the National Guard perhaps, so that the States can have on-the-ground expertise that is feeding information and data and intelligence back up to the Department, so that you have a fully integrated defense system for this country. Because if they were bombing a powerplant or they were bombing, or even cyberattacking, a powerplant, you might have a response, or a responsibility, but, because somehow it's an election infrastructure, you have to stay hands-off. So, I hope that you will seek authorities, as you believe from your expertise you think you should have them.

Lieutenant General STEWART. In the closed session, we should probably talk about the changes in authorities over the last 6 months.

Senator GILLIBRAND. Correct.

Lieutenant General STEWART. If you had approached me 6 months ago about the limits of our authorities, I would tell you that it would cause me great frustration.

Senator GILLIBRAND. Yes.

Lieutenant General STEWART. We're in a much better place today, Senator.

Senator GILLIBRAND. I understand. But, I think there's even more authority that you should seek, especially in giving more support to the National Guard to continue to be eyes and ears on the ground. We will—I will pursue this more in closed session, because I think it's so vital.

General Crall, the military's ability to pay for high-quality educational degrees through ROTC [Reserve Officer Training Corps.] programs or direct accession programs for skilled doctors and lawyers have undoubtedly played a key role in recruiting talented indi-

viduals into our uniformed ranks. In addition to paying cyber operators for the skills through specialized compensation, I also believe we should leverage our ability to pay for the educational—education of servicemembers and civilians interested in joining the cyber workforce. Do you believe that a cyber ROTC scholarship or advanced degree-holders would help us to attract skilled military cyber officers?

Brigadier General CRALL. Ma'am, I do. I believe that's a wise course of action. In fact, in the opening, we talked about expanding all the opportunities. But, what I would also add to that is, it's important for us to ensure that, when we track this, we learn what's working and what doesn't work. I've found that sometimes these things are a bit counterintuitive. We have to apply our resources properly, as you would expect us to, and we want to make sure, as the markets change, we follow those trends very carefully and we apply our valued resources to the right population groups and pockets.

But, I will say this. Every university—this is anecdotal, this is me walking around and talking to people in these environments—it is the most talked-about subject matter. Whether we're at the service academies or out in the local communities, we've got a large force of young civilians who are very interested and eager to work in the cyber workforce.

Senator GILLIBRAND. Thank you.

Thank you, Mr. Chairman.

Senator ROUNDS. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman.

Thank you, to our witnesses, for being here today.

Talent management is a critical component of the ability to maintain cyber readiness. That means that we need to recruit and retain for a set of skills that might not necessarily be considered traditional military skills. I was glad to see that talent management is included as a key component of the Department's updated cyber strategy, which was released last week. But, the strategy doesn't offer much detail on the specifics of how exactly the Department plans to recruit and retain men and women with the necessary skills.

So, can I start with you, General Crall? Can you be more specific for us on the Department's long-term plans for cyber talent management?

Brigadier General CRALL. Yes, ma'am, I can. I'll also share with you some shortcomings in that, because I think your instincts of maybe—on some of the leads of understanding that market, we may not be as refined as we need to be. I share—if those are your concerns, I share some of those.

But, yes, when it comes to developing, you know, the recruitment aspect, the military side has a very unique recruiting campaign and designated workforce that gets after that, professional recruiters who work very aggressively at ensuring that message is out. In part of my opening, I described a kind of a vacuum for the Federal Government side. The civilian side, we really don't have, even the initial tenets of our Cyber-Excepted Service, well known. So, we need to get our message out, for one.

One of the ways that we could get that message out is to ensure that we have very robust presences in areas where these people are being trained—in academia, you know, our universities, internships, exchanges with private sector—all of those areas where we can get natural exposure to some of those benefits that only we can provide. And, while it's still, I would say, maybe anecdotal to express it this way, the people that we've spoken to have explained very carefully their desire to serve the Nation, do unique mission sets they can't do in the private sector, and work with emerging technology. Those are things that we can offer that—very unique to our government. So, yes, we need to do more in that.

On the civilian side for Excepted Service, I had mentioned we've covered a few to close some of the pay gaps. Congress has given us the authority to address some of those, to include regional pay gaps, compensation, higher step increases. But, those are normally only known by those who are really at our doorstep already. We need to do a better job of getting the word out on what we can offer, and to pursue those individuals at a very early start.

Senator WARREN. Well, I'm very glad to hear this, General Crall, and glad to hear your enthusiasm for this. You know, our readiness is only as good as our people. If we don't recruit and retain the best and offer the kind of career incentives for people to stay in public service, then we can't mount an effective cybersecurity defense or response. So, thank you for that.

I have one other issue I want to raise. I am a big supporter of the Defense Innovation Unit, which has an office in Cambridge, for piloting new approaches to technology, including cyber and software engineering. I want to ask about one of those experiments. In 2016, the software system at the Al Udeid Air Operations Center in Qatar was so outdated—are you ready for this? In 2016, airmen were using a flight board to manage aerial refueling. Now, in response, DIU [Defense Innovation Unit] worked with the Air Force to sponsor a small program, called the Kessel Run, to teach Active Duty Air Force personnel how to code. In the span of 4 months, at a cost of just about $2 million, they designed a software application that automated the refueling. And because the airmen now have the coding skills, they can continuously update that software to meet the mission.

So, maybe I could ask you, Ms. Miller. Do you think having in-house coding ability like this can also help improve our cyber operational readiness?

Ms. MILLER. Yes, ma'am, I do. That's actually one of the skillsets. If you look at the list of specific skills that we know we need to mature, that is one at the top of the list.

Senator WARREN. So, we're trying to build this in-house. I think that makes a lot of sense. I'm glad to hear it. But, getting the Kessel Run Development Lab up and running was not easy. I understand there was some real resistance within segments of the Department. So, the question I want to ask is, How can we normalize and scale these types of programs up and make technical skills, like coding or cyber defense, a core competency for Active Duty personnel and defense civilians?

General Crall, it looks like you want to answer.

Brigadier General CRALL. Yes, ma'am. This is an exciting question, because you're——

Senator WARREN. Good.

Brigadier General CRALL.—you're spot-on. We have young folks, who are—have zero experience in doing this formally, who are writing programs for us today. Going back to my answer earlier, the proper venue and outlet for this is to ensure that we have the right developers toolkits and the right coding infrastructure, the lateral limits, left and right, so that they know what standards to write these to. We spent a lot of time and frustration in the Department of trying to make these disparate software applications communicate with each other. In the closed session, I can cover some of the solutions we have. But, they are screaming for ways to contribute, and we are taking that onboard, and it's showing great promise. But, there is a lot of work ahead, ma'am.

Senator WARREN. Good. So, I—again, I'm glad to hear your enthusiasm, but I sure want us to concentrate on how we can scale this up and normalize it within the Department.

Thank you.

Thank you, Mr. Chair.

Senator ROUNDS. Thank you, Senator.

Okay, this will conclude the open portion of the session. My intention is to recess until 4 o'clock, and that will be in SVC–217.

At this point, we will recess.

[The open portion of the hearing concluded at 3:42 p.m. The Subcommittees recessed until 4:00 p.m. to meet for the closed portion of this hearing.]

[Questions for the record with answers supplied follow:]

QUESTIONS SUBMITTED BY SENATOR M. MICHAEL ROUNDS

REDUNDANCY

1. Senator ROUNDS. Lieutenant General Stewart, to serve in the interim as the Unified Platform is developed, does Cyber Command have or plan to develop an integrated database or organizing structure of all tools and tool development efforts in the Services and its own capabilities development group?

Lieutenant General STEWART. [Deleted.]

2. Senator ROUNDS. Lieutenant General Stewart, what redundancies has Cyber Command seen in the Services and what efforts are underway to mitigate them?

Lieutenant General STEWART. [Deleted.]

MISSING AUTHORITIES AND OUTSTANDING RESOURCE ISSUES

3. Senator ROUNDS. Brigadier General Crall and Lieutenant General Stewart, please provide a list of missing authorities, outstanding resource issues and misallocations, and interagency issues that are hampering the readiness of the Cyber Mission Force, to include difficulties in using accesses and tools that originate with the intelligence community.

Brigadier General CRALL. My fellow witness, Lieutenant General Stewart, is best positioned to provide a response regarding the authorities related to the Cyber Mission Force.

Lieutenant General STEWART. [Deleted.]

TOOLS

4. Senator ROUNDS. Lieutenant General Stewart, how much do each of the Services and how much does CYBERCOM spend on tool development each year? How does this compare with the NSA?

Lieutenant General STEWART. [Deleted.]

5. Senator ROUNDS. Lieutenant General Stewart, what efforts—manning, technological, and policy—are underway to accelerate CYBERCOM's tool development (including accessing and surveilling of adversary networks)? How can Congress help?
Lieutenant General STEWART. [Deleted.]

INFORMATION WARFARE

6. Senator ROUNDS. Brigadier General Crall, what efforts are underway to integrate cyber operations with information operations, electronic warfare and military deception especially at CYBERCOM? How can Congress help in this regard?
Brigadier General CRALL. [Deleted.]

7. Senator ROUNDS. Brigadier General Crall, how are the PCA and CYBERCOM working with ASD(SO/LIC) and SOCOM to integrate information warfare into cyber operations? What efforts are still required?
Brigadier General CRALL. [Deleted.]

METRICS

8. Senator ROUNDS. Lieutenant General Stewart, it is our understanding that the readiness metrics CYBERCOM uses are built off of those used for conventional forces, assessing manning, training, and "equipment" as percentages instead of measuring the capability and capacity of a given team. How do these metrics compare to those used by SOCOM, and is work underway to determine what the best metrics to measure force capability are going forward?
Lieutenant General STEWART. [Deleted.]

9. Senator ROUNDS. Lieutenant General Stewart, please provide a complete spreadsheet of the manning status of each required position—including tool developer, exploitation analyst, and on-network operator—for each team in the Cyber Mission Force.
Lieutenant General STEWART. [Deleted.]

TIMELINES

10. Senator ROUNDS. Lieutenant General Stewart and Brigadier General Crall, with the Department's cyber posture review and recent policy changes, what is the expected future operational timeline from identification of a target to insertion of malware?
Lieutenant General STEWART. [Deleted.]
Brigadier General CRALL. I support the responses from my fellow witnesses, Lieutenant General Stewart and Lieutenant General Fogarty, on this specific question regarding the expected future operational timeline from identification of a target to insertion of malware.

COMBATANT COMMANDS

11. Senator ROUNDS. Lieutenant General Stewart, how many of EUCOM's priority Russian targets has Cyber Command compromised? For how many of these has Cyber Command developed or identified an extant tool? For how many of these has Cyber Command delivered the tool?
Lieutenant General STEWART. [Deleted.]

12. Senator ROUNDS. Lieutenant General Stewart: How many of PACOM's priority Chinese targets has Cyber Command compromised? For how many of these has Cyber Command developed or identified an extant tool? For how many of these has Cyber Command delivered the tool?
Lieutenant General STEWART. [Deleted.]

QUESTIONS SUBMITTED BY SENATOR KIRSTIN GILLIBRAND

CIVILIAN PERSONNEL AND CYBER FORCE MIX

13. Senator GILLIBRAND. Brigadier General Crall, Cyber Command appears in many respects to have been conceived along the lines of a traditional military operational unit, meaning most immediately that "operators" are primarily military personnel. This has led to much discussion about relaxing military standards to enlist or commission nontraditional recruits for military service. Meanwhile, civilian employees are not subject to these standards, cost less to the Government in terms of pay, benefits, and training, and generally can stay in one place longer as part of a successful career. Moreover, civilian positions can be filled by individuals who are

otherwise not interested or qualified to serve in uniform, leaving those military recruits available for other military duty. For those who are qualified to serve, civilians can also serve in the Guard and Reserve as a compliment to their civilian duties. What is your view of the proper use of civilian personnel in building the cyber force?

Brigadier General CRALL. [Deleted.]

14. Senator GILLIBRAND. Brigadier General Crall, what is your view of the optimum force mix of military and civilian personnel?

Brigadier General CRALL. [Deleted.]

15. Senator GILLIBRAND. Brigadier General Crall, what is the proper force mix between Active Duty and Reserve personnel (who may also be full time civilian employees within the command)?

Brigadier General CRALL. My fellow witness, Lieutenant General Fogarty, is best positioned to provide a response regarding the proper mix between Active Duty and Reserve personnel.

16. Senator GILLIBRAND. Lieutenant General Stewart, among the operational billets in Cyber Command, what percentage are filled by civilian personnel?

Lieutenant General STEWART. [Deleted.]

17. Senator GILLIBRAND. Lieutenant General Stewart and Lieutenant General Fogarty, are any restrictions on the hiring of civilian personnel hampering your ability to hire more civilians? If so, please explain.

Lieutenant General STEWART. [Deleted.]

Lieutenant General FOGARTY. There are restrictions hampering the Army's ability to hire more civilians within the cyber workforce. First is the time requirement to acquire a Top Secret (TS), Sensitive Compartmentalized Information (SCI), Counterintelligence (CI) Polygraph (Poly) security clearance. Cyber professionals are required to obtain and maintain a TS, SCI, Poly which could potentially take over one year to obtain. There may also be an additional security vetting requirement if the place of employment is located with the National Security Agency (NSA) teams/workspace which may take an additional six months for adjudication. The security requirements add significantly to the timeliness of hiring and on-boarding a civilian employee, which may dissuade applicants from applying and following through for these types of positions. However, we are addressing this setback by authorizing civilian new hires to train and work on unclassified mission sets until such time as the security clearance vetting process is complete. Second is the salary rate of cyber professionals working in the private sector compared to that of DA civilians. Private industry can offer significantly higher salaries, stock/share options, bonuses and financial incentives, loan incentives, various types of paid leave packets, daily meals, campus transportation, medical, dental, and child care on work-site as well as an environment that's conducive and attractive to cyber professionals. While dollar for dollar, the salaries are incomparable, the Army can offer a wide range of compensation and incentives that include recruitment, retention, and relocation incentives, student loan incentives, accelerated salary incentives, additional leave incentives, paid federal holidays, paid sick leave, Thrift Savings Plan match incentives, Permanent Change of Station (relocation) benefits and entitlements, coupled with the standard DA civilian compensation packet to include a defined benefit plan (pension) not normally offered in the private sector, plus the stability of the Government workforce. Currently, however, when DA Civilian compensation packages are compared to that of private industry, the Army's inability to offer a comparable industry salary may limit future recruiting and retention efforts of cyber operators.

18. Senator GILLIBRAND. Lieutenant General Stewart, Lieutenant General Fogarty, and Brigadier General Crall, do you believe that existing personnel authorities for military and civilian personnel are adequate to build the cyber force to meet identified requirements?

Lieutenant General STEWART. [Deleted.]

Lieutenant General FOGARTY. A holistic DOD strategy to building a cohesive cyber workforce that includes the current authorities and an industry level compensation program, for both military and civilians, would reduce the retention and recruitment challenges and help stabilize the current highly skilled cyber workforce while building the future identified requirements. The 37 U.S. Code § 353 limits skill incentive pay to $1,000 per month, and proficiency bonuses to $12,000 per year for qualified cyber soldiers. While adequate for most military career fields, these monetary incentives may not be competitive or commensurate with that of other government agencies and private industry in order to retain our highly skilled talent. Amending the law to enable payments up to $5000 per month for skill incentive

pay, and $60,000 per year for proficiency bonuses, provides additional incentives close the compensation disparity between private and military/government sectors. Furthermore, this would enable the services to establish a Cyber Proficiency Pay/Bonus scale similar to that of the Medical and Legal Corps. Furthermore, increased incentive may aid in the retention of the Army's highly skilled, cyber professionals, who are routinely recruited by other government agencies and private industry based upon their extensive training, knowledge, skills and abilities, within key work-rolls. For DA civilians, the current Direct Hiring Authorities (DHA) are adequate. However, the variations between multiple DHAs may hamper the Army's ability to build a cyber civilian workforce. Specifically, streamlined and flexible hiring process would be beneficial to Army Cyber.

Brigadier General CRALL. I support the responses from my fellow witnesses, Lieutenant General Stewart and Lieutenant General Fogarty, on this specific question regarding personnel authorities for military and civilian personnel.