Stenographic Transcript
Before the

Subcommittee on Cybersecurity

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

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

Wednesday, September 26, 2018

Washington, D.C.

ALDERSON COURT REPORTING
2020 K STREET NW
SUITE 700
WASHINGTON, D.C. 20006
(202) 289-2260
www.aldersonreporting.com

JOINT HEARING TO RECEIVE TESTIMONY ON

THE CYBER OPERATIONAL READINESS OF THE DEPARTMENT OF DEFENSE

(OPEN SESSION)

Wednesday, September 26, 2018

U.S. Senate

Subcommittee on Cybersecurity

Subcommittee on Personnel

Committee on Armed Services

Washington, D.C.

The subcommittees met, pursuant to notice, at 2:43 p.m. in Room SD-106, Dirksen Senate Office Building, Hon. Mike Rounds, chairman of the Subcommittee on Cybersecurity, and Hon. Thom Tillis, chairman of the Subcommittee on Personnel, presiding.

Members Present: Senators Rounds and Tillis [presiding], Wicker, Fischer, Nelson, Gillibrand, McCaskill, and Warren.

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

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 Presidential 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 Forces achieving full operational capability in May, the Department 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. And 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, and the CIO 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, 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 defense and national missions, but also for those conducted in support of the combatant commands. I am eager to hear about CYBERCOM's current capability and activity to assist EUCOM's, PACOM's, and CENTCOM's 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 cyber policy shapes, and is shaped by, the capabilities offered 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 its cyber teams. And 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 HON. THOM TILLIS, U.S. SENATOR FROM NORTH CAROLINA

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. And 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 HON. BILL NELSON, U.S. SENATOR FROM FLORIDA

Senator Nelson: In the interest of time, I'll submit it for the record, but 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? And how are we retaining them and managing their careers?

Thanks.

[The prepared statement of Senator Nelson follows:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Senator Gillibrand.

STATEMENT OF HON. KIRSTEN E. GILLIBRAND, U.S. SENATOR FROM NEW YORK

Senator Gillibrand: I will also submit my statement for the record.

[The prepared statement of Senator Gillibrand follows:]

[SUBCOMMITTEE INSERT]

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

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. And 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 '16, and the rollout of that started in '17. And 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. And 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.

And 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. And you've asked us to do that. And 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. And 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. And that coding

effort is largely complete. Goes a long way to making sure that we can develop.

And 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. And 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. And 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 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. And, 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. And, 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. And, 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.

And 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:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Thank you.

And 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 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:]

Senator Rounds: Thank you.

General Stewart.

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

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. And so, 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. And 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. And 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 FY19 NDAA 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:]

Senator Rounds: Thank you, General.

General Fogarty.

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

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, 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 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. And, 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. And in a 6-year enlistment, you get about 3, maybe 3 and a half 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 have already achieved initial operational capabilities. And the Army National Guard is scheduled to have all 11 CPTs at full operational capability by fiscal year '22. In the Army Reserves, 10 CPTs will be fully operational-capable by FY24, trained and equipped to the same standards as the Active component. I'll discuss PCT 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. And

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. And 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. And 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:]

[SUBCOMMITTEE INSERT]

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 the, as they would call, 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, or CMF, 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?

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. And 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. And 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 --

General Fogarty: -- per year.

Senator Rounds: -- you don't quite have it straight yet, so what is that doing to your operational timelines today?

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 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:]

[SUBCOMMITTEE INSERT]

Senator Rounds: And, 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:]

[SUBCOMMITTEE INSERT]

Senator Rounds: Thank you.

With that, Senator Tillis.

Senator Tillis: Thank you, Mr. Chair.

And again, thank you all for being here.

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

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

Ms. Miller: Yes, sir, along with --

Senator Tillis: And P&R 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: And 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. And, you know, some -- 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. And 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.

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.

General Stewart: So, for the training component, the Army will take that persistent common training environment. And 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 --

General Stewart: So, we're moving in that --

Senator Tillis: Okay.

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 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.

And, 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. And we'll discuss those in the -- we'll discuss those in the hearing or in meetings that we'll have in my office.

And, 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 Forces to execute their mission?

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 either trained to a certain level or not. And, 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?

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?

General Stewart: We've now mandated or laid out the requirements for 1,000-2,000 level. That's the basic entry-level training. And 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. And, 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 IONs, for instance, we have to now define whether or not we have the right number of IONs 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 IONs, 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. And 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?

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 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. And 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?

General Fogarty: Senator, that's actually a succinct way of saying that, but we're --

Senator Nelson: Okay.

General Fogarty: -- we're not there yet --

Senator Nelson: Let me --

General Fogarty: -- for sure.

Senator Nelson: Let me ask General Crall. Cyber Command, created in '09, but it wasn't until '13 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?

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?

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 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. And 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.

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

Senator Gillibrand: Correct.

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.

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. And 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 programs or direct accession programs for skilled doctors and lawyers have undoubtedly played a key role in recruiting talented individuals 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?

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.

And thank you, to our witnesses, for being here today.

Talent management is a critical component of the ability to maintain cyber readiness. And 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?

General Crall: Yes, ma'am, I can. And 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. And 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. And 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 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. And 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.

General Crall: Yes, ma'am. This is an exciting question, because you're --

Senator Warren: Good.

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. And, 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.

[Recess until 4:00 p.m.]