

**THE CURRENT AND FUTURE CYBER WORKFORCE
IN THE DEPARTMENT OF DEFENSE AND THE
MILITARY SERVICES**

HEARING
BEFORE THE
SUBCOMMITTEE ON
PERSONNEL
OF THE
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

APRIL 21, 2021

Printed for the use of the Committee on Armed Services



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

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

COMMITTEE ON ARMED SERVICES

JACK REED, Rhode Island, *Chairman*

JEANNE SHAHEEN, New Hampshire	JAMES M. INHOFE, Oklahoma
KIRSTEN E. GILLIBRAND, New York	ROGER F. WICKER, Mississippi
RICHARD BLUMENTHAL, Connecticut	DEB FISCHER, Nebraska
MAZIE K. HIRONO, Hawaii	TOM COTTON, Arkansas
TIM Kaine, Virginia	MIKE ROUNDS, South Dakota
ANGUS S. KING, Jr., Maine	JONI ERNST, Iowa
ELIZABETH WARREN, Massachusetts	THOM TILLIS, North Carolina
GARY C. PETERS, Michigan	DAN SULLIVAN, Alaska
JOE MANCHIN III, West Virginia	KEVIN CRAMER, North Dakota
TAMMY DUCKWORTH, Illinois	RICK SCOTT, Florida
JACKY ROSEN, Nevada	MARSHA BLACKBURN, Tennessee
MARK KELLY, Arizona	JOSH HAWLEY, Missouri
	TOMMY TUBERVILLE, Alabama

ELIZABETH L. KING, *Staff Director*
JOHN D. WASON, *Minority Staff Director*

SUBCOMMITTEE ON PERSONNEL

KIRSTEN E. GILLIBRAND, New York, *Chair*

MAZIE K. HIRONO, Hawaii	THOM TILLIS, North Carolina
ELIZABETH WARREN, Massachusetts	JOSH HAWLEY, Missouri
	TOMMY TUBERVILLE, Alabama

CONTENTS

APRIL 21, 2021

	Page
THE CURRENT AND FUTURE CYBER WORKFORCE IN THE DEPARTMENT OF DEFENSE AND THE MILITARY SERVICES	1
MEMBER STATEMENTS	
Statement of Senator Kirsten Gillibrand	1
Statement of Senator Senator Thom Tillis	9
WITNESS STATEMENTS	
Litton, Leonard G., III, Acting Deputy Assistant Secretary for Defense for Military Personnel Policy	2
Sherman, John, Acting Department of Defense Chief Information Officer	4
Hinton, Veronica E., Acting Deputy Assistant Secretary for Defense for Civilian Personnel Policy	10
Crall, Lieutenant General Dennis A., USMC, Director, Command, Control Communications and Computers/Cyber and Chief Information Officer, Joint Staff, J6	16

**THE CURRENT AND FUTURE CYBER WORK-
FORCE IN THE DEPARTMENT OF DEFENSE
AND THE MILITARY SERVICES**

WEDNESDAY, APRIL 21, 2021

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

The Committee met, pursuant to notice, at 2:30 p.m. in room SR-232A, Russell Senate Office Building, Senator Kirsten Gillibrand (Chairman of the Subcommittee) presiding.

Committee Members present: Gillibrand, Hirono, Tillis, and Hawley.

OPENING STATEMENT OF SENATOR KIRSTEN GILLIBRAND

Senator GILLIBRAND. Good afternoon, everybody. The subcommittee meets today to receive testimony on the current and future cyber workforce requirements of the Department of Defense and Military Services. Our witnesses include Mr. John Sherman, Acting Department of Defense Chief Information Officer; Ms. Veronica Hinton, Acting Deputy Assistant Secretary for Defense for Civilian Personnel Policy; Mr. Leonard Litton, acting Deputy Assistant Secretary for Defense for Military Personnel Policy; and Lieutenant General Dennis Crall, Director, Command, Control Communications and Computers/Cyber and Chief Information Officer, Joint Staff, J6. Welcome. Thank you.

In March, General Nakasone testified to the full committee that USCYBERCOM conducted two dozen operations to counter foreign threats to the 2020 election, and threats that followed on the heels of Russia's tampering with the 2016 election. In December, we learned that foreign hackers had penetrated software widely used by the U.S. Government the private sector and went undetected for months, exposing thousands of public and private networks to exploitation.

This election interference and SolarWinds hack recently prompted President Biden to issue a new round of sanctions against Russia. But make no mistake about it—Russia is not our only adversary. Cyber intrusions and attacks from all quarters will only increase moving forward, and it is our responsibility to ensure that we have the capability to defend the United States on this new front. The need for an effective, talented, and diverse cyber workforce within the Department of Defense (DOD), the Military Serv-

ices, and really across the whole of government has never been clearer.

Growing and maintaining a cyber capability sufficient to prevent these attacks and to meet national defense objectives starts with the people behind the keyboard. Our ability to field the world's strongest military has always come from the collective talent and dedication of our servicemembers and the civilian workforce who support them. We must recognize and commit to meeting these new threats by developing, fielding, and maintaining the world's most capable cyber force.

That brings us to the topic we will discuss today. In short, how do we recruit and retain the very best for civilian and military service in the cyber workforce? How do we attract top talent, hire them, pay them, manage them, and keep them? How do we keep their skills fresh and provide meaningful career progression and professional development to ensure we have a cyber workforce for the defensive capability to protect the nation's networks and the offensive capability to deter aggression, not just by traditional cyber adversaries like China and Russia, but also by the likes of Iran, North Korea, non-state actors, and criminal cartels. What is the proper role for the reserve component, especially the National Guard? What are the personnel policy implications of sustainable and effective management with the private sector?

I am especially interested in our witnesses' views on the proper civilian-military mix for the cyber workforce of tomorrow, how we set the course to achieve that mix, and how we ensure that our cyber workforce possesses the very best talent America has to offer.

Lastly, I want to know why the Department of Defense has been slow to implement some of the authorities it already has to hire and retain the best cyber personnel, such as the ability to directly hire cyber personnel we enacted in Section 502 in fiscal year 2019 NDAA.

I am also interested in the status of the authorities Congress passed in last year's NDAA regarding Cyber Reserve, Cyber Mission Force, and the National Guard Cyber Workforce. Have these and other previous authorities to attract and retain the best cyber personnel resulted in the expansion and improvements necessary for the DOD to detect and defeat the cyber intrusions and attacks we are now facing? A

Again, I am so grateful to our witnesses here today. I welcome them all and appreciate hearing your testimony.

What we will do is we will take your testimony now, but when Senator Tillis returns we will pause in your testimony so he can give his opening remarks, I will run and go vote, and then I will come back, and you can continue your testimony. But we will not postpone the hearing for the vote. We will just keep it running.

Our first witness, Mr. Litton, would you like to go first?

STATEMENT OF LEONARD G. LITTON III, ACTING DEPUTY ASSISTANT SECRETARY FOR DEFENSE FOR MILITARY PERSONNEL POLICY

Mr. LITTON. Yes, ma'am. Thank you. Chairwoman Gillibrand and distinguished members, thank you for the opportunity to appear

before you to today to discuss the health of the DOD cyber workforce. I appreciate your support on this very important issue.

My role in performing the duties of the Deputy Assistant Secretary for Military Personnel Policy is primarily an enabling one, so I will speak to the overarching military personnel policies that support the Services and enable them to access, support, and attain and retain a highly ready force.

The Department does desire to be the employer of choice, not only for individuals with cyber-related skills but for all Americans who are looking and working hard every day to join the military. Enabling our cyber forces to operate and defend against today's threats will require us to maintain the authorities and resources we have now, but also ensure that our warriors are properly assessed, compensated, and retained to fight and win against these threats.

As you know, ma'am, the Military Services conduct a whole-person assessment of each candidate who applies for either an officer commissioning or the enlisted force. This holistic process looks at a number of factors, including citizenship, age, education, physical fitness, conduct, and aptitude. The general model is to recruit and assess a qualified field of applicants, placing them in a best-fit occupational specialty and career trajectory, and provide them the necessary technical training to meet those operational objectives. This process provides a steady pipeline of highly qualified personnel for the required tasks.

The Military Services can also employ an accession option known as "lateral entry." This process allows the active and reserve components to recruit highly qualified individuals directly from industry to fill those critical requirements and bring them in at advanced grades, based on their previous level of education and experience.

The Military Service Academies and Reserve Officer Training Corps also have programs focused on attracting young, talented officers into the cyber fields.

For enlisted accessions, the Services utilize an array of assessments designed to understand the technical training, including cyber. For example, in enlisted cyber specialties, the Services utilize a combination of the Armed Services Vocational Aptitude Battery (ASVAB) and a targeted cyber knowledge test, called the Cyber Test, to identify applicants with specific aptitude for cyber career field accessions.

Additionally, we continuously evaluate new types of assessments, for example, a fluid intelligence test called "Complex Reasoning" was recently developed, and we hope to have that ready in the 2024 time frame to help us better attract and identify cyber capabilities among those who apply.

The Department realizes that military members with cyber experience are in great demand and can command top salaries within the private sector. In addition, we have a robust military compensation package and a toolkit of bonuses and incentives and special pays designed to attract and retain these servicemembers with cyber skills.

We have the authority for enlistment bonuses, and we thank you for that, up to \$50,000 for those who agree to serve at least 2 years

in a specified career field, as well as retention bonuses up to \$30,000 per year of service obligation. The Services also have the authority to offer other monetary and non-monetary incentives for service in certain cyber-related occupational specialties. Non-monetary incentives may include choice of duty assignment, guaranteed training, advanced education, and other professional development opportunities. Additional monetary incentives include the authority for assignment incentives and special duty pays that can be as much as \$5,000 per month.

The Department prides itself on building a strong and viable total force that delivers combat capability around the globe. Our cyber personnel are and will remain a critical component of the Department's ability to defend the nation.

I look forward to your questions. Thank you.

[The joint prepared statement of Ms. Hinton and Mr. Litton proceeds Ms. Hinton's statement.]

Senator GILLIBRAND. Thank you. Mr. Sherman?

**STATEMENT OF JOHN SHERMAN, ACTING DEPARTMENT OF
DEFENSE CHIEF INFORMATION OFFICER**

Mr. SHERMAN. Ma'am, good afternoon, and thank you for the opportunity to testify today regarding the efforts of the Department of Defense to enhance the cyber workforce across our enterprise.

My name is John Sherman. I am the Acting Department of Defense Chief Information Officer, a position I have held since 20 January. I work alongside my colleagues to establish policy and provide oversight, direction, and guidance for the cyber workforce. We have come far in focusing our efforts to be proactive, agile, and competitive in order to recruit and retain the most innovative individuals with high-demand skill sets while also encouraging increased representation of minorities and women.

I would like to highlight how my office is developing the cyber workforce through new policies and governance, using my existing oversight. I will speak to how we are leveraging special hiring authorities granted to us by Congress and how we are recruiting from a diverse pool of candidates.

However, there is still work to be done. We have put many of the key foundational mechanisms in place and have actively leveraged the tools at our disposal, but we must build on the progress by updating our overarching strategy to ensure our workforce is prepared to implement zero trust and the other latest approaches to defending our enterprise.

Our existing cyber strategy from 2018 provides some key points on the cyber workforce, but we need a more holistic North Star to guide our future cyber workforce efforts. I have given my office direction that drafting and coordinating this new strategy is a priority going forward.

Our DOD cyber workforce is comprised of individuals including military, civilian, and contractor personnel. Our goal has been to refine and hone this critical workforce, but we first had to define its composition and ensure we had a solid workforce management structure.

To do this, we created and implemented the DOD's Cyber Workforce Framework, which has enabled my office to establish a stand-

ard lexicon to describe the scope of work in the cyber field. We then identified and analyzed cyber work roles with greater specificity in order to inform workforce priorities and initiatives beyond the legacy occupational descriptions, which are too broad in many cases.

To fully realize the potential of this framework, we are developing a new policy series called 8140, which will drive implementation and compliance of our vision. In 2015, Department leadership signed the associated DOD directive and then updated it late last year. The instruction and manual for this policy series are in the final stages of coordination, and we are working with Department stakeholders to get these over the goal line in the coming months, if not sooner.

Additionally, we established a tri-chaired form called the Cyber Workforce Management Board to govern and oversee implementation of the activities in the policy series with representation from my office, the Under Secretary for Personnel and Readiness, and the Principal Cyber Advisor. We recognize this whole-of-department challenge and our approach must match.

Very importantly, we have leveraged the Cyber Excepted Services, or CES, personnel system to meet more quickly the immediate need of the Department. We now have over 9,000 positions designed for CES across 10 DOD components, and we plan to increase this number even more later this year as Army Cyber comes into the fold. Moreover, we are taking lessons learned on workforce feedback related to their decisions on moving into the CES to inform ways we can socialize this great opportunity even more effectively in the future.

Meanwhile, we are also conducting the congressionally directed zero-based review of cybersecurity personnel. Once complete, the zero based review (ZBR) will provide us with the input to conduct data-driven analysis of our current and future workforce needs. We are aiming to complete the initial phase of data-gathering by September, and look forward to updating the committee later this year, as directed in legislation.

While we have improved our ability to identify and develop the cyber workforce in the past 3 years, I recognize we still have work to do, especially as we move out on zero trust. This is an approach based on extensive network segmentation and protection of the data in the systems, with an assumption that adversaries have already breached the perimeter at some point. For this and other evolving cyber strategies, we can expect to draw an even wider range of skill sets in areas like data and artificial intelligence.

I am confident that our workforce, now and in the future, is up to the challenge, and am proud of their ongoing work to build, secure, operate, defend, conduct intelligence activities, and enable operations through cyberspace. We realize that it is an ever-changing space. However, our continual workforce updates and upskilling will be critical. Our adversaries are definitely not standing still, and we must not either.

Finally, I am committed to continue our efforts to reach out to all of this nation's human capital through an ongoing focus of the National Security Agency's Cyber Scholarship Program and Centers of Academic Excellence accreditation.

Thank you for the opportunity to speak with you today, and I am grateful for the attention you have dedicated to Secretary Austin's top three priorities on taking care of our people. I stand ready to answer questions.

[The prepared statement of Mr. Sherman follows:]

PREPARED STATEMENT BY JOHN SHERMAN

INTRODUCTION

Good afternoon Chairwoman Gillibrand, Ranking Member Tillis, and other members of the Committee. Thank you for the opportunity to speak with you today on our most valuable resource to our national security: our workforce. In order to continue to lead the way in cyberspace, we must continue to modernize our approach to recruit and maintain talent.

In the modern cyber environment, the race to recruit and retain the most innovative individuals with high-demand skillsets is a top priority for government and industry leaders alike. Emerging cyber talent are faced with an abundance of employment opportunities across the private sector where lucrative incentives are available to those with high-demand skillsets.

To maintain a viable cyber-talent pipeline, the DOD CIO is focused on a strategy that attracts high-demand skillsets while encouraging increased representation of minorities and women. Additionally, the strategy recognizes that prospective candidates tend to have a preference to have many diverse jobs over the span of a career and seek the flexibility to move between industry and the DOD untethered by unnecessary barriers. The strategy is built around the DOD Cyber Workforce Framework and an associated policy series (8140), which is used to govern the workforce and define the work roles necessary to achieve success in the cyber domain and information environment. We are also working to recruit, train, develop, and retain the best and most diverse talent through the Cyber Excepted Service personnel system, the Cyber Scholarship Program, and the creation of a platform that helps better match a job opportunity with a candidate.

DEFINING THE WORKFORCE

The DOD cyber workforce is comprised of individuals including military, civilian, and contractor personnel. The Department is implementing policies and procedures to synchronize the management of cyber talent across each of these populations, and across the various mission sets required to establish and maintain a competitive advantage in the cyberspace domain. The DOD has developed targeted approaches to identify critical skill gaps and, subsequently, recruit, retain, and develop cyber professionals in an agile manner. As we move through this discussion, you will see that the DOD Cyber Workforce Framework, or DCWF, is central to DOD's approach for cyber talent.

The DCWF establishes a standard lexicon to describe the work of DOD personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations in and through cyberspace; and project power in or through cyberspace. We developed the DCWF by incorporating content from both the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework and the Department's Joint Cyberspace Training and Certification Standards (JCT&CS) to enhance communication and coordination with our partners across government, industry and academia, while maintaining a mission focus. Notably, the DCWF provides the foundation for a broad range of cyber workforce management activities across the DOD enterprise.

This Framework contains 54 'work roles' covering the full spectrum of cyber skill sets required for the conduct and support of missions within the cyberspace domain. As a result, the DCWF enables the Department to understand specific and varied cyber skill requirements, and to drive cyber work in a targeted manner independent of historical occupational structures that are too generic or rigid to properly support our cyber workforce. Specifically, we are using the DCWF to conduct targeted identification and analyses of the DOD cyber workforce and, subsequently, inform workforce priorities and initiatives. Similarly, the DCWF enables us to identify the work roles of critical need and develop the mitigation strategies for identified gaps in both staffing levels and workforce development activities. Additionally, and very importantly, we are leveraging the DCWF to inform for targeted recruitment under Cyber Excepted Service, as well as comprehensive qualification and management activities as defined under a DOD policy series that guide this activity (8140).

To keep pace with advancements in technology, tactics, techniques and procedures within this arena, we designed the DCWF to be updated periodically. This approach provides us with a more responsive mechanism, as compared to traditional government occupations and human resources practices, whereby we can ensure workforce specifications are based in current standards. In fact, we are currently engaged in refresh activities, which are (in part) focused on expansion of the DCWF to include related emerging technologies such as control systems security, advanced data analysis, software development, artificial intelligence (AI) and machine learning. The Framework allows the Department to be agile in its approach to the cyber workforce, as it is able to include new emerging technologies under a common umbrella to meet the mission needs of our operational stakeholders.

DEVELOPING THE WORKFORCE ...

... THROUGH NEW POLICIES

To facilitate strategic cyber workforce management activities, we are developing the 8140 policy series, which will drive implementation of our vision for a robust and trained workforce necessary to meet our current and future cyber challenges. These policies accomplish this goal by providing a targeted, role-based approach to identify, develop and qualify cyber personnel leveraging the DCWF. This series includes three components:

- 1) *The DOD 8140 Directive*, first signed in 2015 and recently updated in late 2020, establishes the DCWF as the Department's primary mechanism for cyber human capital and talent management at the Enterprise level. It unifies the cyber workforce according to cyber workforce elements (i.e., IT, Cybersecurity, Cyber Effects, Cyber Intelligence, and Cyber Enablers) and defines the roles and responsibilities across the DOD enterprise.
- 2) *The DOD 8140 Instruction*, which is currently in Legal Sufficiency Review (a final stage of coordination), will establish the procedures for the identification, tracking and reporting of cyber workforce requirements. Specifically, every DOD position requiring the performance of cyber work will be required to be coded with the appropriate DCWF work role. The Instruction also requires the reporting of vacancy information and key position designators which will allow the Department to engage in strategic workforce planning activities.
- 3) *The 8140 Manual*, which is also in final coordination, will establish enterprise-baseline qualifications program for the DOD cyber workforce and encourage the responsible DOD Component or Command to augment the baseline standards with environment-specific requirements based on specific technology and known threat vectors. This policy will provide the DOD with flexibility needed across varied cyber mission sets, while moving away from a legacy compliance-based approach to focus on demonstration of capability.

... THROUGH GOVERNANCE AND OVERSIGHT

To govern and oversee implementation of the activities specified in the policy series, we have established the Cyber Workforce Management Board (CWMB) to provide executive level oversight over the implementation of the DCWF and the human capital and management policies described in the 8140 policy series. This forum is tri-chaired by representatives from my office, the Undersecretary of Defense for Personnel and Readiness (USD (P&R)), and the Principal Cyber Advisor. The CWMB Charter also includes other aspects of management across the functional communities that comprise our cyber workforce, to include coordination and communication of recruitment and retention activities, identification and management of hiring authorities, and implementation of the Cyber Excepted Service Personnel System.

... BY LEVERAGING SPECIAL HIRING AUTHORITIES

The Department faces a range of challenges centered on Talent Management of the Cyberspace workforce. Employing the authority to establish the Cyber Excepted Service (CES) via Section 1599f of title 10, U.S.C. addresses these challenges head-on. Working together DOD CIO and USD (P&R) have focused on tools for The CES which currently applies to ~9,000 identified positions covered under CES with 6,500 who have been converted or appointed for (1) classification and recruitment and (2) pay setting/compensation flexibilities with the capability to expand beyond the current CES workforce.

- (1) Classification and Recruitment: The ability to recruit top-tier talent starts with changing how organizations and HR professionals source job opportunities and reducing the amount of time it takes to hire talent. In order to recruit the sort of diverse and sought-after cyber talent we need here at DOD, we've

found that we need to leverage alternate talent resources outside of USAJobs (i.e., virtual job fairs, organization-specific job announcement websites, and on the spot job offers) to hire and onboard cyber candidates, as well as leverage the flexibilities afforded in the CES Personnel System. Starting in fiscal year 2021, we in DOD CIO provided access for CES organizations to leverage the DOD Emerging Technologies Talent Marketplace, AI platform that contains a broad Federal Occupational Database with job/position classification standards and DCWF work role codes. The expedited position classification streamlines the recruitment process. Additionally, the platform serves as an open talent marketplace with a Candidate-Centric design, focusing on the needs, objectives, and Point of View (POV), for long-term relationship building.

It also means relying less on traditional measures, like the length of experience, in favor of matching candidate competencies and skills to positions in the organization holistically. This candidate-centric approach allows non-traditional sources of talent (ex: self-taught technologist) to gain access to jobs and that, in turn, expands diversity as well as employee engagement by targeting non-traditional sources (reference artifact) of talent.

- (2) Pay Setting/Compensation Flexibilities: Hiring, training, and developing a highly-skilled workforce will remain a constant struggle without equal importance being placed on retaining a qualified workforce. To address this, in January 2021, the DOD CIO working through USD(P&R), deployed a CES Targeted Local Market Supplement (TLMS) applicable to seven mission-critical DCWF work roles. The TLMS is designed to reduce attrition of critical civilian employee segments, as well as, attract, engage, and retain high-potential cyber talent.

... AND THROUGH EDUCATIONAL OPPORTUNITIES

The DOD Cyber Scholarship Program (CySP) is a useful tool to enhance the skills of our workforce, as well as to offer opportunities to new and more diverse entrants to our team. This program is a result of commitment from DOD and Congress to support higher education as a means to prepare the DOD workforce to deal with threats against the Department's critical information system and networks. It is authorized by Chapter 112 of U.S.C., Section 2200, designed to encourage the recruitment of the nation's top cyber talent and the retention of DOD personnel who have skills necessary to meet DOD's cyber requirements. It provides scholarships to students in pursuit of cyber-related degree at National Centers of Academic Excellence in Cybersecurity (NCAE-C), Cyber Defense Research (CAE-R) or Cyber Operations (CAE-CO).

There is an additional option for NCAE-C's to apply for modest institutional capacity building. DOD CIO will outline the projects for each application cycle in the annual solicitation. The projects may be tied to two specific DOD-focused initiatives: DOD Partnerships and Outreach to K-12, Minority-Serving Institutions, Community Colleges; and technical schools.

LOOKING AHEAD TO THE FUTURE

While we have improved our ability to identify and develop the cyber workforce over the past three years, we still have work to do with regards to other high-tech skillsets. As noted earlier, we are pushing forward an expansion of the DCWF to include related emerging technologies such as control systems security, advanced data analysis, software development, AI, and machine learning. Additionally, we are working to make the current DOD Talent Marketplace platform operational so that it can be used to recruit the entire emerging technologies workforce. Unlike traditional Federal hiring platforms The "Talent Marketplace" platform enables an understanding of each candidate's unique preferences to enable a "Smart Match" of candidates to the jobs that align with their needs and desires. Content is regularly pushed to candidates to keep them abreast of new opportunities and new developments. Digital personalization is made possible by artificial intelligence and data analytics algorithms to allow for a scalable process that is, at the same time, very engaging.

Meanwhile, as directed by the Fiscal Year 2020 National Defense Authorization Act (NDAA), we are conducting a zero-based review (ZBR) following a phased approach using representative organizations for each Military Service/Component and the 4th Estate to review Civilian and Military workforce positions in Cyber Security and Cyber IT functional areas for the workforce. Every Component will conduct a ZBR and submit reports to the Tri-Chair (which includes DOD CIO, PCA, and USD (P&R)) by December 2021; the Tri-Chair will then brief Congress and recommend changes by June 2022.

To date, the ZBR has provided us with a useful metric to demonstrate the effectiveness of the DCWF and the forthcoming 8140 policy series. We plan to use the findings of the current ZBR effort to inform our decisions regarding the direction of the workforce and related workforce management activities. Furthermore, a process is being established as part of the ZBR NDAA 1652 requirement. The CWMB established an initial plan, put in the individual steps and lessons learned during Phase 1 (Singular pilot organization) and are currently testing and refining the process with the remaining organizations during Phase 2. Once completed it will be an official process in the form of a ZBR "How to Guide", used to repeat the evaluation of other functional areas of the cyber workforce, be used on any size effort at multiple echelons; positioning the Services and Components to proactively assess their current workforce state across all cyber functional areas; enabling the development of well-justified plans for the future that ensures alignment to the Department's strategic priorities.

Thank you for the opportunity to address the committee today and for your continued partnership. We would also like to take this opportunity to thank our dedicated and talented workforce who work every day to defend our Warfighters against our adversaries in cyberspace. These professionals are our frontline in an unending battle, and we owe our continued ability to accomplish our mission to their steadfast determination and expertise.

Senator GILLIBRAND. Now I would like to introduce Senator Tillis for his opening remarks. I will run and go vote, and then when you are completed you can call on Ms. Hinton and then Lieutenant General Crall, and I will be back ASAP.

STATEMENT OF SENATOR THOM TILLIS

Senator TILLIS. Thank you, Madam Chair, and thank you all for being here today. I am sorry I was late. We are doing the tag team for voting.

I just want to say the success in the cyber domain is uniquely reliant on highly skilled personnel. We all know that. We have had several discussions and meetings about it. Where stealth technology and smart weapons provide the United States with a discernable advantage in traditional warfighting domains, the U.S. military does enjoy a similar technological advance when it comes to cyberspace. Rather, we must rely on the intelligence, creativity, and cunning of our people if we are to be successful with this rapidly changing environment.

Fortunately, this country still produces the world's most innovative cyber talent. The Department of Defense's challenge is to make itself appealing to that talent. Since success in cyberspace is so heavily dependent on skilled people, the last several NDAs included numerous provisions focused on military and DOD civilian workforce.

I look forward to asking questions about the creative recruiting and retention ideas, some of the authorities we have given, whether or not they have been fully implemented, and what more authorities and creative thinking we should consider to be absolutely certain we are bringing the best and brightest into the cyber domain within the Department of Defense.

So thank you all for being here. We will continue the introductions. Ms. Hinton?

STATEMENT OF VERONICA E. HINTON, ACTING DEPUTY ASSISTANT SECRETARY FOR DEFENSE FOR CIVILIAN PERSONNEL POLICY

Ms. HINTON. Ranking Member Tillis, thank you for the opportunity to appear at today's hearing to discuss the health and readiness of the DOD's cyber workforce.

Today, as the Acting Deputy Assistant Secretary of Defense for Civilian Personnel Policy, I am representing the Office of the Under Secretary of Defense for Personnel and Readiness, the Department's chief human capital officer, to discuss matters related to the civilian cyber workforce.

Important to this discussion is the acknowledgement that we live in a relentlessly evolving and fiercely competitive world where technological achievements are driving immense change across political, economic, and social landscapes. As such, the Department strives to cultivate a technologically dominant force that is strategically ready, globally relevant, and flexibly sustainable. Competition for high-quality, experienced cyber workforce personnel is constant and increasingly aggressive. However, the Department shares your vision and commitment to pursuing, recruiting and retaining world-class cyber talent to advance and achieve the DOD's unique mission.

DOD is one of the three largest markets for cyber talent in the United States due to its size, its continuous adoption and adaptation of technology, and its extensive mission requirements. Therefore, we must be tenacious in not only fully utilizing the appointment and compensation flexibilities that Congress has provided but must increasingly invest in human capital initiatives, training and development for the civilian cyber workforce. This focus includes designing and implementing programs and policies that eliminate any barriers and inefficiencies that may detract from our ability to acquire needed and diversified talent, expand pathways to service, and enable a flexible workplace essential to the future of work.

Additionally, we are expanding our outreach, including with the private sector, to recruit top talent from across all segments of society, while retaining and compensating current technical talent and closing mission-critical gaps.

To assess our progress, the Department has established capability to identify, evaluate, and manage the civilian cyber workforce, and is also leaning forward utilizing advanced data analytics and technological tools to better match potential candidates and current employees against talent and competency gaps in various locations across the globe, proving real-time solutions to organizational needs. We are working closely with industry experts in the cyber community to build hiring assessments that will better match top talent to specific competency and skills needs, reducing time to hire, and equipping hiring managers with the best talent.

In recent years, Congress has provided several DOD-exclusive civilian hiring authorities that are helping to meet our objectives. In particular, Section 1109 of the National Defense Authorization Act of fiscal year 2020 granted streamlined and enhanced direct hire authorities, including an expanded direct hire authority for cyber workforce positions. The expansion of this coverage has been bene-

ficial in that it has allowed the Department the ability to directly hire for any and all critical cyber skill sets.

The Department is also utilizing a variety of compensation tools, including the use of Federal-wide special salary rates and the added flexibility of the cyber-accepted service that allows the Department to implement targeted local market supplements for certain cyber occupations and locations. The Department appreciate such authorities which expand our toolkit, and are much needed to attract and retain the best talent and compete with the private sector for the same skill sets.

The Department further acknowledges that civilian personnel policies should be as clear and concise as possible. We are committed to ensuring that we are training and assisting human resource professionals and managers alike in the use of cyber personnel management authorities and flexibilities. This not only includes streamlined and efficient guidance on the use of the authorities and implementation procedures, but also gathering and analyzing data to better equip practitioners with the necessary information to proactively address emerging requirements.

The Office of Personnel and Readiness continues to ensure that information disseminated across the Department encompasses the full spectrum of hiring options that enable hiring managers to reach the right talent, at the right time.

We thank you for your continued interest and support of the DOD civilian workforce. I look forward to your questions.

[The joint prepared statement of Ms. Hinton and Mr. Litton follows:]

JOINT PREPARED STATEMENT BY MS. VERONICA HINTON AND MR. LEONARD LITTON

Chairwoman Gillibrand, Ranking Member Tillis, and distinguished members of the subcommittee, thank you for the opportunity to appear before you today to discuss the role of the Office of the Undersecretary of Defense for Personnel and Readiness (OUSD(P&R)) in supporting and maintaining the health of the Department of Defense (DOD or Department) cyber workforce.

The Department is committed to pursuing, recruiting, and retaining world-class cyber talent, enhancing and improving the lifecycle management of the cyber workforce, and modernizing personnel policies and programs which best support the cyber critical functions and personnel needed to advance and achieve the DOD's unique mission. We recognize that in order to defeat our adversaries, now and into the future, we must keep pace with the dynamic security environment and ensure that our policies and procedures are rapidly adapted to equip our workforce with the tools needed to address emergent national security cyber requirements.

The DOD cyber workforce consists of both a civilian and military component, and we continue to pursue and employ the necessary authorities to efficiently recruit and retain top cyber and other technical talent. We are working diligently to close critical talent gaps, enhance professional development, and build a robust student pipeline that will position the Department of Defense for future success. Furthermore, DOD supports the removal of barriers necessary to facilitate the acquisition of critical talent, expand pathways to service, and enable the flexible workplace essential to the future of work. The Department appreciates, and continues to exercise the flexibilities granted by Congress to design and implement programs and policies that promote the health of the cyber workforce.

CIVILIAN FORCE

The civilian cyber workforce is overseen by a single overarching Department-level cyber governance structure that ensures successful implementation, and proper and effective use of Congressionally approved authorities and flexibilities. The governance structure, known as the Cyber Workforce Management Board (CWMB), includes stakeholders from across DOD, including the USD(P&R), the Principal Cyber

Advisor, and the DOD Chief Information Officer (CIO), as well as the Under Secretary of Defense for Intelligence and Security, the U.S. Cyber Command (USCYBERCOM), and representatives from each of the Military Departments.

The USD(P&R), who also serves as the DOD Chief Human Capital Officer, exercises broad oversight for civilian personnel programs and functional communities for the Department, and is responsible for providing key advice and assistance to the CWMB on cyber workforce matters. The USD(P&R) partners with the DOD CIO to develop, manage, and evaluate cyber workforce policies and programs, including those related to hiring, compensation, and the development of civilian cyber talent.

OUSD(P&R) remains actively engaged in the oversight of the Cyber Excepted Service (CES), including its training and implementation objectives, and serves as an active participant in the planning and phased execution of the Department's Zero-Based Review of cyber and technology personnel. Pursuant to this governance structure and engagement, the Department is well positioned to manage, evaluate, and advance the cyber civilian workforce.

Cyber Civilian Workforce

The Federal Cybersecurity Workforce Assessment Act of 2015 required all Federal Agencies to develop procedures and code positions performing information technology (IT), cybersecurity, and other cyber-related functions. The DOD CIO issued implementing guidance, which required DOD Components to code all civilian cyber workforce positions, including legacy IT positions, those involved in cybersecurity, and key positions engaged in research and development, test and evaluation, program management, acquisition, software development, engineering, intelligence, and other relevant activities. Given the complexity of defining these roles in certain populations, this effort remains ongoing; however, it has proven crucial to the Department's ability to manage, evaluate, and educate the cyber civilian workforce.

To that end, the USD(P&R) supports the DOD CIO's efforts to track and monitor the cyber civilian workforce by providing regular, recurring personnel data reports on the cyber coded workforce, and in collaboration, develops new reports and provides additional analyses of the workforce's health and behaviors. Currently, the DOD cyber coded workforce is made up of over 65,000 personnel, including over 6,500 who have been converted or appointed into the CES. Ten DOD organizations have converted into the CES, with the Army Cyber Command expected to begin conversion in fiscal year 2022.

The cyber civilian workforce is demographically consistent to the appropriated fund civilian workforce; however, in comparison, the civilian cyber workforce has a higher percentage of those holding Bachelor's and Master's degrees to those of the broader population (Cyber Bachelor: 38.17 percent versus APF: 28.76 percent; Cyber Master: 20.26 percent versus APF: 17.62 percent). Between fiscal year 2018 and fiscal year 2020, the overall cyber workforce increased an average of 6 percent (fiscal year 2018: 6.9 percent; fiscal year 2019: 7.8 percent; fiscal year 2020: 3.4 percent). When coupled with that of average annual loss, 0.7 percent, and the number of those currently eligible to retire (13.93 percent), the Department is postured to continue to renew its talent and expertise while maintaining continuity of mission.

Civilian Hiring Authorities and Compensation Flexibilities

In recent years, Congress has provided several DOD-exclusive civilian hiring and compensation authorities that have better postured the DOD to be able to recruit and retain an effective and highly qualified cyber civilian workforce. We appreciate Congress' recognition of our need for increased flexibilities to attract, hire, and retain high quality civilian personnel in a timely manner. The Department continues to proactively ensure their effective application across cyber-specific functional/organizational areas, and assess the need for new authorities to aid recruitment and retention. It is through partnership with CIO, the DOD Components, and the cyber functional community, as well as with private industry, that we will continue to effectively implement our flexibilities and further expand our outreach and pathways to recruit and hire top talent from across all segments of society, while retaining current technical talent and closing mission-critical gaps.

DOD Hiring Authorities

The CES, codified in section 1599f of title 10, United States Code (U.S.C), authorizes the Secretary of Defense to hire cyber personnel to positions in the excepted service in the USCYBERCOM headquarters, elements of USCYBERCOM enterprise relating to cyberspace operations, and in supporting elements of the Military Departments. This authority, coupled with certain enhanced pay flexibilities, provides agility, mitigates challenges of recruiting and retaining quality civilian talent, and thus, helpful to the Department in competing with the private sector for cyber talent.

Additionally, in Fiscal Year 2017, section 1643(a)(3) of the National Defense Authorization Act (NDAA), authorized the Secretary of Defense to appoint qualified individuals directly into the USCYBERCOM and its enterprise in positions in the competitive service. This Direct-Hire Authority (DHA) provides interim authority to improve the Department's ability to hire civilian personnel necessary to support the cyber mission, and is intended to be superseded upon full implementation of the CES. Like other DHAs granted to the Department, this authority provides flexibility to hire critical cyber talent without applying traditional title 5 competitive procedures.

The Department recently sought streamlined, simplified, and standardized authorities to enable efficient hiring for mission critical positions that enhance readiness. Section 1109 of the NDAA for fiscal year 2020 granted such streamlining and enhanced certain existing DOD DHAs, including an expanded DHA for cyber workforce positions. The expansion of coverage has been beneficial in that it has allowed the Department the ability to directly hire for any and all critical cyber skillsets. The streamlined authority, which has been in use for a part fiscal year 2020 and fiscal year 2021, garnered a significant average decrease in time-to-hire from fiscal year 2019 (fiscal year 2019: 117 and fiscal year 2020/21: 89). The Department expects to see continued decreases under the streamlined approach.

Between fiscal year 2019 and fiscal year 2021, the utilization of direct hiring authorities for cyber security professionals has yielded over 4,200 cyber professionals to date, with hires expected to increase each fiscal year. During the same timeframe, the Department utilized other hiring authorities to appoint over 12,500 cyber coded civilians. Of note, in fiscal year 2021, DOD utilized the expanded cyber DHA about 32 percent of the time, while continuing to utilize the full range of delegated examining, veterans hiring, and other competitive and noncompetitive authorities to reach qualified and diverse cyber talent.

Compensation Flexibilities

The Department utilizes a variety of compensation flexibilities in order to recruit and retain its top cyber talent. Entry and developmental computer engineers, computer science specialists, and IT specialists are all brought in under the Federal-wide special salary rates, which are higher than normal rates of basic pay which allows the Department to more comparatively compensate these specialties to that of the private sector. The added flexibility of the CES has also allowed the Department to implement targeted local market supplements for certain cyber occupations and locations, and to extend the pay scale to the equivalent of step 11/12 on the GS pay scale. Additionally, the Department utilizes advanced-in rates to recruit its talent, bringing 39.9 percent of the cyber workforce new hires in fiscal year 2020 at a step 2 or higher (36 percent in fiscal year 2018; 39.5 percent in fiscal year 2019).

Furthermore, we utilize recruitment, relocation, and retention, as well as student loan repayment incentives to better attract and retain this in-demand talent. In fiscal year 2020, of the 2,143 cyber workforce hires, 30.3 percent were given a recruitment or relocation incentive, a 21 percent increase from fiscal year 2019 (9.27 percent); 3.87 percent were given student loan repayment (3.1 percent in fiscal year 2019); and 1.68 percent (1,058) of the total cyber workforce in fiscal year 2020 were given a retention incentive (0.33 percent in fiscal year 2019 (194)).

Finally, section 241 of the NDAA for fiscal year 2021 afforded the Department the authority to provide special pay incentives for proficiencies beneficial to national security interests, including in computer or digital programming languages. The Department is working in partnership with the DOD CIO to implement the policy for this section of law. Such authorities expand the Department's toolkit of compensation authorities much needed to attract and retain the best talent and to compete with the private sector for the same skillsets.

Human Resource (HR) Training

The Department acknowledges that civilian policies should be as clear and concise as possible to enable DOD organizations to acquire talent where and when needed to increase readiness and lethality across the Department. This requires the effective professional development of our HR workforce. The Department is committed to ensuring that we are training and assisting HR professionals and managers alike in the use of cyber personnel management authorities and flexibilities, and increasing our partnerships with hiring managers and organizations to achieve the common objective of bringing on new talent. This not only includes streamlined and efficient guidance on the use of the authorities and implementation procedures, but also proactively gathering and analyzing data to better equip practitioners with the necessary information to proactively address emerging requirements.

In implementing our cyber authorities, the OUSD(P&R) worked closely with the DOD CIO and cyber functional community in its development and delivery of CES training for the affected workforce, leadership, and HR professionals. Encapsulated within the DOD Cyber Exchange public facing site are online courses and job aids that cover concepts from CES history; understanding employment and placement authorities and flexibilities; compensation administration; and the overall execution of the HR lifecycle for the CES workforce.

Additionally, OUSD(P&R), in its functional oversight role, continues efforts to ensure that information provided to HR personnel across the Department encompasses the full spectrum of hiring options that enable hiring managers to reach the right talent at the right time. Information is disseminated regularly through policy, memoranda, community messaging, job aids, and recruitment, compensation, and functional community-specific working groups to ensure the HR workforce is prepared to meet their customer's needs.

Specific to this role, most recently, section 246 of the NDAA for fiscal year 2021 required the Department to develop a training program for HR personnel in best public and practices for attracting and retaining technical talent, which would include cyber talent. The Department is working with the Under Secretary of Defense for Research and Engineering and other functional managers of technical, digital, and cyber workforces to implement a pilot program by January 2022 focused on the use of DHAs, competitive and accepted service authorities, special pay authorities, and private sector practices.

MILITARY FORCE

Maintaining a strong military force requires Service end-strengths that are appropriate and cost-effective. The Department manages the total military workforce through broad-based personnel policies promulgated to allow the Services and functional communities to have the tools and flexibility they need to meet their manning requirements.

Threats in the cyberspace domain are constantly evolving and emerging. Enabling our cyber forces to operate and defend against these threats will mean maintaining the military authorities and resources we have today, while also ensuring our cyber warfighters are properly accessed, compensated, and retained to prepare for these threats.

Military Accession Standards and Recruiting

The Military Services conduct a “whole person assessment” of each candidate who applies for either an officer commissioning program or the enlisted force. This holistic process reviews a number of factors including citizenship, age, education, medical/physical fitness, drug and alcohol abuse, conduct, and aptitude. This process is continuously evaluated, ensuring we use valid, reliable, and fair criteria and measures. Continuous refinements result in an improved ability to select a talented and diverse cohort, which in turn contributes to improved training graduation, lower attrition, greater lethality, and improved retention. The general DOD model is to recruit and access a qualified field of applicants, place them on best-fit occupational career trajectories, and provide the necessary technical training required to meet operational objectives. This process provides a stable pipeline of highly qualified personnel for education and training in emerging fields, such as cyber and artificial intelligence.

The Services can also employ an accession option known as “lateral entry.” This process allows the active and reserve components to recruit highly qualified individuals directly from the civilian population to fill critical requirements. These individuals are allowed to enter at advanced grades based on the level of their education and experience.

The basic eligibility criteria and screening process for cyber recruits is the same as it is for all other candidates: each must meet Service and DOD standards for enlisting or entering an officer commissioning program. Once qualified, the process for assigning officer candidates and enlisted recruits into occupational specialties is based on a talent management model which includes measures of operational requirements, cognitive ability, personality, and interest.

The Military Academies and Reserve Officer Training Corps programs have been successful at attracting talented young officers into the cyber fields. The Academies and Senior ROTC (Reserve Officer Training Corp) all have a cyber-focused program, with a curriculum that immerses students in the cybersecurity discipline while educating them to become future military leaders. These programs exist to educate Cadets/Midshipmen on the needs of the national cyberspace operations community, helping them develop skills necessary to fight and win in the cyber domain.

The Services' ongoing collaboration with industry leaders to further the skills sets of these officers also provides an incentive for individuals to consider military service. For enlisted accessions, the Services utilize an array of assessments to assign individuals to technical training, including cyber. For example, in enlisted cyber specialties the Services utilize a combination of general aptitude assessment based on the Armed Services Vocational Aptitude Battery, and a targeted cyber knowledge test, called the Cyber Test (CT) to identify applicants with aptitude and applicable knowledge in the cyber career field. CT was developed to specifically predict performance in cyber-related training, and includes items to assess knowledge and ability across four dimensions: Computer Operations, Networking and Communications, Security and Compliance, and Software Programming and Web Design.

Additionally, the Office of the Secretary of Defense and the Services are continuously evaluating new types of assessments that can provide added information in identifying applicants with the highest aptitude for cyber. For example, a fluid intelligence test called "Complex Reasoning" was recently developed. This assessment will further complement the current battery of tests by measuring abilities such as problem decomposition, abstraction, pattern recognition, and analytic ability, all of which have been shown to be indicators of success in the cyber field.

Military Compensation

The Department realizes that military members with cyber experience are in great demand and can command top salaries within the private sector. In addition to the robust military compensation package the Department offers, the Services can also offer bonuses and incentives to attract and retain Service members in all specialties, to include those in the cyber community.

Today, the military offers a range of enlistment, reenlistment, and Selective Retention Bonuses to encourage individuals to enlist, re-enlist, or extend their enlistments. Similarly, the Department also has the ability to offer a variety of bonuses and incentives to attract and retain officers who commit to serve in cyber warfare communities for specified periods.

The Department has the authority, pursuant to title 37, U.S.C. section 331, to offer a general bonus for enlisted members. This enlistment bonus is up to \$50,000 for those who agree to serve for at least two years in a specified career field—such as cyber—as well as a retention bonus of up to \$30,000 per year of service obligation. A companion authority for officers, 37

U.S.C. section 332, allows bonus payments of up to \$60,000 for an initial minimum of 3 years of service upon commissioning, and an annual retention bonus of up to \$50,000. The Reserve Component also has retention bonuses available—up to \$12,000 annually for officers.

The Services have the authority to offer other monetary and non-monetary incentives for service in certain cyber-related occupational specialties and duty assignments. Non-monetary incentives may include choice of duty assignment, guaranteed training, advanced education, and other professional development opportunities. Additional monetary incentives currently include the authorities for assignment incentives and special duty assignment pays. These pays can cumulatively be as much as \$5,000 per month (\$60,000 annually).

Overall, the monetary and non-monetary incentive authorities available to the Department and Military Services are robust, and provide the Department with the ability to selectively target incentives to members in specific skills and cyber-career fields. This allows the Department to remain competitive in attracting and retaining our military cyber workforce.

Military retention

The Department continues to exhibit strong retention through the first two quarters of the fiscal year and is projected to meet fiscal year 2021 retention goals. Although shortages in specialty areas do exist, in addition to the statutory requirements directed at the Department to increase retention, our Department of Defense Instructions govern bonuses/incentive pays that establish the minimum service obligations/additional service obligations members must fulfill in exchange for receiving training and or a bonus/payment. Additionally, in order to mitigate these shortages, the Services utilize retention levers in the form of monetary and non-monetary incentives (e.g. bonuses, stabilizations, station of choice, etc.) to retain the best and brightest in all of our specialties which would include our cyber community.

We are confident that our retention polices are adequate to present a mission-ready cyber workforce, and the Military Services do not currently feel additional authorities are required to achieve our cyber personnel targets.

CONCLUSION

The Department prides itself in building a strong and viable Total Force that delivers combat capability around the globe. Our cyber personnel are and will remain a critical component of the Department's ability to defend the Nation. Through the use of the processes, procedures, and policies we have in place, we can attract, appropriately compensate, and retain the best Total Force in the world. We look forward to any questions you may have at this time.

Senator TILLIS. [Presiding.] Thank you, Ms. Hinton. General Crall.

**STATEMENT OF LIEUTENANT GENERAL DENNIS A. CRALL,
USMC, DIRECTOR, COMMAND, CONTROL COMMUNICATIONS
AND COMPUTERS/CYBER AND CHIEF INFORMATION OFFICER,
JOINT STAFF, J6**

General CRALL. Sir, thank you for the opportunity to share a few thoughts and then certainly get into your questions.

It is very clear that the committee knows the challenge we face. You know, we are about warfighting businesses in the Joint Staff, and the digital nature of the fight that we expect, especially at pace and speed, is going to demand workforce and talent level that we have not seen before. The human-machine interface brings a demand that is going to have to be found, cultivated, educated, and implemented to get that level of experience as we learn and work our way through this new capability set.

You have heard from my partners up here the number of efforts that are underway, but I take maybe a more sobering look at where the need lies ahead, to make sure we fulfill your charge. You said be absolutely certain that we are getting the right talent, basically delivered at the right time, and I am not absolutely certain.

I had the opportunity to do some traveling with the Vice Chairman the week before and talk to some industry leaders, and I specifically challenged them as to how they went about finding the talent to fill the same billets that we are looking to fill, the same people with the same skill sets. We always talk about money as being maybe the driving factor, but I learned some things that challenged my previous thinking on our approach to this.

So while many of the endeavors that you have heard about and will hear today are certainly worthwhile as we work our way through feeling out what works best for us, I do not think we know our target audience as well as we need to. We need to find out what really motivates individuals to want to serve in the capacity that we are offering.

We also need to do a better job in evaluating the very programs that we are describing. I do not believe that while they are interesting to approach and employ, they may not all deliver in the way that we expect, and we certainly want to tweak the ones that can be maximized to deliver that output, and maybe retire some that are not working. So we owe a better understanding and study of our own efforts and our own audience.

So while I am excited and optimistic at the opportunity to get after fulfilling this talent range that we need, I am concerned about pace. I think the divide between the need is growing, compared to what we are able to fulfill. I am not sure we are closing the gap, and I think time is ticking for us to do so. So the challenge is certainly understood, I think on both ends, and we are looking

to maximize the very empowerments that Congress gave us to get after this. But I think more time and more effort and a faster pace is needed, and probably a new approach to our thinking, to make sure that we can meet the need.

Thank you, sir. I look forward to your questions.
[The prepared statement of General Crall follows:]

PREPARED STATEMENT BY LIEUTENANT GENERAL DENNIS A. CRALL

Thank you Chairwoman Gillibrand, Ranking Member Tillis, and Members of the Personnel Subcommittee. It is an honor to appear before you to discuss the military requirements relating to the cyber workforce within the Department of Defense. I appear before you today in my role as the Director for Command, Control, Communications and Computers/ Cyber and Chief Information Officer for the Chairman and Vice Chairman of the Joint Chiefs of Staff.

My testimony will focus on the cyber workforce required to meet current and future defense requirements and mission demands as well as the talent management required for recruiting and retaining world-class, cyber professionals. These comments serve to complement my DOD CIO colleague's discussion of Department-wide cyber workforce initiatives, and my Personnel and Readiness colleagues' civilian and military workforce policy review.

Requirements. The Cyber Mission Force consisting of approximately 6,187 personnel, comprising 133 active component teams, grew out of the DOD Requirements process in fiscal year 2012—USCYBERCOM initially submitted a Program Budget Review (PBR) 2014 issue paper requesting 1,204 billets to "Defend the Nation," which was composed of 479 National Security Agency billets and 725 Service billets. This was focused on deterring/ defeating cyber-attacks against the US.

During the PBR 2014 process, United States Cyber Command (USCYBERCOM) briefed emerging operational requirements to the Joint Chiefs of Staff, identifying the need for additional offensive and defensive manpower to address Combatant Command warfighting requirements. This expanded the original manpower requirements issue paper request from 1,204 to 6,244 billets in the active component, distributed across the United States Army, Air Force, Navy and Marine Corps. Chairmen of the Joint Chiefs of Staff (General Martin Edward Dempsey, at the time) endorsed the requirement. It was approved at the Deputy's Management Action Group (DMAG), fully sourcing in the 2014 Program Decision Memorandum. This remains, by and large, the Cyber Mission Force that we have today. I will note that in fiscal year 2014 the Department of the Army also made an internal Service decision to establish 21 Cyber Protection Teams (11 in the Army National Guard and 10 in the Army Reserve), the development of which would be phased over time with them all becoming fully mission capable by fiscal year 2022.

In June of 2020, the Commander USCYBERCOM briefed the Secretary of Defense as part the Combatant Command Review process on the need for assessed force growth to address ever emerging threats presented by persistent adversaries. Accordingly, USCYBERCOM submitted a new Issue Paper for 14 additional Cyber Mission Force Teams during the fiscal year 2022–2026 Program Review.

Talent Management. The Department must seek all opportunities to garner new talent whether through traditional recruiting offerings or authorities provided through initiatives such as the Cyber Excepted Service (CES) personnel system. The Fiscal Year 2020 NDAA House Armed Services Committee encouraged the Department to better utilize statutory authorities for recruitment and retention. Within my Directorate of the Joint Staff, I worked with the Cyber Workforce Management Board to identify areas where we can leverage the existing authorities in section 1599f of title 10, U.S. Code, to further efforts to recruit and retain talent as part of the CES. Within the Department, more components are currently assessing where that authority can best be leveraged.

The Department must also re-think our perspectives related to recruitment and retention, a lesson we may be able to learn from industry. For example, industry leaders have explained to me that new recruiting successes are those that allow individuals to work where they desire to live. The nature of many of these digital work roles may lend themselves to remote work if the facilities are provided to accommodate classified work (when required). Additionally, private sector corporations are abandoning conventional recruiting campaigns where they advertise billets and pay for leads of prospective applicants. Instead, they are increasing partnerships with universities to create a "human supply chain" of sorts where they set education / experience requirements and hire from these sources almost exclusively. Partici-

pating schools agree to align their curricula with the skillsets required for their mission-specific work roles and thus have direct placement at higher rates than those who do not follow a like model.

Security Clearance Reform. Critical to recruiting and hiring our cyber warriors for the ever-changing and growing challenges within the cyberspace domain are the Department's processes, practices, and onboarding efforts. Our lengthy security clearance process timelines continue to hinder the onboarding of talent, often resulting in applicants deciding to pursue employment in the private sector. There are two components to this challenge: eligibility and access. The Department has made great strides in determining eligibility through the establishment of the Defense Counterintelligence and Security Agency (DCSA). As for access, we continue to work with the Intelligence Community refining processes that allow new cyber workforce civilians and military personnel to utilize the tools of their new trade. That work is ongoing and continues to improve. Identifying applicants early in the process has proven the most promising to date. For example, the University of South Carolina Reserve Officer Training Corps program has taken the innovative approach to ensure Midshipman graduate with a Top-Secret clearance so they are prepared to support their respective Service mission on day one. This concept should also work for internships and other similar programs where applicants can be evaluated over time and in an environment related to their cyber training and education.

Retention. The Department continues to face retention challenges. While more study is needed to ensure we have a thorough understanding of this dynamic, an area to strengthen retention opportunities is likely through enhanced and expanded student loan repayment authorities and appropriations for the Department to leverage.

Way-Ahead. The Department must continue to explore traditional and non-traditional options for recruitment, develop, and retain our workforce by potentially assessing and leveraging our Reserve Components; seek partnerships with Academia and Research institutions; decrease our security clearance timeline to efficiently onboard our talent; assess and obtain a greater understanding of our talent pool's motivations; and assess the viability of a strengthened talent management exchange between government and industry. To that end, I will continue to partner across the Department as an advocate for the cyber workforce and cyber-related initiatives. I am grateful for Congress's strong support towards the Department of Defense in building the cyber forces needed to be lethal and deter in cyberspace. I thank the Subcommittee's interest in these issues and look forward to your questions.

Senator TILLIS. I am going to—we will wait on, or we will see Senator Gillibrand go back, but I will go ahead and ask some questions, and if she takes a little time I will ask more questions.

General, I am going to ask Ms. Hinton a question second, but your comments made me reflect on a discussion I had yesterday with the Personnel Subcommittee staff. I worked in research and development and product management back in the '80s, and I was trying to think about, we were having a tough time attracting talent back then. This is a perpetual problem in the private sector, and even more difficult, I think, in the government sector.

But one thing that we had in place that I do not even know how we would structure it here, but you had these highly motivated, technically competent software and hardware engineers that we created an economic incentive, on their day job, work on fulfilling their mission set, to use your terms, but if they chose on weekends and nights to come up with something creative that was relevant to what you were doing but was creative, we had an economic and other reward systems that encouraged that sort of extracurricular activity.

Any thought, for any of the panelists, any thought on the applicability of that same sort of thing, that still continues to this day in a lot of the software and hardware research and development shops, how something like that would even work or whether or not it would make sense, given your mission goals?

General CRALL. Sir, it is interesting because that overlaps quite well. You know, even the time frame that you said. I will be careful because my observations, I believe, are anecdotal. I had a chance to talk to probably a few dozen individuals who are right squarely in the market of the type of individual we want to recruit. What I found interesting was their answers were almost identical, so not a true statistical sampling that I would trust, necessarily, but this is what has me some pause.

Not only did the CEOs [Chief Executive Officers] and CIOs [Chief Information Officers] tell me this, I discovered it for myself. The number one area that came back in feedback to me was people want to live where they want to live. The idea of moving to someplace they do not want to live, no matter what other feature is offered, is apparently quite unattractive. If you look at some of the hubs that we have to offer, that is going to be a challenge for us.

There are some interesting solutions, given the work and the nature that maybe we need to explore about creating spaces where that work can be done literally anywhere, as long as the security environment is set for that. But living in the community they want to live in seemed to be a strong driving factor.

The other one was in team composition, which gets after what you described. The hierarchy of the government isn't something that is really motivating to them at all. They want a flat organization where everyone has equal input into driving an outcome. For many of them, wearing the uniform was not attractive. They like working hours from noon until 3 a.m., is their prime working hours, and again, does it matter if productivity is there? Our organizations do not normally look like that.

Senator TILLIS. I even had a ponytail back in the day.

[Laughter.]

General CRALL. Yes, sir.

Senator TILLIS. It was not a good look.

General CRALL. Student debt was more important than the salary itself, which seemed odd to me, because it appeared that higher salaries could retire student debt, you know, maybe over time, but they looked certainly at the idea of what programs could address the debt they are in.

The last piece that we did very well in, the reason we were even having the conversation, was cause. They want to work for a cause, something that is meaningful, something that is viable, not just simply to make money. The government, especially the Department of Defense, was unusually attractive to them, to give back some level of service, and to do activities they could not do in other jobs.

So, you know, again, sir, that is maybe just a few ideas that I learned.

Senator TILLIS. Well, thank you. I am going to yield back to the chair and then reserve the right for a second round, if that is okay.

Senator GILLIBRAND. [Presiding.] Absolutely, and you can ask another question if you prefer.

Senator TILLIS. Well, Ms. Hinton, I will ask you a question. I do have some for the other witnesses, but I am kind of curious about your view of the Cyber Excepted Service, what is working, what is not working. I am particularly interested in loan repayment benefit.

Ms. HINTON. Yes, sir. So Cyber Excepted Service has given us incredible flexibilities that are not resident in traditional civil service authorities. In particular, we have found great use in the hiring authorities that are associated with Cyber Excepted Service, that ability to target recruitment opportunities to get the talent that we need.

Another piece of the Cyber Excepted Service that has been beneficial has been the compensation authorities. In particular, we have recently rolled out targeted local market supplements that enable us to compensate at a higher level for seven areas. So it gives us that ability, while General Crall mentions that compensation is not the only factor that weighs in an individual's decision to serve, it certainly is a factor, and our ability to compete with the industry through those compensation flexibilities helps us get at that targeted skill set that we need.

Additionally, with the Cyber Excepted Service, it gives us some authorities to think about how we classify work, how we organize work, how we describe work, and how we look at the qualifications associated with the individuals that we need.

I will say that there are some challenges with Cyber Excepted Service, and I would really back that up to a broader perspective in the whole cyber-coded workforce, which is not just Cyber Excepted Service.

So first, as we think about compensation authorities that we were given, we are still held to the existing pay caps that we have under Title 5. So while we have some flexibility to change policies and processes associated with how we compensate, we are still held to the higher limits. So that really does not make us, in certain areas, as competitive as we could be to get certain talent.

The other sort of nexus with Cyber Excepted Service that I would highlight is that it is tied to United States Cyber Command and those supporting elements, and so when we think about the cyber workforce writ large, Cyber Excepted Service is just one subcomponent of a broader cyber mission set. So as we think about where there are opportunities to expand the use of Cyber Excepted Service, we have had to look at what are some different ways that we can determine what are elements that are supporting Cyber Command on a position-by-position basis, to be able to expand that authority. So that is one area where I think there is opportunity to look at the authority and see does it have broader application, broader use.

Additionally, there are some authorities in some of our sister alternative personnel systems, like Acquisition Demo demonstration project or our Defense Civilian Intelligence Personnel System, that allow for some additional flexibilities around streamlined classification that I think would bolster the Cyber Excepted Service.

But all in all, we are very thankful for this authority. It has given us additional flexibility, and I will defer to Mr. Sherman for additional information about that.

Senator TILLIS. I am going to come back with questions for Mr. Sherman. I particularly want to know about the current loan benefit, and back to General Crall's point, I do think that they place a value on that. Even though the compensation may be offsetting,

there is something attractive about just getting that debt retired as quickly as possible.

But I am going to ask some additional questions. I will defer back to the chair.

Senator GILLIBRAND. Thank you very much. For the whole panel, the National Security Commission on Artificial Intelligence has recommended a digital academy to address the skills gap in cyber workforce hiring, which will be fully accredited and independent from the government, with students doing government and private sector internships during breaks.

The Department of Defense does have some existing authorities to address the skills gap now. We talked about the CES program. There also exists authority for the Department of Defense to grant cyber scholarships, paying for up to 3 years of college, and there is, of course, the ROTC commissioning programs that currently pay for up to 4 years of college, and even for graduate and professional school beyond 4 years, in some cases.

So for each of you, I would like to start with Ms. Hinton and then go to Lieutenant General Crall, then Mr. Sherman, then Mr. Litton, what are the most important components to consider regarding this recommendation for a digital academy? Is this a necessary step? Could we also work to fill the skills gap from diverse sources, using existing authorities such as the cyber scholarships or a generous ROTC program?

Ms. HINTON. Thank you, Senator Gillibrand. That is a great question, and we are very interested in the digital academy as another potential Federal-wide avenue to reach the talent that we need. Certainly, in the Department, as we look through standing up the Defense Civilian Training Corps, which is an authority that we received recently, we thought through how and what type of academic programs we need in order to reach this talent, and the digital academy would be another complementary avenue for us to be able to identify that diverse segment of the population and to bring them into Federal service, and to entice them into Federal service.

In particular, to Senator Tillis' point around student loan repayments, the ability to offer paid education in exchange for service to the country is an area where we think that will enable us to reach this talent and entice them and attract them to support not just the Department of Defense but from a U.S. digital academy perspective, benefit to the entire government.

In terms of authorities that we use to attract a diverse workforce, I will mention again that the streamlined direct hire authority that Congress has granted us, has so generously granted us, has been an incredible tool for us, to be able to target our recruitment and outreach, in complement with our scholarship programs. In particular, when we look at our cyber student hiring authorities, we see that even if I look at fiscal year 2021, we have been able to attract 20 percent of our student hires, cyber student hires, have been Asian Americans. We see in our Cyber Excepted Service 20 percent of our Cyber Excepted Service hires have been African American.

So these hiring flexibilities make a difference for us to go out and target the diverse segments of the country, and then the scholar-

ship programs add that additional bonus of enticing them to serve in exchange for their paid education. Thank you.

Senator GILLIBRAND. Thank you. Lieutenant General Crall?

General CRALL. Ma'am, to your specific question about the digital academy, I really do not know whether that is a good idea or not a good idea. I think through the throughput and what the volume of that academy might produce might really be the answer.

What I have found interesting is attending two universities last week, meeting with staffs and what degrees they offer and what motivates them and how they build curricula, it seems there is a very willing audience in the university system writ large to cater to this audience. Some of our more technical universities have created what is almost a human supply chain with industry, to build the very individual that can be placed immediately into the corporate world, and that means they come with security clearances, background, training for the years and internships that build up to that. That long-term relationship, that may be buttressed by the ROTC programs at large, for all the services, to include service in the Guard. There are a lot of opportunities.

But the National Center of Academic Excellence in Cybersecurity, that whole apparatus, which is a formal partnership, I think is up to over 80 schools now. The last two schools that we looked at were just joining that consortium, which lays out that curricula and provides an interface with the Department, again, to build that cyber warrior for which we are looking. Then all these things can be applied on top of it, to include the internships, scholarships, et cetera.

What I find lacking in this, though, is that the colleges and universities that have signed up for this thus far do not represent the full scope that we ought to be interacting with. I believe there is room for more diversity in the schools and outreach to make sure that we get greater participation.

Senator GILLIBRAND. Mr. Sherman?

Mr. SHERMAN. Thank you, ma'am. I would agree with my colleagues' comments on this, and I want to build on what General Crall said. From my view as CIO, the Centers for Academic Excellence for Cyber, they do offer a pretty broad and diverse set of schools we can get to, everything from North Carolina A&T to NYU, from University of Missouri-Columbia to Honolulu Community College. It is a broad swath there.

I would certainly welcome a digital academy as an additional pipeline, but I would not want to do it at the expense of this broad swath of schools, from rural, urban, all across the country, historically black colleges and universities (HBCUs), larger universities, et cetera.

What we have through the National Security Agency (NSA) Cybersecurity Scholarship Program, leveraging these Centers for Academic Excellence, back to what General Crall was saying about the pipeline of talent, I think it has been diverse, as Ms. Hinton indicated, for African Americans, Asian Americans, I would add Hispanic Americans, Latinos, Latinas coming into our workforce. I would want to continue to leverage that.

So I think a digital academy would be a good complement to that, but what we are doing on the CIE front, with the broad

swathe of opportunity, I would want to keep that up as well, because we are seeing return on investment there. Thank you.

Senator GILLIBRAND. Mr. Litton.

Mr. LITTON. Yes, ma'am. Each year the Military Service Academies and senior ROTC programs produce approximately 450 cyber officers for the military. Most of these universities with senior ROTC programs, and, of course, the academies, are certified as National Centers for Academic Excellence in cyber defense education by the National Security Agency, and most, as well, have a cyber institute dedicated to research to promote the understanding of cyber and cyber to be used in defense.

The Citadel, along with the five other senior military colleges, have each received approximately \$1.5 million of Federal funds to establish these cyber institutes as pilot programs on their campuses, and so I think your idea is very well taken, ma'am.

Senator GILLIBRAND. Thank you. Mr. Tillis—Senator Tillis.

Senator TILLIS. Thank you. Mr. Sherman, last Congress we authorized the CYBERCOM enhanced pay authority. It was based on a generally viewed successful program out of Defense Advanced Research Project Agency (DARPA). I understand that CYBERCOM has chosen not to implement that. Is that true, and what was the rationale for not doing it?

Mr. SHERMAN. Sir, I am going to tell you I am frankly not sure on that particular authority there. I would have to go back and take that one for the record and check with General Nakasone on that, sir.

Senator TILLIS. Okay. Thank you.

[The information referred to follows:]

Mr. SHERMAN. USCYBERCOM endorses this authorization and is exploring and identifying up to 10 scientific and engineering positions that coincide with the use of this authority granted to USCYBERCOM by Congress and contained in Section 1708 of the Fiscal Year 2021 National Defense Authorization Act.

Mr. Litton, I just had a question, I think it was the Fiscal Year 2019 NDAA. It included several provisions to disrupt the standard tenure-based military career path. We were especially concerned with cyber careers. The alternative promotion authority, in particular, meant to provide more flexibility for promotions. What is the current status?

Mr. LITTON. Yes, sir. My understanding is that we have largely implemented that. If you are referring to our ability to rank officers on the promotion list based on their skills and abilities, and our need for them in the service to be promoted before the other—

Senator TILLIS. The military departments are authorized to use it?

Mr. LITTON. Yes, sir, they are.

Senator TILLIS. Thank you.

General Crall, the Defense Digital Service, DDS, put in place some innovative personnel policies, and we have seen some of the best cyber officers that enlisted spend time at DDS. What is special about it, and should we extend this kind of mindset to the broader military cyber workforce?

General CRALL. Yes, sir. I am personally a huge fan of DDS for the very reasons you have mentioned. They approach problems in

a non-conventional way. They are not intimidated by rank, structure, hierarchy. They seem to get to—

Senator TILLIS. Well, that too.

General CRALL.—yes, sir, a very flat organization. They do not look like us. They do not act like us. But I have found that the value of getting to the truth and getting to the bottom of something, that they operate at much greater speed. Again, their ability to, you know, recruit such a diverse population, from all backgrounds, from all experiences, make the team composition one that is fairly complete. No blind spots. They are able to really fill some holes neatly, and tailor their workforce to our very specific problem set.

The last piece I would offer is they appear to be very current, because their operations and their influence in what they read and who they interact with comes from sources well outside of the Department. So they have been extremely valuable, and I do agree that those lessons learned export quite well to the condition that I offered in my opening statement.

Senator TILLIS. Yeah, I think that kind of creates a—sort of casts a wider net for that organizational framework that I think works and that exists.

Senator GILLIBRAND. Senator Tillis? Can you describe, for the record, what DDS is, how many people you have? Just describe it from start to finish.

General CRALL. Well, I apologize that I do not know the exact numbers that they have, but they are a small force, and that small force was created a few years back to get after these problem sets in an unconventional way. The recruitment for that team has been largely left up to the DDS leadership, and was managed by the Secretary of Defense proper, and they had a pretty wide authority in their hiring. They could onboard very quickly, they could go seek the talent they needed, and they are very independent. In fact, when I first met them, they were almost inspector general-like, meaning their level of independence, not beholden to anyone in the building, but to really get after truth was pretty impressive. The speed with which they delivered was also impressive.

Senator TILLIS. If we can get back those details for the record.

Senator GILLIBRAND. Yeah, for the record. So who do they report to, how many people are there, what is the salary range, just so we can describe the program accurately, to know if we should replicate it or augment it or make it bigger than it is today.

General CRALL. Yes, ma'am. I have that for action.

Senator TILLIS. I did have a question that goes to education. I will ask anybody on the panel that may want to answer it. I like the idea that we are investing in some of the military-oriented institutes, but what kind of a net have we cast? This may sound parochial, but if there are institutions like this elsewhere then they should be included.

But Montreat College, for example, in western North Carolina, just outside of Asheville, has had a four-year cyber program for several years. It actually dates back to the time that I was Speaker of the House. We provided funding to help them stand up facilities and get that program going. They have had a couple of graduated classes now.

So to what extent have we cast a wide net for any institutions, public or private, that look like they would be good feed stock and good places for investment to vector people into government service, either uniformed service or civilian service?

Mr. SHERMAN. So with the program, sir, with the ROTCs that I think you are referring to, at six universities—Texas A&M, my alma mater; North Georgia; Virginia Tech; VMI, Virginia Military Institute; Citadel, and Norwich. So six of the civilian institutions with rather large ROTCs, core cadets type functions. That was the initial group here with the initial grant investment, as Mr. Litton indicated just a minute ago. I think in terms of expanding the net, or expanding the applicability to this, we are very early in this, to see how the return on investment turns out. But this was just an initial group of institutions that have established ROTCs, sir, and so I would not see why we would not want to expand in the future, perhaps to similar institutions.

Senator TILLIS. Senator Gillibrand, if I can just ask one more question. Another discussion that came up in brainstorming about this is almost a civilian analog to the ROTC, programs where you would put them in place, they would provide civilian service to the government. Where are we with that thinking, and to what extent do you all think that is a good idea?

Ms. HINTON. Yes, sir. As mentioned previously, we are working through establishing the Defense Civilian Training Corps, which is the concept that you mentioned, the ROTC-like program. We have developed an initial implementation plan and are still exploring and building out what that will look like.

But to your point, we are looking across the nation at what institutions would have the right capabilities and program and curricula to support not just acquisition, which is a priority area we are looking at under the Defense Civilian Training Corps, but also our modernization priorities. So when we look at that program, coupled with the Defense Science, Mathematics, and Research for Transformation, the SMART Defense fellows program—sorry, I had to look down to get that correct—which is one of our many scholarship programs that is offered throughout the country, we are going after those science, technology, engineering and mathematics (STEM), technical areas to find that talent. That is another area where we are looking at, are there new outreach, new partnerships that we need to explore to find the diverse talent.

Senator TILLIS. You can do that under current authorities?

Ms. HINTON. Yes, sir.

Senator TILLIS. The last open question, really, for maybe feedback for the record—I may have a couple of questions for the record too—would be any additional authorities or modification of current authorities that would help you better tackle this problem, please get it to us. I am sure that the Chair agrees that that would be helpful, as we lead up to the NDAA process. Thank you.

[The information referred to follows:]

Ms. HINTON. The Department appreciates the many civilian personnel hiring authorities provided by Congress, including those that afford the ability to streamline hiring for critical cyber talent. The Department needs to operate with agility and aggressiveness, not only in recruitment, but in our ability to provide attractive incentive packages in the competitive global market.

Authorities such as the cyber excepted service and similar alternative personnel systems provide the flexibility to recruit, compensate, and retain highly qualified talent to meet our unique and extensive mission requirements. They enable the Department to compete for talent with an unconstrained private sector by allowing for expeditious recruitment with corresponding compensation and incentive flexibilities, such as pay banding for pay setting flexibility and/or targeted market pay. However, full use of these authorities is constrained by limitations on organizational or functional coverage and, in certain technical areas, by uncompetitive salary caps.

The Department finds that it is increasingly reliant on the full use of recruitment and retention incentives, often at the maximum authorized levels, in order to successfully attract and retain critical cyber talent. Additionally, the student loan repayment program has grown into a crucial recruiting tool, yet the program is becoming less attractive to effectively recruit and retain highly desired personnel due to statutory limitations.

Senator GILLIBRAND. Our future military leaders across all specialties must be educated on cyber issues to ensure that our military remains the world's most effective fighting force. Professional military education institutions can ensure that world-class cyber faculty are positioned to teach our officers about the ways in which cyber strategy, policy, and operations affect the Armed Forces and shape future conflict.

Several questions. When it comes to institution on topics like cyber policy, strategy, and operations, how effective are professional military education institutions across the service branches, number one? How is the effectiveness of professional military education institutions evaluated? To what extent are cyber programs and curricula standardized across the service branches? What is the expected standard of performance for professional military education institutions and educational cyber programs across the service branches? Lieutenant General Crall?

General CRALL. Yes, ma'am. There is a lot there. So I would say that maybe taking it from the highest question and working down. I know that the National Defense University, for example, that has a program, its cyber college was the first that I was aware of to offer a senior-level program, rather than curricula off to the side or maybe electives, but really a full discipline aimed at building that cyber policy professional. That is kind of a rarity. Yes, ma'am.

Senator GILLIBRAND. So there is a lot of concern right now regarding the DOD's potential elimination of the College of Information and Cyberspace (CIC) as a component institution of the National Defense University. As you mentioned, CIC provides critical mission of consolidating intellectual resources and providing joint higher education for the nation's defense community. Now more than ever, we need every resource available to bring together and grow our military's knowledge base on cyber issues, and we really should not miss an opportunity to impart that knowledge on the military's rising leaders.

With these concerns in mind, what is your long-term vision for the College of Information and Cyberspace at the National Defense University, and how can Congress help achieve that vision?

Mr. SHERMAN. The Under Secretary of Defense for Policy provided a report on April 9, 2021, to the Armed Services Committees regarding the future plans for the National Defense University's College of Information and Cyberspace (CIC), as required by Section 1741 of the Fiscal Year 2021 National Defense Authorization Act. One of the recommendations in the report is for a follow-on study regarding future requirements in order to educate DOD leaders (civilian and military) in the Information Environment / Cyberspace Domain). The Under Secretary for Policy is spon-

soring a Federally Funded Research and Development Centers (FFRDC) study that will begin in June 2021 and end approximately one year later.

General CRALL. So, ma'am, I will leave the chairman to maybe inform what his personal vision is. I will give you my personal vision is I am a big believer in that college, and I have hired many of the graduates from that program, and have employed them, and I actually seek them. So I think there has been tremendous value added with that program.

The other aspect, as far as standardized training for leadership across all the Services, we are clearly not there. There is a greater interest, and I find that our younger servicemembers and civilians come better trained and probably just more experienced, based on their age. But I have seen training programs in the Services. I just do not know that they are necessarily aligned and they are all equal. There certainly needs to be more work done to make sure that that level of training is consistent and effective.

Senator GILLIBRAND. Thank you. Ms. Hinton? You can answer any of the questions I posed on this topic.

Ms. HINTON. Yes, ma'am. So I would take the question for the record as it applies to the civilian workforce and joint professional military education. We certainly, as part of our leadership development competencies for our civilian workforce use the joint professional military education venues as an avenue for our civilians to grow and develop the same competencies as our military. But I will have to take your question for the record.

Senator GILLIBRAND. Mr. Sherman?

Mr. SHERMAN. Ma'am, I would agree with everything my colleagues said, and also for the record, the one thing I would add is on the College of Information and Cyber at National Defense University. This is, of course, aligned to Joint Staff and support them, but as a functional advocate for them we are strongly supportive of them, and as General Crall indicated, they turn out many, many good graduates, many of whom work for me as well, and we think it should be sustained and continued. We are a big fan of it. Thank you.

Senator GILLIBRAND. Mr. Litton?

Mr. LITTON. Yes, ma'am. If I might, a tangentially related issue is one of the most exciting things to me in this area is the U.S. Space Force. They are creating a digital service from the ground up. The Chief of Space Operations, Jay Raymond, has directed his leaders to improve digital education across all members of the Space Force. To that end, the Space Force has stood up a digital university which gives air and space professionals access to over 7,000 training courses in which they can access on duty, off duty, and receive qualifications and certifications to that end.

He has also directed his leaders in the U.S. Space Force to build a cadre of software developers, "supercoders," he is calling them, with the skills, knowledge, and ability to access the right and deploy software to military systems at the speed of relevance. Yes, ma'am.

Senator GILLIBRAND. We do not have a Space Force Academy. Should we?

Mr. LITTON. Ma'am, that is a good question. I think right now that the United States Air Force Academy is doing an adequate

job. I think as the Space Force grows and matures, that is something that the Department should take a hard look at.

Senator GILLIBRAND. Do you believe that the U.S. Air Force has the state of the art cyber technology department?

Mr. LITTON. Well, all of the Services have cyber capability. All of the Services are really doing their best and trying really hard to acquire that talent and develop them to meet the need of the warfighters. That is more kind of in General Crall's lane than mine. Mine is the policy to access and enable the Services to retain and support those members.

Senator GILLIBRAND. Lieutenant General Crall, can you speak to having a Space Force Academy, whether the Air Force has enough expertise in developing it, and speak to perhaps—I know West Point has a cyber program. Can you speak to each of these departments and whether they need to augment what they offer or whether they are doing what they need to do sufficiently?

General CRALL. So, ma'am, I will have to take the comment on the academy and whether the Air Force has an adequate, you know, presence, I would have to take that for the record because I do not know.

Senator GILLIBRAND. Okay.

General CRALL. But to the other question about where the talent comes from across all the Services, I think it is important to note that if we believe—and I do believe—that United States Cyber Command has amassed, really, our most technical individuals in the cyber community, it is important to note from where they come. Those are service-provided individuals. So as Cyber Command sets, as a joint force provider and joint force trainer, that common curricula and standard, it is the Services who are recruiting and putting those individuals through the pipeline.

So I think the Services do have pretty good footing and a pretty equitable talent base.

Senator GILLIBRAND. Could we get a report on that, of what is the personnel makeup of Cyber Command, and an analysis to the question about whether we should be standardizing the teaching across service academies, but also the question of do we need a Space Force Academy? Then, which you have already said, you do believe that we could have a separate Federal cyber academy for all Federal workforce needs, not just the Services.

General CRALL. Yes, ma'am. I will take that for the record.

Senator GILLIBRAND. I would like your opinion on it.

Mr. Tillis?

Senator TILLIS. Just for my part—

Senator GILLIBRAND. Oh, sorry. Senator Hirono is on Webex. Senator Hirono.

Senator HIRONO. Hello? Thank you, Madam Chair.

Senator GILLIBRAND. We can hear you.

Senator HIRONO. This is for the panel. In Hawaii we have several cyber education programs that work collaboratively with the NSA and Department of Homeland Security (DHS), such as the National Centers of Academic Excellence in Cyber Defense and Center of Academic Excellence in Research. However, we also struggle to retain these trained cybersecurity experts in Hawaii. One thing that we find in Hawaii is that we can have a lot of excellent people who

come to Hawaii but if they do not particularly have ties to the community, they tend to cycle out.

So my first question is how is the Cyber Workforce Management Board, CWMB, collaborating with other Federal and state agencies, where relevant, to continue investments in education, particularly in STEM programs, to meet the growing need of cybersecurity professionals? Particular, probably, in a state like Hawaii, how do we go out and reach the local community to engage in these kinds of educational programs, because they are more inclined to stay in Hawaii once they get their education. Panel?

Ms. HINTON. Senator Hirono, this is Ms. Hinton. I will touch on two areas and then I will ask my colleague, Mr. Sherman, to talk a little bit about the broader interagency collaboration.

Through the Chief Human Capital Officers Council, the Federal Human Capital Officers Council, we look at these broad-reaching interagency challenges and work in partnership with the Federal Chief Information Officers Council to identify innovative programs, solutions that get to the problems that you identify specifically, whether it is retention or recruitment. We work together to identify those best practices, that if one agency has found a way to solve an issue, how do we share that across the interagency space?

We are particularly doing that as well within the national security workforce in identifying are there specific challenges associated with the recruitment and retention of, say, the cyber workforce, and how can we learn from each other.

To Hawaii, specifically, I would mention the Department's ability to retain our talent in some of our remote locations or locations where we have seen throughput, we have relied and leaned heavily on our authorities to offer incentives, to incentivize talent to stay in those locations where we need them. We have found success in using those incentive programs, but we have also found that we have to go pretty close to the cap of our authority in order to retain talent in these places. So as we use our incentives more and more, we are finding that it is taking us to that 25 percent cap, which the Department is authorized to use for these relocation and retention incentives, and we can envision a future state where we will need higher authority to compete with industry to retain individuals in these locations.

Senator HIRONO. Thank you. Anyone else want to weigh in?

Mr. SHERMAN. Senator, this is John Sherman, Acting CIO, ma'am. Just to thank Ms. Hinton, who hit many of the key points, and we are proud of the five Centers of Academic Excellence within the State of Hawaii that we are able to work with through the NSA accreditation there.

With regard to working across interagency, Ms. Hinton talked about the Federal CIO Council, where best practices are shared. We are also doing things in terms of, say, how career succession happens. We have something called the Cyber Pathways tool that we developed in concert with Department of Homeland Security (DHS) and VA, to show cyber professionals how they can work across different trade crafts, what their career path could look like, and that was a good interagency effort between VA, DHS, and the Department of Defense.

We are sharing best practices. Of course, within the Department of Defense we are very pleased to have the Cyber Excepted Service authorities you all in Congress have provided to us, and we do use those aggressively and are continuing to expand those and then share our lessons learned with some of our interagency partners. So there is an active dialogue on that, and we are trying to be forward-leaning in that regard. Thank you.

Senator HIRONO. I am glad to hear that there are efforts to work with the other departments, because there are some common challenges with regard to recruiting and retaining a cyber-educated force.

How is DOD partnering or working with universities across the country to provide a pipeline to DOD's cyber workforce? Any of the panelists.

Mr. SHERMAN. Senator, this is John Sherman again, the Acting CIO. You noted the Centers for Academic Excellence, an NSA-accredited program that we advocate for here at the Department of Defense level, across many dozens of institutions all across the country, constantly adding more to that. The neat thing about this is as schools come in, other schools can help shepherd them to get their accreditation, and it really is a truly, truly diverse grouping of schools.

I was noting a minute ago, it is everything from Tuskegee University to Honolulu Community College, from University of Missouri-Columbia to North Carolina A&T. There are many, many schools in this, and the goodness of this is bringing in the different institutions across a very diverse population—rural, urban, otherwise—to get to a broader, more diverse set of candidates and students, in places where it cannot only apply the scholarships to and get them on board through there, but to get people interested in working in the Department of Defense, who might not otherwise think about a cyber career in national security.

So this is something we are very excited about. It is an ongoing effort. It requires effort by the schools to get the accreditation. But it is very diverse, as I said, through community colleges all the way to much larger institutions, ma'am.

Senator HIRONO. I am running out of time. This may have been touched upon before, but are you making concerted efforts to recruit women and minority people?

Ms. HINTON. Senator, this is Veronica Hinton. Absolutely, and we appreciate the authorities Congress has given us, in particular around direct hiring authorities to enable us to target our recruitment to underrepresented, underserved communities. We have found that using these authorities have enabled us to expand our outreach, to go where the talent is, and to attract them into the Department.

We see that through these authorities, whether they are student direct hire authorities or general streamlined direct hire authorities that we have had results in increasing minority hires, in particular with our student authorities. As I mentioned earlier, we have, in the past fiscal year, 20 percent of our student cyber hires have been 20 percent Asian American. We have seen growth in our African American as well as our female representation.

So we really appreciate the authorities that enable us to diversify the workforce and really find where the talent pools are, to partner with minority-serving institutions and other colleges and universities to get at this issue.

Senator HIRONO. Thank you very much. Thank you, Madam Chair.

Senator GILLIBRAND. Thank you, Senator Hirono. Senator Tillis.

Senator TILLIS. Thank you, Madam Chair. I will not ask any more questions here, but Mr. Litton, I am going to offer a couple of questions for the record, particularly around the temporary promotion authority for the DDS, kind of an idea of what slots have been provided, or if none have, why not. Also on constructive credit, I think the Army is the only one that seems to be using it now. I am curious why there is a reluctance, or why it has not been implemented in the other service lines.

Mr. Sherman, I want to dig a little bit deeper, for the purposes of future considerations, the clearance issue. When we do security clearance you have got maybe a hotshot that is going to take 90 days or more to get a clearance. We had given some authority to provide, I think, unclassified workspace to onboard them. That may work, but I would like to talk more, we can talk about after the hearing, give us feedback on how we can accelerate that.

The clearance process is a problem across the whole of government, but in this particular field, where they are highly sought after resources, we can have a lot of leakage if we do not get better at it, onboard them as quickly as possible. So we will talk about that after the hearing and make sure my staff follow up.

Madam Chair, thank you for the hearing. This is very important, and again, we welcome your feedback on things that we should be looking at to either tune or introduce additional authorities to tackle this, because I tend to agree with General Crall's sobering mindset. We have got a lot of work to do here if we want to get the run right where we need it. Thank you, all.

Senator GILLIBRAND. If anybody wants to answer Senator Tillis' question now, because you know the answer, please do, because I have the same question about how do we increase the time for security clearances, how do we speed it up?

Mr. SHERMAN. I would just add, ma'am, we will need to take that for the record. As we work with the Under Secretary of Defense for Intelligence and Security and the Defense—I am sorry, DCSA; I always get backwards on that—DCSA, to make sure we have their input on that, we will take that for the record and make sure we get you a holistic answer back on that, ma'am.

Mr. SHERMAN. The Under Secretary of Defense for Intelligence and Security (USD(I&S)) is responsible for the personnel security clearance policy and processes. I understand that USD(I&S) is working in collaboration with the Office of the Director of the National Security Agency and the Office of Personnel Management on a new vetting concept, Trusted Workforce (TW) 2.0. TW 2.0 is a new framework designed to transform the Federal Government's personnel vetting process resulting in faster, less expensive investigations for the Federal Government. Additional questions regarding personnel security clearances should be referred to USD(I&S).

Senator GILLIBRAND. Thank you. Mr. Litton, in your testimony, you mentioned that the basis eligibility criteria and screening process for Military Service is the same for recruits as it is for non-cyber military occupational specialties. Are current Military Service

standards restricting our ability to fill the ranks with the cyber talent we need? If so, how do you recommend addressing this issue, and how do we balance the need for officers to possess the cyber-specific skills and knowledge necessary for their branch, but also the leadership skills necessary for them to enjoy meaningful career progression and be competitive for leadership and command opportunities?

Mr. LITTON. Yes, ma'am. Thank you for that question. Overall, recruiting, both in the enlisted and the officer corps, in general, has been very good. I think the military incident processing command has done a tremendous job during this COVID environment, keeping the Military Entrance Processing Station (MEPS) stations open and keeping that pipeline flowing for those that want to serve their country, and filling the ranks in the Military Services.

Right now our retention is really excellent. I think it has been a benefit, if you will, for the Department of this uncertain environment that we currently find ourselves in, that all the retention numbers are well over 100 percent.

So that being said, our recruiting and retention specifically for our cyber warriors is good. There are some specific areas in which we are below our needs. But generally those are because we have increased the requirements on the other end. So we are fighting on one end to bring in the right person, but also those requirements increasing on the other end make it a dual challenge, if you will.

Senator GILLIBRAND. Does anyone else want to add to that answer?

Ms. HINTON. Senator, I would echo Mr. Litton's comments. We find the same dynamic on the civilian side. Our retention rates, in particular for our cyber workforce, are generally good, and generally across the Department we see that folks are not really leaving right now, just because of the uncertain dynamic. But we find that there are pockets of challenges within the cyber workforce. In particular as we talk to Army Cyber Command and some of the very specific, very highly technical areas, we do see some churn there, that we are using in leveraging all of our authorities to close those gaps.

But there is a dearth of expertise in the country in some of these instances, and so we bring to bear what we can, but certainly we can do more.

Senator GILLIBRAND. What are the differences—maybe for Lieutenant General Crall and Mr. Sherman—what are the differences between civilian versus uniformed employees in our cyber workforce? What strategic advantages do each bring, and what percentage of current cyber workforce is civilian versus military? What do you think the proper mix should be, and how do we ensure we have the proper mix 5 years and 10 years from now?

Mr. SHERMAN. I will go on that first part about the current mix, ma'am. We have what is called the Defense Cyber Workforce Framework, where we capture this data. We have roughly, as we have got the skill sets coded, 65,000 civilians and 67,000 military in the ranks there.

In terms of the mix, I will defer to General Crall to amplify this. The military brings longer consistency, longer-term time on target there. The civilians, you may have a little bit different turnover,

and, of course, the different richness of skill set and experiences, perhaps from industry or academia or elsewhere.

My personal view, as Acting CIO, is that this is about the right mix we have now, in terms of about the half and half, to keep that modulated. Just to build on what Ms. Hinton said, we do have certain skill sets that are very applicable, as Senator Tillis was indicating at the outset, out in the civilian workforce. Cyber operators, for example, is one of the coded ones. Network assessors. Jobs that could get very quickly picked up in the private sector.

Using this framework, blocking and tackling we have, we can watch as these get above a 10 percent rate that we need to start, when the vacancies get above a certain area, that we can start amping up the hiring and using the cyber-accepted service authorities you all have granted to us to start doing things like targeted local markets, supplement TMLS for living in the National Capital region, and so on. So we try to use that to modulate, but the mix, I believe, is about right, but I will defer to General Crall and the others for their views.

General CRALL. I think in a generic sense the mix is about right the way it sits now. There are tradeoffs, and those tradeoffs, I agree with the Action CIO in that you get some consistency on the military side. People that make careers of it stick around, and they have a unique experience that relates very well to the combatant commands. Make no mistake, from the Joint Staff, focused on warfighting and looking at meeting combatant command needs, those relationships work out quite well.

What you trade, though, however, is some of the experience and currency that we tend to get from our civilian workforce, especially those who move in and out from industry back to service with us. So I would probably like to keep both of those pipelines open.

But your most difficult question that you asked was not so much how are things working out today but what does that mix look like five years. I think that is the unknown. I do not know the answer to that. But my guess is it probably will not look like it looks today, because we have not onboarded the very capabilities that we need to employ—machine learning, autonomy, artificial intelligence, a real cloud-based environment, pushing that processing to the tactical edge, and a reformed network.

So the speed with which that is going to require us to operate is going to have a level of human-machine interface we have never had before, and it is hard for me to believe that the force we are looking at today is necessarily rightly aligned to that new mission set. We are going to have to lead turn this, and keep a careful eye on what those skill sets are necessary to bring this on board, and we might have to throttle that mix and that balance to get there.

Mr. SHERMAN. I am sorry, ma'am. I was just going to add one other thing to what General Crall is saying. Absolutely, on the cloud-based capabilities, data, AI, some of the things I mentioned in my opening statement. The one thing we are going to have to get our head around is, as we do, particularly on the civilian side, bringing them in, we might not be bringing them in for 30 years. Indeed, they may come in for 4 years and go out to industry and then come back to us in 5, 6, 7, 8 years, and that is not a bad thing to stay super current with industry practices, academia, and else-

where. With our Cyber Excepted Service authorities, we are able to operate in that space, but this is a different mindset, particular with our civilians. We may not want to hire data scientists for more than 3 or 4 years. We may want them to go back to industry, reaffirm their technological bona fides, and then come back to us later. It is a different mindset we need to get around.

Senator GILLIBRAND. Go ahead, Ms. Hinton.

Ms. HINTON. We need the pathways and the pipeline to be able to do that, the authorities to be able to do that, to have the fungible workforce that gets their experience in industry, comes back into the Department, and maybe goes back out, and so—

Senator GILLIBRAND. So you are saying we do need additional authorities to do that?

Ms. HINTON. Correct.

Senator GILLIBRAND. Okay. So I would like everyone on this panel to write a letter to the committee what those authorities would look like, to have the flexibility we will need 5 years, 10 years out, to get people coming in and out of the private sector, to keep their knowledge current.

Anything else? I cut you off. Did you want to say more?

Ms. HINTON. Nothing.

Senator GILLIBRAND. Okay. Thank you. Senator Hawley.

Senator HAWLEY. Thank you, Madam Chair. Ms. Hinton, let me come back to you, if I could, and ask you a question about our friends at the big tech companies. Just give us a sense, on the committee, have they been supportive of DOD's efforts to attract cyber talent that we need to protect our national security, or are you seeing these companies counter and compete and stand in the way of DOD's recruitment efforts?

Ms. HINTON. I would not couch it in an adversarial manner—thank you for the question, Senator. Certainly we are in a competition with the big tech, but at the same time, they have also been friends to the Department. We have used the private-public talent exchange authority that Congress has given us to open up those pathways, to allow our employees to go learn from industry, and to allow industry to come learn from the Department. We are in the process of expanding that authority, based on direction in the last NDAA.

But certainly as we look at our compensation authorities and try to compete, we cannot compete based on money, quite frankly. In some areas we can—we do have some authorities—but across the board, generally we cannot win the money competition, so we win the service competition, the call to service, to serve the country. We work on some incredibly advanced opportunities, and that is where we win the universities, we win the industry.

So I would say a mix of partnership, but also a mix of competition.

Senator HAWLEY. Very good. Speaking of universities, I am curious how the Department has used scholarships or other programs for high school students and college students to attract top quality talent.

Ms. HINTON. We have a mix of programs, Senator, that we use, whether it is the Cyber Scholarship Program, whether it is the STEM Scholarship Program. We have a plethora of scholarships,

fellowships, internships, where we use that to go after talent. We are also looking at the Defense Civilian Training Corps, which is a new authority we received in the Fiscal Year 2020 NDAA, to stand up a ROTC-like program. We use our direct hire authority. We have a student direct hire authority that enables us to reach out and directly hire students into the Department. That has proven to be a successful authority, albeit with some limitations. So we have a variety of tools available to us.

Senator HAWLEY. I am curious if there are any particular regions that you have targeted or types of schools.

Ms. HINTON. We target a variety of universities, a variety of schools, depending on the mission sets that we need. We have a diverse network of partnerships with a variety of universities, a variety of outreach programs that help us find talent. Mr. Sherman, if you have some specifics?

Mr. SHERMAN. Sure. There are dozens and dozens, Senator, of schools, and we were talking about this a little bit earlier, from community colleges all the way up to University of Missouri-Columbia, to very large schools, everything from rural to urban. So we are aiming for a very broad swath of talent, to get these Centers of Academic Excellence accreditations to be able to do that.

Also, Ms. Hinton mentioned these ROTC-focused efforts we have going on. There are six institutions—Texas A&M, North Georgia, Virginia Tech, VMI, Citadel, and Norwich—all schools that have large ROTC programs, to encourage the cadets there to focus on cyber. Within some of them, for example, Citadel within the Charleston area, is reaching out to schools within the area, high schools and so on. So they are taking this kind of a step further there, as well.

So the bottom line, sir, is a pretty broad shot group there of what we are trying to go after, getting the most diverse talent and folks who may not have thought of a career at the Department of Defense or national security.

One of the things Ms. Hinton noted, if I can go to this, about why do people come to work, and it goes to the education piece. They can make more money in tech, but where else can you go after ISIS, or help us stand up against the Chinese, or thwart the Russians? There is a certain amount of, you cannot do this anywhere else. So we may get them for 4 years, maybe they go off to industry and make more money. The key is getting them back after that, for the next bite at the apple, for a higher level of management or technical capacity they would have, sir.

Senator HAWLEY. Let me ask you in, in closing, when you think about the mix of programs and recruitment tools that you have just been talking about, have any proved particularly successful or effective, that you would look at and say, "That has really been good for us"?

Ms. HINTON. Sir, I feel like a broken record, but I really am very thankful, the Department is very thankful and appreciative of the direct hire authorities, because they enable us to get through the hurdles and the inefficiencies in some of the Title 5 hiring authorities, and really get to where is the talent, how do we bring them in, how do we attract them without having to go through the overly burdensome hiring process that we had.

So they have proven to be effective tools, and I would couple that with the Cyber Excepted Service authority that we have, that we are growing, that has proven to be another effective personnel tool.

Senator HAWLEY. Very good. Thank you very much. Thank you, Madam Chair.

General CRALL. Sir, if I could offer one piece to that, not often well received, but I think important to note. Not all of our talent comes from credentialed degree holders. We have a lot of talent that comes in our enlisted forces, or maybe with no degree whatsoever, that have shown unbelievable prowess and acumen in this field. While I would never dismiss the idea of pursuing the formally trained university partnerships, which go a long way, to some of our high-end performers, we have a lot of performers who do not hold degrees, and they have proven extremely valuable to our work.

Senator HAWLEY. That is great.

Senator GILLIBRAND. Just a couple questions on our Cyber Reserve and our National Guard. In the fiscal year 2021 National Defense Authorization Act, it required leaders in the DOD to evaluate reserve models tailored to support cyberspace operations. I am interested in the possibility of creating more flexible options for personnel who want to serve but want alternatives to full-time, active-duty service. We look forward to receiving that report.

To inform our reading of it, when it comes—thank you, Senator—how is the Department currently thinking of non-traditional military reserve models for service on cyber issues? What are the current military reserve options for individuals who have cyber skills and are interested in service? Then on the National Guard question, we asked for a report to evaluate the use of National Guard for the response to and recovery from significant cyber incidents. As you conduct that evaluation, what is your long-term vision for the successful integration of the National Guard into cyber incident response, and what should the collaboration be between the National Guard Bureau and Federal agencies looking like and preparing for and establishing resilience to future cyber incidents?

Whoever wants to address it can address it.

General CRALL. I see everyone looking at me. So, ma'am, we certainly owe you the details in the reports that you had mentioned. You know, I had a chance recently, the week before last, to get up to Washington State and talk to one of their elite Guard units there on cyber. Incredibly impressive. Clearly they are not the only one—those are starting to grow, both in numbers and competency. It offers the very thing that I opened up with. People want to live where they want to live, and do the work that they want to do. I think it also gets after the comment that the Senator asked about, how do you retain that talent in the state? In your state, for example, Hawaii, that is certainly one way to get after that. It offers the financial incentives that go after that.

But nobody knows your local territory like your Guard. So if you think about, you know, election security and the infrastructure involved with that state, they know their infrastructure better than most.

So I think that there is a lot of room for both Guard and Reserves, to get after your comment on integrating, resilience, and

that additive feature that appears to be very attractive to many. I believe we need more Guard units, specifically with a cyber competency, maybe even as a standalone entity, as a specialty, would be my opinion on that.

Senator GILLIBRAND. Can you please make sure that is addressed in the report that is forthcoming?

Then just one last question for Mr. Sherman and Ms. Hinton, and maybe, again, Lieutenant General Crall. This is about the private sector and just enhancing our relationship.

Your opening statement cited the emerging practice of private industry to create a human supply chain by partnering with universities to supply a ready supply of talented and trained individuals into all our cyber forces. Should the DOD seek to establish such a reserve via partnerships like the private sector, in doing with the nation's colleges and universities, and what should that system look like? For anyone.

Ms. HINTON. The Department agrees that it needs the flexibility to more rapidly pull from a source of highly qualified candidates in the cyber career field to meet mission needs. The Department has concerns and recommendations for consideration in establishing any such system:

- A civilian cyber reserve system may be counterproductive to the Department's efforts to recruit and retain professionals in the military reserve, whose cyber mission force supports current DoD mission requirements. Such a system may also have an effect on the Department's ability to recruit career civilian employees to support enduring DoD mission requirements. Accordingly, any reserve system must be carefully explored to ensure it not only addresses gaps but also complements on-going efforts to cultivate the cyber workforce.
- Without corresponding incentive structures, as well as employer support similar to that afforded to military reserve personnel, there is not enough data to assess that cyber professionals in private industry would be attracted to short-term government work without guaranteed re-employment, retention of benefits, and future opportunities.

Mr. SHERMAN. I think we could certainly take that on board to consider how formalized that should be. As Senator Hawley was asking, I was going to pile onto one other thing there about, there is not an adversarial relationship. There is a very symbiotic relationship right now with much of industry, in terms of the tech sector and in terms of support for what we are trying to do. Now, there is high competitiveness for those very in-demand skill sets, but recognizing the national security roles, when folks come in here for a few years and then maybe go back out to industry and so on.

In terms of special authorities, ma'am, we will have to take that on board to think about that, but it would also just be us, back to the original point a few minutes ago, recognizing the permeability of folks coming in and out. Whether that requires special authorities or not, we will definitely take that on board, and whether that requires anything special, vis-à-vis industry, we would have to consider. So thank you for the question.

Ms. HINTON. Yes, ma'am. Thank you for the question. I agree with Acting CIO Sherman. We will take it for the record, to look at the authorities that we have and the authorities we may need. We have had conversations around the notion of opening up pathways for individuals to come in and out of service. You know, whether or not that translates into a civilian reserve corps of individuals to fill talent gaps is a conversation we are having right now, and we can come back to you with further information.

Senator GILLIBRAND. Thank you, everyone, for participating. Senator Tillis, do you have anything else?

Senator TILLIS. Thank you very much. We appreciate your answers to questions, and again, we will submit a few for the record. But thank you for being here. Thank you for having this hearing.

Senator GILLIBRAND. Thank you for your dedication. Adjourned. [Whereupon, at 3:53 p.m., the Subcommittee adjourned.]

