NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE

STATEMENT OF

MS. VERONICA HINTON,

ACTING DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR CIVILIAN PERSONNEL POLICY

AND

MR. LEONARD LITTON,

PERFORMING THE DUTIES OF THE DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR MILITARY PERSONNEL POLICY

BEFORE THE

SENATE ARMED SERVICES MILITARY PERSONNEL SUBCOMMITTEE

ON THE HEALTH OF THE CYBER WORKFORCE

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 FY22.

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 FY 2018 and FY 2020, the overall cyber workforce increased an average of 6 percent (FY18: 6.9 percent; FY19: 7.8 percent; FY20: 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 FY 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 FY20 and FY21, garnered a significant average decrease in time-to-hire from FY 2019 (FY19: 117 and FY20/21: 89). The Department expects to see continued decreases under the streamlined approach.

Between FY19 and FY21, 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 FY21, 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 FY 2020 at a step 2 or higher (36 percent in FY18; 39.5 percent in FY19).

Furthermore, we utilize recruitment, relocation, and retention, as well as student loan repayment incentives to better attract and retain this in-demand talent. In FY20, of the 2,143 cyber workforce hires, 30.3 percent were given a recruitment or relocation incentive, a 21 percent increase from FY19 (9.27 percent); 3.87 percent were given student loan repayment (3.1 percent in FY19); and 1.68 percent (1,058) of the total cyber workforce in FY20 were given a retention incentive (0.33 percent in FY19 (194)).

Finally, section 241 of the NDAA for FY21 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 FY21 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 excepted 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 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.