STATEMENT BY

JOHN SHERMAN

ACTING CHIEF INFORMATION OFFICER FOR DEPARTMENT OF DEFENSE

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON PERSONNEL

ON

CYBER WORKFORCE

APRIL 21, 2021

NOT FOR PUBLICATION UNTIL

RELEASED BY THE SENATE ARMED SERVICES COMMITTEE

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 FY21, 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 FY20 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.