STATEMENT BY

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

BEFORE THE
SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEES ON
CYBERSECURITY AND PERSONNEL

ON

"CYBER OPERATIONAL READINESS OF THE DEPARTMENT OF DEFENSE"

SEPTEMBER 26, 2018

NOT FOR PUBLICATION UNTIL
RELEASED BY THE SENATE ARMED SERVICES COMMITTEE

Introduction

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

Department of Defense Cyber Workforce Overview

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

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

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

analysts, and system test and evaluators. Specific to the Cyber Mission Forces, their personnel needs center on planning, coding, forensics, malware, data science, linguists, and cybersecurity professionals.

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

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

Cyber Excepted Service (CES) Personnel System

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

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

Conclusion

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