STATEMENT OF

BRIGADIER GENERAL DENNIS A. CRALL,

U.S. MARINE CORPS,

SENIOR MILITARY ADVISOR FOR CYBER POLICY AND

DEPUTY PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

SENATE ARMED SERVICES COMMITTEE

CYBERSECURITY SUBCOMMITTEE

PERSONNEL SUBCOMMITTEE

SEPTEMBER 26, 2018

Thank you Chairman Rounds, Ranking Member Nelson, and Members of the Cybersecurity Subcommittee, and Chairman Tillis, Ranking Member Gillibrand, and Members of the Personnel Subcommittee. It is an honor to appear before you to discuss cyber operational readiness within the Department of Defense (DoD). I appear before you today in my roles as the Senior Military Advisor for Cyber Policy and the Deputy Principal Cyber Advisor to the Secretary of Defense.

As described in Section 932 of the National Defense Authorization Act for Fiscal Year 2014, the Principal Cyber Advisor (PCA) serves as the civilian DoD official who acts as the principal advisor to the Secretary of Defense on the Department's military and civilian cyber forces and activities. The Office of the PCA (OPCA) synchronizes, coordinates, and oversees the implementation of the Department's Cyber Strategy and other relevant policy and planning documents to achieve DoD's cyber missions, goals, and objectives. At the core of the OPCA is the Cross Functional Team (CFT) of detailed personnel from key departments, services, and agencies. The CFT provides an objective and broad perspective needed to ensure outcomes match both short- and long-term approved, strategic visions. To meet increasing demands outlined in the DoD Cyber Strategy Lines of Effort (LOE) and the DoD Cyber Posture Review's gap analysis, the Deputy Secretary of Defense has made a substantial investment in the OPCA, adding permanent billets including an OPCA Deputy for long-term continuity.

Achieving the DoD Cyber Strategy's five main tenets, one of which is to "cultivate talent," requires an unmatched, professional cyber workforce. Accordingly, this workforce is listed in the Department's "Top 10 Cyber Priorities" and falls within the "First Four" mitigation endeavors already underway. The main workforce governance body, the Cyber Workforce Management

Board (CWMB), was chartered to manage the health, welfare, and maturity of the Department's military and civilian cyberspace cadre and to oversee and assess the use and reliance of contract services in support of that workforce. This decision-making body provides recommendations to the appropriate implementation authorities for cyber workforce determinations related to standards, requirements, personnel systems, qualifications, training, and compliance. Additionally, the CWMB manages the Department's Cyber Workforce Framework: a standardized structure that provides a lexicon of work roles, tasks, knowledge, skills, and abilities to support the development of the common cyber workforce qualification standards for the cyber workforce. The CWMB outputs are fed into the OPCA-led LOE process where implementation actions are coordinated with other enterprise activities.

The Department is pursuing an enterprise approach to recruit, retain, develop, and train cyber professionals, with each detailed below. The focus of my testimony is on the civilian Federal workforce, as I defer to my U.S. Cyber Command colleagues to address uniformed service member's endeavors.

Recruit. The competition between the private and public sectors for high-demand / low-density cyber expertise continues to grow. The military and civilian Federal workforces maintain unique advantages not available in the private sector such as service to the Nation; ability to execute unique, online missions; and exposure to a wide array of new, disparate technology. The Department must continue to seek opportunities to reduce pay disparities between the Federal and private sectors to aid in increasing government service as a viable, sustainable option. Of course, these benefits are only useful to attract top talent if they are widely known, and the Department can do better to ensure we understand and pursue our target, cyber audience. We are currently exploring more focused cyber recruiting for the Federal workforce; increased internships with industry and academia; and greater advertising exposure, to name a few.

Retain. The Department has implemented many changes, with others in-the-making, to preserve our valued cyber teammates. For Federal workers, the establishment of the Cyber Excepted Service (CES) provision is showing initial promise. The CES benefits include non-competitive movement between the CES and Competitive Service across the CES-designated organization; performance-based advancement opportunities (not limited to time-in-grade); and an increased General Schedule step scale (with advancement and job offers up to GS step 12).

Already approved and now in planning are targeted market supplements for high-cost / high-demand regions across the Department; retention bonuses that are immune from current pay caps; and expedited security clearance processing for the timely availability of qualified military, civilian, and contractor cyber personnel.

Phase I of the CES roll-out was a modest implementation with the conversion of 251 employees at U.S. Cyber Command, Joint Force Headquarters – Department of Defense Information Network, and the Office of the Department of Defense Chief Information Officer. The Phase II implementation will be a partnership with Department Components for the conversion of 8,305 CES positions at the Defense Information Systems Agency and the Service Cyber Components. The Department anticipates that as many as ten thousand professionals will take advantage of the CES once the phased implementation is complete and all program attributes are fully functional.

Develop. The CES will establish a Cyber Career Management Program to provide a roadmap for a variety of career paths. Key provisions will strengthen relationships with academia, industry, and private institutions for increased cyber education and internship opportunities as well as provide future rotational assignments across the Department's cyber community.

Train. The Department recently concluded the civilian cyber work role coding effort designed to record a common, skill-set designator across the enterprise for the military and civilian Federal workforces. Once shared in a common, federated repository, this data will allow visibility of available, cyber-skilled professionals; training progression; and readiness investment opportunities. Additionally, a common-core curriculum is under development to ensure baselined and advanced trained personnel are developed equally throughout the Department. These critical CES initiatives will support the Department's efforts to enhance the quality of cyber training and education, which is an objective within the Department's Cyber Strategy LOE.

The Department is committed to building and sustaining a cyber-ready workforce as defined in our Cyber Strategy. We will achieve cyber operational readiness and lethality by recruiting, developing, and managing critical cyber talent. To that end, I will continue to partner across the Department as an advocate to integrate and oversee the development of cyberspace capabilities, activities, and policies within the cyber workforce arena and cyber-related initiatives. I am grateful for Congress's strong support for the Department of Defense in building the cyber forces needed to be lethal and to deter in cyberspace. I thank the Subcommittee for its interest in these issues, and I look forward to your questions.