STATEMENT BY

LIEUTENANT GENERAL DENNIS A. CRALL,

UNITED STATES MARINE CORPS

JOINT STAFF DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS AND

COMPUTERS/ CYBER, CHIEF INFORMATION OFFICER

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NOT FOR PUBLICATION UNTIL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

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 (FY) 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 FY 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 FY 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 FY 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. Participating 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.