RECORD VERSION

STATEMENT BY
LIEUTENANT GENERAL STEPHEN G. FOGARTY
COMMANDER, UNITED STATES ARMY CYBER COMMAND

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

SECOND SESSION, 117TH CONGRESS

ON TRAINING THE NEXT GENERATION OF CYBER OPERATORS

APRIL 5, 2022

NOT FOR PUBLICATION UNTIL RELEASED BY THE COMMITTEE ON ARMED SERVICES

Chairman Manchin, Ranking Member Rounds, and Members of the Subcommittee, thank you for the opportunity to testify today and for your continued support of the dedicated Soldiers and Army Civilians of U.S. Army Cyber Command (ARCYBER) and the entire Army Cyber Enterprise. It is a distinct privilege and honor to represent the Army Cyber Team alongside members of U.S. Cyber Command (CYBERCOM) and my colleagues from across the Department of Defense (DoD), to discuss the Army's contribution to CYBERCOM's Cyber Mission Force (CMF) readiness.

Establishing Army Cyber Command

ARCYBER performs four primary functions: (1) build, operate, and maintain Army networks; (2) defend Army and joint networks, data and weapons systems; (3) execute cyber and electronic warfare attacks against our adversaries; and (4) conduct influence operations. The Army's cyber workforce is comprised of Active Duty, Army Reserve, and Army National Guard Soldiers, Department of the Army (DA) Civilians and contractors. ARCYBER executes the Nation's high-end offensive and defensive missions in cyberspace through our approximately twenty-eight hundred skilled Soldiers and civilians assigned to the CMF.

In 2010, the Army activated ARCYBER at Fort Belvoir, Virginia to serve as the Army Service Cyber Component to CYBERCOM and the Army Service Command for Cyber supporting the Army's cyber requirements. The DoD created the CMF under Cyber Command in 2012 and the Army immediately started the task of organizing, training, and equipping its share of the force to the CYBERCOM directed standard as part of the CMF Build-Assess-Build Methodology. At that time, ARCYBER was spread across three military installations and twelve different facilities in Fort Belvoir, Virginia, Fort Meade, Maryland, and Fort Gordon, Georgia. In 2013, Army leadership directed ARCYBER to move and consolidate the headquarters at Fort Gordon, soon to be the nexus for Army cyber operations, capability development, training, and education.

Maturing Army Cyber Command

Recognizing the advantages of a dedicated cyber force, the Army established the Cyber Branch and the Cyber Center of Excellence in 2014. By the end of 2017, all active component Army Cyber teams assigned to the CMF were declared to be at full operating capacity, a year

ahead of schedule. During this period, ARCYBER and its respective subordinate organizations continually evolved to optimize organizational design, training, and processes as a function of Army lessons learned and CYBERCOM lessons learned within the first CMF Assess phase.

In 2020, following the CYBERCOM formal Combatant Command Review, the Secretary of Defense designated the Secretary of the Army as the DoD Executive Agent for Advanced Cyber Training. Through this designation, the Army's Cyber Center of Excellence initiated a number of activities designed to optimize CMF training solutions and increase available combat power in our most critical areas.

Also in 2020, CYBERCOM, in its Joint Force Trainer role, initiated the CYBERCOM Force Generation process. In partnership with the Army Cyber Center of Excellence and others, CYBERCOM has driven a series of outcomes aimed at better training, certifying, and retaining our fighting force.

Through 2021 and 2022, CYBERCOM improved its ability to act against our adversaries in competition, crisis, and conflict in cyberspace by maturing the Joint Cyber Warfighting Architecture (JCWA) construct. The Army is the acquisition lead for the Joint Common Access Platform and the Persistent Cyber Training Environment (PCTE), which are critical operations and training components for JCWA.

Army Cyber Command Current Readiness

CYBERCOM and ARCYBER's readiness provides the foundation of success for all cyber operations. Although the Army contribution to the CMF continues to improve, we currently do not meet all readiness metrics. Achieving readiness requires a joint certified workforce, an operational infrastructure, and continuous training. ARCYBER recognizes readiness, and mission success, is directly tied to our ability to recruit, develop, employ, and then retain world-class people, including Soldiers across all components and Army Civilians. Within this framework of recruitment, development, employment, and retention, we consistently and successfully recruit the quality workforce we require. Our enlisted Soldiers possess the highest Armed Services Vocational Aptitude Battery scores in the Army. The Cyber Branch uses all available commissioning sources, including the United States Military Academy at West Point, the Reserve Officers' Training Corps, Officer Candidate School, and leverages the fiscal year (FY) 2019 National Defense Authorization Act (NDAA) direct commissioning

authorities. ARCYBER attracts talented cadets from highly rated universities across the Nation, as well as interested candidates who would like to participate in the direct commissioning program. The direct commission authorities provided by the FY 2019 NDAA enables ARCYBER to attract individuals possessing a wide variety of highly technical skills from the commercial sector. Our skilled DA Civilians add necessary experience and continuity to the mission; however, highly technical positions experience a high rate of workforce turnover.

The Army's number one readiness challenge is retaining a sufficient portion of our military and civilian workforce. ARCYBER, like the rest of the Joint Force, faces significant retention challenges, as private industry and other Federal agencies aggressively compete for our cyber talent. ARCYBER actively uses the entire array of authorities provided by Congress to address these retention challenges—authorities for which we are grateful and appreciative. We are recognizing the achievements of our top performing officers through brevet and merit-based promotions, as authorized in the FY 2019 NDAA.

The number of personnel operating in our most critical work roles remain insufficient to meet demand. These cyberspace operators, exploitation analysts, and capability developers primarily generate our tactical outcomes. We recognize that the most impactful action to improve our readiness is to increase the throughput for personnel trained to fill our most critical work roles. We have requested CYBERCOM commit to increasing cyber operator and exploitation analyst training billets during 2022-2024 to increase our capacity. We currently generate the required number of capability developers to meet our CMF requirements. We remain jointly committed to hosting, funding, and filling all necessary training courses to ensure we meet readiness targets as soon as possible.

Training alone is not the complete answer. Members in our critical work roles must also complete an extensive qualification process to conduct operations. The Army leads the effort to grow the PCTE which enables the CMF to close this gap through operational simulation. The PCTE gives CYBERCOM the ability to certify more cyber personnel, in more scenarios, and faster than at any previous point. PCTE supports individual work role certification and also functions as the system for collective unit-of-action training and certification. This simulation capability promises to have significant positive impact on readiness going forward.

To retain proficient Soldiers, ARCYBER employs incentive payments and bonuses such as Cyber Assignment Incentive Pay, Special Duty Assignment Pay, Warrant Officer retention

bonus, and tiered Selective Retention bonuses. Retention incentives, both monetary and non-monetary (such as bonuses, Training with Industry and Advanced Civil Schooling) provide options for local commanders to keep talent within the Army.

The Army will implement Cyber Excepted Service (CES) this fiscal year. CES will help the Army reduce the compensation gap with the private sector, thereby improving hiring and retention of Department of the Army Civilians, especially with Targeted Local Market Supplements. ARCYBER additionally uses recruitment bonuses, student loan repayment options, academic degree funding, superior qualifications or special salary rate, relocation incentives, and retention bonuses as incentives to recruit and retain the approximately five hundred DA Civilians assigned to support the CMF.

ARCYBER recognizes 21st Century talent management requires successful formations to be data driven, learning organizations. We have conducted multiple studies on our Army Cyber recruitment and retention challenges. These studies have helped shape our incentive and retention focus for military and civilian personnel, while also enabling the command to see ourselves better. To ensure we have a current picture of the cyber workforce landscape, the Army has commissioned a RAND study titled “Recruitment, Career Path Development, and Retention for Cyber Operations” to identify Army-centric answers that help identify our core issues, and provide additional guidance on the direction of future recruitment, development, employment, and retention efforts.

Current events demonstrate the imperative for a mission-ready CMF. Our Soldiers and Civilians are currently surging to support urgent operational requirements beyond our normal OPTEMPO. Fortunately, we can reach into robust defensive and offensive capabilities provided by our Army Reserve and Army National Guard teammates. This Total Army approach is critical to our success. Over 50 percent of the Army’s defensive mission teams are in the Reserve and National Guard Components, and these teams meet the same CYBERCOM joint certification as their active counterparts. Our reserve component Soldiers often bring a wealth of expertise gained in civilian life to our mission. They are true force multipliers.

The Cyber Center of Excellence training pipeline is strong, and continues to provide the required amount of forces for the CMF. The consistent ability to provide trained and capable personnel is a critical enabler in the evolution of the CMF. The total growth of Army Cyber

Branch Soldiers has resulted in greater than 500 percent increase in students at the Army Cyber School from FY 2017 to FY 2022.

Conclusion

Thank you, again, for the invitation to appear before the Subcommittee to discuss CMF readiness. Your support to the entire Army Enterprise allows us to remain ready for the daily operation and defense of our networks, to conduct offensive operations in support of national defense, and to support Army and Joint forces globally. The opportunities available to Army Cyber Command have not slowed since our inception and I am confident that the character and competence of our Army Soldiers and Civilians will continue to make a significant impact on the security of our Nation.