RECORD VERSION

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

BEFORE THE

SUBCOMMITTEES ON CYBERSECURITY AND PERSONNEL
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

SECOND SESSION, 115TH CONGRESS

CYBER OPERATIONAL READINESS

SEPTEMBER 26, 2018

NOT FOR PUBLICATION UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Chairman Rounds, Chairman Tillis; Ranking Members Nelson and Gillibrand; and Members of the Subcommittees on Cybersecurity and Personnel, thank you 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's an honor to represent the Army's Cyber Team, alongside my colleagues from the Department of Defense and U.S. Cyber Command, to discuss the critical issues associated with sustaining a ready Cyber Mission Force (CMF). My testimony addresses the following topics as requested by the Subcommittees: retaining and maintaining the Army's cyber talent; individual and unit level training of the Army's CMF; integration of the Army's Reserve Component into the CMF; and the development of the National Cyber Range Complex and Persistent Training Environment.

Retaining and Maintaining the Army's Cyber Talent

Army Cyber Command's mission success rests with recruiting, retaining, and rewarding talented people, and as such we put tremendous focus on talent management. Thanks to congressional support, Army talent management initiatives continue to show increased results in civilian hiring and military recruiting. The Army is on pace to man, train, and equip Total Army cyber forces to meet current and future threats. Readiness of the total force requires that our investments in cyber ensure that Active and Reserve forces are trained and equipped to one joint standard. We have established innovative and tech-centric recruiting cells; are exercising our direct hiring authority for cyber professionals supported by FY2017 National Defense Authorization Act; and using internships, scholarship programs, and talent management initiatives focused on attracting, employing, developing and retaining technical people, including our Cyber Officer Direct Commissioning Pilot supported by FY2017 National Defense Authorization Act. The first two 1st Lieutenants under the Direct Commissioning Program are now training and we are assessing the next accessions from hundreds of applicants. With the expanded constructive service credit (up to O6 (Colonel) level) included in the FY2019 National Defense Authorization Act, we intend to attract candidates from a wider pool of applicants in the coming months.

To help the Army resolve some of our toughest talent management and technical challenges, we have partnered with the Pentagon's Defense Digital Service (DDS) to bring technically-gifted Soldiers together with interns and top private sector civilian talent to rapidly develop immediate-need cyber capabilities. We have also partnered with DDS on a Civilian Hiring as a Service Pilot to streamline the hiring process for technical talent and better leverage hiring authorities and incentives. We are working with DDS and the State of Georgia to expand this program to Fort Gordon and the region surrounding Augusta, Georgia, the Army's center of gravity for cyber operations and training. This innovative partnership is solving problems and serving as a powerful retention and recruitment tool. Additionally, in partnership with DDS, ARCYBER and the Cyber Center of Excellence launched a training pilot in January 2018 to compress and streamline joint cyber training courses.

Individual and Unit Level Training of the Army Cyber Mission Force

The Army's philosophy for training is to "Train as you fight!" For the Army's teams within the DoD's Cyber Mission Force (CMF), training to a joint standard is predicated on a culture of adaptive learning, where operations inform training at every level. A "train as you fight" philosophy in cyberspace also depends on employing realistic, dynamic, and complex cyber range environments against simulated peer and near-peer adaptive adversaries. Cyber Mission Force training is tough, realistic, relevant, and holistic.

With the achievement of Full Operational Capability of the Army CMF, the Army and Joint Force are shifting focus to measuring and sustaining CMF readiness. Readiness of the CMF's ability to conduct cyberspace operations reflects a teams' ability to plan; develop access; report and maneuver in cyberspace; hold targets at risk; and deliver capabilities based on assigned missions; this is the standard we use for training. This includes a focus on non-standard access methodologies, Title 10 operator training, and integration with mission partners to improve mission readiness.

The readiness of our defensive teams is tested daily, during remediation of routine incidents; proactive defensive cyberspace operations; and during contingency operations. Training programs must constantly sharpen our edge to adapt faster than

our adversaries. Mission rehearsals, simulating complex conditions, are necessary to ensure sufficient procedures are in place, while real-world operations grow our understanding of our adversaries' capabilities and add a decisive edge to our collective training.

The Army's Cyber Protection Brigade has taken the lead in Cyber Protection Team (CPT) training by developing a concise training manual, known as "Cyber Gunnery Tables," that defines the tasks individuals, crews, and mission elements must master. These tables provide foundational training for individuals and teams and serve as training and readiness validation events, certifying that a crew has the required knowledge, skills, and abilities to participate in collective exercises as part of a mission element. They also provide a metrics-based assessment to determine individual and crew readiness.

The Army's Cyber Electro-Magnetic Activities Support to Corps and Below (CSCB) initiative provides another venue to improve team readiness levels. Teams are integrated into the Combat Training Center rotations, War Fighter Exercises, and senior leader developmental exercises and events that train and challenge supported units and keep teams proficient on individual and collective skills. Army Cyber Command has built real-time reach-back links between Corps and Below level forces at the National Training Center and cyber operators at Fort Meade, Maryland and Fort Gordon, Georgia, that further enhance training capabilities for the Army's Brigade Combat Teams as well as our cyber forces. Based on lessons learned from the CSCB initiative, the Army will start building a Cyber Warfare Support Battalion (CWSB) in FY2019, dedicated to integrating tactical operations with strategic cyber capabilities, and supporting Electronic Warfare and cyber planning and integration.

Training is critical for operators and teams, but the CMF also needs infrastructure, tool development, and mission alignment of these ready teams. In 2017 the Army completed the second of two joint mission operations centers for offensive cyberspace operations, located at Forts Meade and Gordon. The Army has also established tool development workspaces at three locations and aligned talented personnel to innovate the creation of these in-house tools. To support this effort, the Army is developing a sustainable career map for tool developer Officers and Warrant

Officers.

The Army is also leading the way with broadly-scaled multi-domain exercises for the Active, Reserve, and National Guard components. These exercises take place at existing CTCs and purpose-built environments like Muscatatuck, Indiana's "Cybertropolis" facility. In September, 2018 the Army exercise "Cyber Blitz" based out of Joint Base McGuire-Dix-Lakehurst, New Jersey will allow Total Army forces to synchronize new technologies and define how the information warfare capabilities can be employed in the Multi-Domain fight. Specifically, the Army is looking at how Cyber Operations, Information Operations and Electronic Warfare can be synchronized with maneuver warfare and precision fires to bring effects to bear against adversaries.

The Army's Investment in Fort Gordon, GA as a Power Projection Platform

Thanks to congressional support and over $1 billion in cumulative construction and modernization projects, Fort Gordon, Georgia will be the Army's focal point for cyberspace operations and training for responsive and enhanced support to the Army and the Joint forces. The ARCYBER headquarters will relocate to Fort Gordon beginning in 2020. The new purpose-built, modern headquarters will support more than 1,300 new cyber Soldiers and civilian employees at Fort Gordon, is projected to be ready for occupation in summer 2020 and fully operational by 2022. The co-location of Army cyber operational and institutional forces will enable collaboration, flow of instructors, and speed up requirements development and acquisition.

Additionally, the transformative modernization project of the Army Cyber Center of Excellence (Cyber CoE) at Fort Gordon will break ground in fiscal year 2019. This will increase training capacity and provide modern training and workspaces to gain efficiencies across the installation. The Cyber CoE continues to make significant progress growing the cyber, electronic warfare and signal workforce. The Cyber CoE is the Army's principal organization for future cyberspace, EW and signal innovation, providing capability through concepts, design and experimentation, across Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and

Policy. In addition to training, the Cyber CoE provides force modernization, capabilities and career management for Signal, Cyber and Electronic Warfare forces.

The Cyber CoE trained over 13,000 students in fiscal year 2018. This includes students from the Cyber School, Signal School and the Non-commissioned Officer Academy. The Cyber School trains officers, warrant officers, and enlisted Soldiers from all three force components (Active, Guard, and Reserve), provides training across the joint forces, and offers two industry certifications tied to training.

The Signal School provides trained Soldiers to the operational force to conduct Department of Defense Information Network (DODIN) operations and cybersecurity, training 17 military occupational specialties and providing 42 industry certifications tied to training. Signal Soldiers install, operate, and maintain the Army's portion of the DODIN. The Signal School provides a common foundation in networking fundamentals in support of DODIN Operations to all new Signal Soldiers.

Integration of the Army's Reserve Component into the CMF

The Reserve Component (RC) is approved to build and maintain 21 CPTs; 11 in the Army National Guard (ARNG) and 10 in the U.S. Army Reserve (USAR). One ARNG and two USAR CPTs have already achieved Initial Operational Capability, the ARNG is scheduled to have all 11 CPTs at Full Operational Capability (FOC) by FY22, and the USAR's 10 CPTs will be FOC by FY24; trained and equipped to the same standards as the Active Component.

Beyond the build of these teams, Soldiers from the Army's Reserve and National Guard are trained, ready, and on-mission today, performing critical and unique support and effects-delivery roles for Army and Joint cyber missions. The 91st Cyber Brigade was initiated in September, 2017, as the Army National Guard's first cyber brigade. In August, 2017, the all-National Guard Task Force Echo was launched to engineer, install, operate, and maintain critical networks for U.S. Cyber Command.

Our RC cyber Soldiers bring critical skills that are a force multiplier. Continued support from Congress for programs to attract Soldiers, such as Direct Commissions,

Special Duty and Assignment Pay, and Cyber Affiliation Bonuses will assist in recruiting and retaining RC cyber talent.

The National Cyber Range Complex and Persistent Cyber Training Environment

Currently, DoD operates four Cyber Training and Test Ranges: the DoD Cyber Security Range; the Joint Information Operations Range; the National Cyber Range Complex; and the C5 Assessments Division range. The Persistent Cyber Training Environment (PCTE) is a material solution that provides the total cyber force a training platform to conduct joint training (including exercises and mission rehearsals), experimentation, certification, as well as the assessment and development of cyber capabilities and tactics, techniques, and procedures for missions that cross boundaries and networks. PCTE will use resources from all four of the DoD ranges, as well as resources from other existing cyber training facilities.

Headquarters, Department of the Army is the DoD's Executive Agent for Cyber Training Ranges, a responsibility led by the Army's Deputy Chief of Staff, G- 3/5/7. Army Cyber Command is in support as a primary advisor to the G- 3/5/7, with the Army's Program Executive Office for Simulation, Training, and Instrumentation (PEO-STRI) serving as the lead for acquisition, prototyping, and deployment of PCTE. The entire PCTE effort is governed by a board that includes Army Cyber Command, the DoD's Principal Cyber Advisor, and the Undersecretaries of Defense for Personnel & Readiness and Acquisition, Technology, & Logistics, as well as U.S. Cyber Command's J7, through which the Joint Cyber Service Components take part in shaping the PCTE to meet current joint operational needs.

The PCTE v1.0 prototype was delivered 31 July 2018, just one year after the Army received initial funding for the project, and is currently undergoing limited user assessment, with feedback informing the next prototype, PCTE v2.0. Follow-on capability drops are projected to occur every six months (v2.0 in January 2019; v3.0 in July 2019; etc.). To meet the requirements for individual and lower-level collective training, the Army is also using a commercially available cyber range product. To meet higher collective training tasks, the Army is evaluating another commercial platform used by the U.S. Navy, which provides a broader collective training environment. All

Services are currently using, or considering, both platforms to meet training requirements. These tools will be a bridging effort until the PCTE is fully operational.

Conclusion

Thank you again for inviting me to appear before you today representing the Army Cyber Enterprise. Your support has been enormously important to the maturation of Army Cyber Command, the Army Cyber Enterprise, and the critical mission our dedicated and talented Soldiers and Army Civilians conduct for the Army and the Nation. The Army Cyber Enterprise has made tremendous progress during the last eight years—building a cyber branch, schoolhouse, cyber infrastructure, and a Total Army cyber force. Although much remains to be done, I am confident that with your sustained support we will continue to make progress and achieve mission success. The tasks before us are great, however the talent and drive of our people is greater.