READINESS STATEMENT OF

MAJOR GENERAL KEVIN KENNEDY

CHIEF OF OPERATIONS, UNITED STATES CYBER COMMAND

BEFORE THE 117TH CONGRESS

SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE FOR CYBER SECURITY

APRIL 05, 2022

Chairman Manchin, Ranking Member Rounds, and Members of the Subcommittee, thank you for allowing me to appear before you today and to represent the men and women of United States Cyber Command (USCYBERCOM). Thank you for your continued support. I am honored to represent the Cyber Force today alongside my colleagues from across the Department of Defense to discuss General Nakasone's number one priority, the readiness of the Cyber Mission Force (CMF).

*Establishing the Cyber Mission Force*

In 2012 the Department of Defense (DoD) authorized the creation of the CMF, with 133 teams sourced from the Army, Navy, Air Force, and Marines. In 2016 USCYBERCOM declared all CMF teams attained initial operating capability (IOC), though they would not reach full operating capability until 2018. In 2016, Congress authorized the Cyber Excepted Service (CES), which was implemented in 2018 and allowed for flexible hiring authorities in filling civilian vacancies and recruiting top cyber talent. Also in 2018, USCYBERCOM declared our 133 teams fully operationally capable (FOC), thus satisfying the final requirement for elevation to a unified combatant command and assumption of Unified Command Plan Joint Force Provider and Joint Force Trainer Responsibilities.

Building the metrics and systems to measure and track readiness has been an evolving process. The CMF was fielded using a *Build-Assess-Build* methodology, with the initial *Build* phase occurring from 2012 to 2018. During this period, our teams were first stood up and measured against readiness metrics aimed at determining progress towards IOC and FOC. Services reported using non-standardized systems and metrics, which made comparison between Services a challenge.

After reaching FOC, Commander USCYBERCOM directed the *Assess* phase, with the objective of improving readiness standardization across the force. Additionally, the *Assess* phase analyzed optimum team design, force structure, and employment strategy. The *Assess* phase concluded in 2019, leading to three Deputy Secretary of Defense Memorandums from 2019-2021 establishing our current metrics. The second *Build* phase focused on implementing our newly-approved readiness standards and force design across our components.

Today we have implemented unit-of-action level metrics across all five CMF Team types, encompassing both our offensive and defensive mission areas. The Defense Readiness Reporting System (DRRS) is the standard Service team-level reporting system, where Services report against a combination of USCYBERCOM-directed and Service-owned measures. USCYBERCOM also measures readiness at the unit-of-action level.

*Maturing the Cyber Mission Force*

In 2019, the Secretary of Defense approved the Cyberspace Operations Forces (COF) concept, which created a clear definition of the forces belonging to USCYBERCOM. The COF Memorandum provides USCYBERCOM with the authority to measure and report readiness for all forces defined as USCYBERCOM COF.

In 2020, following our 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 has initiated a number of activities designed to optimize CMF training solutions and increase available combat power in our most critical areas.

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

Through 2021 and 2022, USCYBERCOM improved our ability to act against our adversaries in competition, crisis, and conflict in cyberspace by maturing our Joint Cyber Warfighting Architecture (JCWA) construct. When fully realized, JCWA will deliver unified capabilities for the COF, integrating the data from offensive and defensive cyberspace operations in ways that help commanders gauge risk, make timely decisions, and act. Additionally, JCWA's training capability, the Persistent Cyber Training Environment (PCTE), will be the way we certify our operators to conduct missions going forward.

As part of the FY22 NDAA, Enhanced Budgetary Control (EBC) is expected to provide more opportunity, responsibility, and flexibility for training and equipping our force. This mandate will begin in FY24, and will positively impacts military and civilian members of the workforce.

Military Services will retain their Program Executive Officer (PEO) role for JCWA capabilities following EBC's implementation. This includes acquisition authority. The Army will maintain their PEO role for PCTE and our Joint Common Access Platforms, while the Air Force will maintain their role in Unified Platform and Joint Cyber Command and Control (JCC2). Fielding JCWA will remain a shared responsibility going forward.

*USCYBERCOM Current Readiness*

As I stated in my March 8th testimony, the CMF's readiness remains the Command's number one priority. Both offensive and defensive readiness are foundational to the success of operations in defense of the nation and Integrated Deterrence. In recent years, USCYBERCOM has made significant strides in multiple key areas, however readiness remains insufficient to meet all of the responsibilities assigned to us through the National Defense Strategy and National Military Strategy.

The number of fully trained and qualified personnel in critical work rolls remains our biggest challenge. These cyberspace operators, exploitation analysts, and cyber capability developers comprise the units of action that generate our tactical outcomes. We recognize that the most impactful action to improve our readiness is to increase the number of personnel trained to operate in our most critical work roles. As such, we have asked our components to commit to increasing CMF fill rates where required. In support, we have initiated a training surge in 2021

and 2022 to increase our ability to train these individuals. USCYBERCOM and our components remain jointly committed to maximizing hosting, funding, and filling all necessary training courses to ensure we meet readiness targets in the future.

Training alone is not the complete answer. Members in our critical work roles must also complete an extensive qualification process in order to operate. Our efforts to grow the Persistent Cyber Training Environment (PCTE) are where we begin to close this gap through operational simulation. The PCTE gives USCYBERCOM the ability to certify more cyber personnel, in more scenarios, and faster than at any previous point. PCTE goes beyond 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.

Finally, USCYBERCOM and our components agree that, in order to maximize the benefits for the CMF, we must increase our collective efforts and cooperation aimed at retaining our talent, including our civilian workforce. Each component has initiated multiple efforts to attract and retain top cyber talent, and USCYBERCOM has engaged at the Office of the Secretary of Defense-level to provide advocacy and support.

*Conclusion*

Thank you for the invitation to address the committee and represent the men and women of United States Cyber Command. I welcome the committee's continued support as we drive our readiness to the levels required to comprehensively meet our assigned mission sin support of the National Military Strategy.