WRITTEN TESTIMONY OF THE HONORABLE KATHERINE E. SUTTON

ASSISTANT SECRETARY OF WAR FOR CYBER POLICY

BEFORE THE

SENATE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY

January 28, 2026

SUBJECT: CYBERCOM 2.0

Introduction

Chairman Rounds, Ranking Member Rosen, and distinguished members of the Subcommittee, it is an honor to appear before you today. I am grateful for the opportunity to discuss the Department of War's comprehensive efforts to organize, train, and equip our cyber forces to meet the complex challenges of the 21st-Century strategic landscape. The subject of today's hearing, CYBERCOM 2.0, represents the most significant transformation of U.S. Cyber Command (USCYBERCOM) since its inception over 15 years ago and is a cornerstone of the Department of War's strategy to ensure American dominance in the cyberspace domain.

The Strategic Imperative and the Challenge We Face

For several years, the Department has recognized that our approach to building cyber talent has not been keeping pace with the rapidly evolving and increasingly contested cyberspace domain. Our adversaries are investing heavily in cyber capabilities and building forces designed to operate in this domain. Meanwhile, we have been constrained by traditional Military Service (Service) models which, while effective for conventional forces, fail to fully address the unique requirements of cyberspace operations.

This misalignment has created significant challenges for the Department in recruiting the right people with the right aptitude and skillsets, retaining our most skilled and experienced operators in the face of lucrative private-sector opportunities, and providing the hyper-specialized, agile training needed to win against our nation's adversaries. The result has been a force-generation model that hinders our agility to adapt to evolving threats, like Volt Typhoon and Salt Typhoon, and emerging technologies like artificial intelligence and cloud computing. To secure the nation's interests, we must have a cyber force equipped to operate with precision, agility, and lethality. CYBERCOM 2.0 is the vehicle for achieving that vision.

CYBERCOM 2.0: A Fundamental Reimagining of Force Generation

To address these systemic challenges, the Secretary of War approved CYBERCOM 2.0, a fundamental reimagining of how the Department builds and manages our cyber forces. This initiative is not merely an incremental adjustment, but a deliberate and comprehensive overhaul designed to deliver greater operational outcomes for the Joint Force. CYBERCOM 2.0

efficiently synchronizes Commander, USCYBERCOM's authorities, as provided in Title 10, U.S. Code, section 167b (10 U.S.C. § 167b), with the authorities and activities of the Military Departments. At its core, CYBERCOM 2.0 is founded on three fundamental principles that will drive the Department's cyber forces for years to come.

1. Domain Mastery: The Department is fundamentally shifting away from the traditional military rotational assignments to one that fosters deep, career-long expertise. Our objective is to cultivate a cadre of cyber professionals who achieve true mastery in specific areas of cyberspace, rather than rotating through cyber assignments as generalists. This approach builds a cyber force better capable of addressing emerging threats, such as exploitation of industrial control systems in critical infrastructure or cyberattacks automated by artificial intelligence. CYBERCOM 2.0 enables increased influence by the Commander, USCYBERCOM, in the talent management of our cyber forces. Instead of cyber operators rotating out after a basic qualification, they will have a career path that allows for extended tours in the Cyber Mission Force (CMF), followed by an assignment with a Service cyber unit to broaden their experience and bring their deep expertise back to their Service formations. This model cultivates experts who possess a deep portfolio of experience in specific, mission-critical areas.

2. Specialization: The cyber domain is incredibly diverse; as such, a traditional one-size-fits-all approach to force generation is ill-suited to deliver the operational outcomes required. CYBERCOM 2.0 establishes dedicated pathways for our cyber forces to develop deep expertise in highly specialized fields such as cloud security architecture, industrial control systems, and artificial intelligence. This will result in the formation of dedicated units of specialized experts aligned to critical missions, such as a team with deep expertise in space asset protection or another focused on securing critical energy infrastructure.

3. Agility: The threat landscape in cyberspace evolves with unparalleled speed. As such, the Department requires a force capable of rapid adaptation and dynamic allocation of talent to ensure we maintain a proactive posture against emergent threats. In practice, this means that if a new vulnerability is discovered in a widely used cloud architecture, a specialized team with expertise in that area can be rapidly assembled and deployed to mitigate the threat, rather than pulling personnel from unrelated, mission-essential tasks.

The Seven Core Attributes of CYBERCOM 2.0

To achieve the foundational principles, CYBERCOM 2.0 is built upon seven foundational force generation attributes. While each attribute offers individual merit, their true power lies in their synergy, which creates an exponential effect on our ability to generate and sustain talent.

1. Targeted Recruiting and Assessments: We are shifting from general recruitment to targeted talent acquisition by leveraging USCYBERCOM's operational insights to enhance the Service recruiting enterprises. By employing advanced tools like a Cyber Assessment Battery, we can better identify individuals who possess the aptitude and problem-solving skills for cyber warfare, ensuring the right people are matched to the right work roles. Our pilot initiative will be an in-Service recruitment effort to target in-

Service talent (across career fields) outside the CMF. This targeted approach ensures the Department matches the cyber talent with mission requirements.

2. Incentives for Recruitment and Retention: To remain competitive with the private sector, we are implementing a robust system of incentive pay and retention bonuses designed to reward mastery and specialization. For instance, a master-qualified Cyber Operator might earn a significant monthly bonus, similar to the compensation of Special Operations Forces. Furthermore, we will standardize incentive pay across all Services, ensuring that operators performing the same mission with the same skillset receive equitable compensation.

3. Tailored and Agile Training: The Advanced Cyber Training and Education Center (ACTEC) serves as our platform for advanced and specialized training. It delivers mission-specific skills and knowledge on demand, ensuring our forces remain ahead of technological advancements and adversarial tactics. For instance, if a new adversarial tactic is identified, the ACTEC can rapidly develop and deliver a training module—pulled from in-house expertise, industry, or academia—to relevant cyber forces, ensuring they are prepared to counter the threat. The ACTEC ensures our teams aligned against the most consequential targets have the advanced training resources pulled from the most cutting-edge capabilities at the Department's disposal.

4. Tailored Assignment Management: The Department is engineering career paths, informed by USCYBERCOM, that enable sustained operational engagement to build domain mastery and specialization into the force. This will allow a cyber operator to build a comprehensive portfolio of experience across multiple mission sets, such as completing an extended tour on a National Mission Team, followed by an assignment with a Service's tactical cyber unit. This approach forges unrivaled domain mastery rather than forcing our best talent to move on after a single tour.

5. Specialized Mission Sets: We are developing dedicated units of experts focused on highly specialized missions, such as the protection of space assets or the defense of critical infrastructure. These teams will constitute the world's leading authorities in their respective fields. For example, within CYBERCOM 2.0, we can cultivate teams trained specifically to defend satellite communications and GPS systems, while other teams specialize in protecting power grids and transportation networks.

6. Integrated Headquarters and Combat Support: Our tactical cyber teams will be provided with dedicated headquarters and combat support elements. This structure ensures they have the leadership, resources, intelligence support, and institutional backing necessary to focus on and execute their missions effectively, without being pulled away to perform administrative or other ancillary functions.

7. Optimized Unit Phasing: To maintain high readiness and prevent operator burnout, we are instituting a unit phasing model that creates a sustainable operational tempo. CYBERCOM 2.0 will create a rotational cycle, in which a team member spends a rotation on a mission set followed by a dedicated period for training and recuperation.

This keeps our personnel fresh and effective over the long term and ensures their operational experience is reinvested in the force.

The Three Enabler Organizations

The CYBERCOM 2.0 attributes are driven and supported by three critical enabler organizations:

- Cyber Talent Management Organization (CTMO): CTMO Serves as the main integration point between USCYBERCOM and the Service talent management organizations to discover, assess, select, and retain elite cyber talent. By embedding liaison officers with all Service branches, the CTMO will coordinate recruitment strategies and leverage data to identify and fill critical mission gaps across the force.

- Advanced Cyber Training and Education Center (ACTEC): ACTEC acts as the central delivery point for advanced, mission-specific training. It rapidly identifies emerging requirements, maintains a centralized catalog of cutting-edge training from both internal and external partners in industry and academia, and ensures our forces have access to the right knowledge at the time and place needed. The ACTEC will lead USCYBERCOM's effort to drive training and education partnerships with industry and academia, and to deliver those capabilities at the required scale to the operational force.

- The Cyber Innovation Warfare Center (CIWC): CIWC designed to deliver end-to-end solutions to the Cyber Mission Force at the speed of need. The CIWC serves as the focal point for our research partnerships and spearheads the development of not just technology, but operational capabilities that fully incorporate non-material aspects such as new tactics, techniques, and procedures and doctrine. By maintaining close ties to the operational force, the CIWC can identify requirements and deliver critical capabilities much faster than traditional military acquisition processes. By pairing rapid technological innovation (material and non-material) to critical operational requirements, USCYBERCOM will be able to adapt to meet the dynamic challenges of the cyber domain.

The Path Forward

These seven attributes and three enablers are integral to the success of CYBERCOM 2.0. As directed by the Secretary of War, I will oversee the implementation of 97 tasks across 26 lines of effort, executed by 17 key Department stakeholders. This revised model empowers the Commander of USCYBERCOM, under the authorities granted by 10 U.S.C. § 167b, to directly shape how our cyber forces are generated. It establishes the processes, policies, and relationships that grant the operational commander appropriate input into how cyber forces are manned, trained, and equipped.

CYBERCOM 2.0 is designed to deliver immediate warfighting outcomes while also preserving future decision space. We are implementing foundational force generation initiatives now—such as developing career paths, creating screening assessments, and establishing advanced training—that are essential elements of cyber force generation regardless of any future organizational

decisions. The core principles of mastery, specialization, and agility are indispensable for meeting our strategic objectives, irrespective of which organizational model ultimately emerges.

A cornerstone of my oversight, in lockstep with the DoW CIO and USW P&R, will be to forge the world's most capable and dominant Cyber Mission Force out of the broader DoW Cyber Workforce. To do this, we will apply DoW Cyber Workforce Management policies and aggressively utilize authorities granted by the Cyber Excepted Service to ensure we can out-compete our adversaries for and retain this elite, mission-ready talent. Underpinning all these efforts is a commitment to a closer partnership with both industry and academia to secure our homeland and harness America's unparalleled strength in talent and innovation.

Conclusion

CYBERCOM 2.0 is the beginning of a necessary journey to build the cyber forces our nation needs. As a cornerstone of the Departments' broader strategy, it works in concert with other initiatives—such as validating and updating our cyber force design and employment models—to ensure maximum operational outcomes for the Joint Force. At its heart, CYBERCOM 2.0 is a commitment to our cyber warriors, providing them with the careers, training, and support they deserve. By addressing critical force generation challenges, CYBERCOM 2.0 will significantly increase the lethality and effectiveness of our cyber forces. Its purpose extends beyond cyberspace; it is a critical Joint Force capability that must be integrated across all warfighting domains, sending a clear message to our adversaries of our commitment to maintaining cyber superiority in support of our national interests.

The true strength of our nation lies in the potential of its people. With CYBERCOM 2.0, we are unleashing that potential to build and integrate a world-class cyber force across all warfare domains.

Thank you for the opportunity to testify today. I look forward to working closely with this Subcommittee on this critical national security priority, and I welcome any questions you may have.