RELEASE

Department of War Establishes Revised Cyber Force Generation Model

Nov. 6, 2025

The Department of War (DoW) is establishing a revised cyber force generation model, aimed at increasing the lethality of the Department's cyber forces and providing greater operational outcomes for the Joint Force. The revised model, based on core attributes and key organizations, enables the Department to build mastery, specialization, and agility in the cyber forces assigned to the United States Cyber Command (USCYBERCOM).

"The War Department is laser-focused on strengthening our military's cyber capabilities to defend the homeland and deter China. The Department has implemented an updated cyber force generation model that will enhance our ability to respond decisively against evolving threats in the cyber domain," said Elbridge A. Colby, Under Secretary of War for Policy.

Addressing Cyber Force Generation Challenges

Since its inception over a decade ago, USCYBERCOM has relied on traditional military services' man, train, and equip models to source its cyber forces. While appropriate for other warfighting domains, these traditional models have not met the unique requirements necessary to fight and win in the cyber domain.

The revised cyber force generation model addresses the unique requirements by integrating USCYBERCOM with the military departments to recruit, assess, select, train, and retain the Department's cyber forces.

“This model will accelerate our efforts to build the leading cyber capabilities required to address acute and emerging cyber threats, and to deter escalating aggression in the cyber domain,” said Anthony J. Tata, Under Secretary of War for Personnel and Readiness. “Under the leadership of Secretary Hegseth, the Department is acting swiftly to establish policy, implement programs, and execute a new approach to recruiting, developing, and retaining cyber talent, ensuring that we remain ready to achieve peace through strength.”

The revised cyber force generation model is comprised of seven core attributes and three enabling organizations.

These core attributes focus on building mastery, specialization, and agility:

1. Targeted recruiting and assessments – Recruit for assignment to USCYBERCOM and assess for cyber work role fit.
2. Incentives to recruit and retain top cyber talent – Incentivize cyber domain mastery and retain talent within the Cyber Mission Force.
3. Tailored and agile advanced training – Provide specialized, mission-specific training to meet operational requirements.
4. Tailored assignment management – Adopt career paths that enable the development and retention of cyber domain mastery within the Cyber Mission Force.
5. Specialized mission sets – Shape unit specialization and collective training based on tailored mission requirements.
6. Presented with headquarters and combat support –Present fully functional tactical headquarters that drive operational outcomes.
7. Optimized unit phasing – Implement unit phasing to support a sustainable operational tempo.

Three USCYBERCOM organizations are key enablers for the revised cyber force generation model:

1. Cyber Talent Management Organization – Identify, attract, recruit, and retain an elite cyber force.
2. Advanced Cyber Training and Education Center – Develop and deliver mission-specific training and education to build expertise and mastery.
3. Cyber Innovation Warfare Center – Accelerate the rapid development and delivery of operational cyber capabilities.

Delivering Lethality at the Speed of Cyber

The revised cyber force generation model produces a cyber force capable of defeating threats posed by China in cyberspace and delivering asymmetric options otherwise unavailable to national decision makers and joint force commanders.

“The model fundamentally changes the Department’s approach to generating cyber forces, enabling increased lethality in our cyber forces and establishing a warrior ethos built on domain mastery, specialized skills, and mission agility,” said Katie Sutton, Assistant Secretary of War for Cyber Policy and Principal Cyber Advisor to the Secretary of War. “The initiatives approved by the Secretary of War are foundational to the nation’s immediate needs in the cyber domain, while supporting future decisions on the Department’s cyber forces.”