STATEMENT BY

LESLIE BEAVERS
DEPARTMENT OF DEFENSE PRINCIPAL DEPUTY CHIEF INFORMATION OFFICER

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

ON

FINDING 500,000: ADDRESSING AMERICA'S CYBER WORKFORCE GAP

JUNE 26, 2024

Good morning, Chairman Green, Ranking Member Thompson, and esteemed Members of the Committee. The Office of the Department of Defense Chief Information Officer (DoD CIO) is charged with securing and modernizing IT, enhancing command capabilities, and fostering a digital workforce. Today, I am honored to discuss the strengthening our nation's cyber workforce within the Department of Defense (DoD) with you all.

The Department of Defense requires a skilled and motivated workforce to stay ahead of evolving risks and latest technologies. The Department is identifying and bridging workforce gaps to ensure we are prepared to meet the challenges of today and tomorrow. Specifically, the DoD Cyber Workforce Strategy and its implementation plan were designed to further amplify our efforts to secure top talent. Developing and maintaining our skilled workforce is critical and the introduction of the Cyber Excepted Service (CES) significantly increased our flexibility in attracting and retaining the specialized skills necessary for our mission's success. Additionally, we developed a comprehensive outreach program aimed at recruiting the diverse abilities needed to fulfill our talent requirements. Together, these initiatives underscore our commitment to fostering a thriving workforce that can propel the Department, and by extension the Nation, towards its goals.

Federal Cohesion and Coherence

As part of the ongoing effort to strengthen and empower the Federal workforce, especially those with cyber roles, DoD is leading and coordinating with interagency partners to implement priorities in the President’s Management Agenda. In addition, the DoD CIO was a crucial partner in helping to shape the content of the National Cyber Workforce and Education Strategy (NCWES) released in July 2023. Given this close coordination, DoD can ensure harmonization with Federal cyber workforce efforts with interagency partners and the implementation of the NCWES through our

active engagement in the National Cyber Workforce and Coordination Group, led by the Office of the National Cyber Director. One key success of this coordination is the growing number of institutions obtaining the National Center of Academic Excellence (NCAE) designation, having increased from 420 to 450. In other words, we have more academic partners at higher education institutions aligning their curriculum in a way that supports the cyber work needed in the Federal government. The continued collaboration with the interagency ensured Federal government cohesion that can maximize cyber talent for the nation.

Cyber Workforce Strategy and Implementation Plan

The DoD Cyber Workforce (CWF) Strategy, released in March 2023, and its implementation plan released in August 2023, remains a top priority. Our goals are to address workforce gaps by recruiting top-tier cyber professionals, expanding our cyber workforce, and enhancing the skills of our existing talent. This initiative is crucial for safeguarding our digital and critical infrastructures, ensuring they are operated securely to defend against cyber risks and protect our data from adversaries. The CWF Strategy outlines four human capital pillars – identifying workforce requirements, recruiting talent, developing talent to meet mission requirements, and retaining talent to resolve the department's workforce retention challenge. The successful execution of the CWF Strategy, through this Implementation Plan empowers the Department and its components to foster the most capable and dominant cyber force in the world.

The CWF Strategy and Implementation Plan is an enterprise-wide talent management program aimed at aligning force capabilities with present and future cyber requirements. As previously stated, this effort directly supports the National Cyber Workforce and Education Strategy and

supports Administration's consistent effort to modernize Federal hiring and strengthening the Federal workforce starting with the President's Management Agenda.

As part of the interagency collaboration and in support of NCWES implementation, DoD is committed to reducing the vacancy rates of its critical cyber positions by 2% per year over the next 2-5 years, with the goal to reduce the overall cyber workforce vacancy rate to below 15%. To accomplish the reduction and bolster cyber readiness, DoD plans to benefit from the newly established Cyber Academic Engagement Office. Additionally, DoD will reduce vacancy rates by leveraging existing and under-development authorities that support innovative hiring practices (including skills-based hiring), with targeted recruiting, retention, and relocation bonuses and other related pay related programs. DoD anticipates an additional 2,000 successful cyber workforce hiring actions in each year for the next 2-5 years.

We are cultivating a transformation across the Department to enhance personnel management practices on a broader scale and promoting collaboration and partnerships to enrich capability development, operational efficiency, and career advancement opportunities across the organization.

Development and Retention

Professional development through education and training plays a vital role in supporting and enhancing our cyber workforce capabilities. We have several ongoing partnerships and rotation programs to provide professional development opportunities to our workforce.

The Department recently established the DoD Cyber Academic Engagement Office (CAEO). This office will oversee cyber-focused engagement programs, and enhance coherence, coordination, and

management across the enterprise. The primary objective is to streamline processes and establish a clear pathway for academic institutions seeking engagement with the DoD, serving as the consolidated focal point for engagements between the Department of Defense and academic institutions regarding cyber-related matters.

The Department offers two cyber and IT focused rotation and exchange programs that foster innovation and enables the Department to develop and retain our existing cyber talent. We administer Office of Personnel Management's Federal Rotational Cyber Workforce Program (FRCWP) and the DoD Cyber and Information Technology Exchange Program (CITEP) for the DoD cyber workforce. The FRCWP enables cyber-coded government civilians to hone or develop cyber knowledge and skills through applying for, and serving in, rotational details outside their home agencies across the federal government. Rotations promote intra-agency and interagency knowledge sharing, integration and coordination of cyber practices, functions, and personnel management. The DoD CITEP facilitates a unique opportunity for industry and DoD civilian employees working in the cyber and IT fields to participate in an exchange opportunity between the two sectors. Participants share best practices, gain a better understanding of cross-sector cybersecurity operations and challenges, and gain exposure to a different organization's processes.

Cyber Excepted Service (CES)

The Department appreciates Congress' recognition of the need for flexibilities in attracting, hiring, and retaining quality cyber personnel. Section 1599f of Title 10, U.S. Code, authorized the CES personnel system for DoD civilians supporting the U.S. Cyber Command, providing pay flexibilities to mitigate recruitment and retention challenges. Similar to the Department of Homeland Security's (DHS) Cyber Talent Management System (CTMS), the DoD's CES features

a mission-focused occupational structure, qualification-based professional development, and advancement opportunities without time-in-grade requirements, along with agile recruitment and retention strategies, recruitment incentives, and market-based compensation.

Tracking the Cyber Workforce through the DoD Cyber Workforce Health Report provides leadership with enterprise-wide insights into the cyber workforce through the lens of the DoD Cyberspace Workforce Framework (DCWF) work roles, enabling them to identify workforce gaps and timely address recruiting and retention challenges. This platform reports on the state of the civilian and military cyber workforce, manage the CES Targeted Local Market Supplement (TLMS) incentive and provides commanders with a means of identifying and mitigating workforce health challenges.

Cyber Workforce Qualifications

To provide guidance to the Department on the implementation of our Cyber Workforce Strategy, we released the third publication in the DoD Cyber Workforce policy series to set the foundation for managing, identifying, qualifying, and upskilling our workforce according to the DCWF. The manual plays a crucial role in our workforce by setting forth the qualification standards for every DCWF work role, ensuring that personnel assigned to cyber positions possess the capability to meet mission demands effectively.

Since the publication of the DoD Manual 8140.03 on February 15, 2023, the Department has been working aggressively to implement the qualification of personnel identified as members of the DoD cyberspace workforce. The Department has an established timeline to ensure existing civilian and military personnel meet the new foundational and residential qualification standards by 2025

and 2026 respectively, across the various cyber workforce elements. To address ongoing workforce challenges, we incorporated three DCWF mission critical cyber work roles (to include Cyberspace Operator, Exploitation Analyst, and Software Developer), with potential for future expansion of the DCWF to ensure qualified personnel are recruited and retained to support the cyber mission across the DoD. In addition, the Department is working concurrently across the Services, OSD, and the 4th Estate to ensure that cyber workforce positions are accurately coded. We continue to work with our partners from across the Department to improve the fidelity of our cyber workforce coding using key performance indicators, to in turn report and measure the health of the cyber workforce. Improving the accuracy of our data will further enable the Department to quickly plan and execute the cyber missions.

Academic Outreach and Partnerships

As cyberspace risks continue to evolve in complexity and frequency, fostering collaboration between the Federal Government and academic institutions becomes imperative. Earlier this month, we established in alignment with FY24 NDAA Section 1531, the DoD Cyber Academic Engagement Office (CAEO). My office will use the enhanced authorities granted to serve as a nexus for forging partnerships, facilitating information exchange, and nurturing talent in cyberspace workforce. Additionally, the CAEO signifies a concerted effort to track data and metrics regarding academic programs and their graduates. By systematically monitoring the performance and outcomes of covered academic engagement programs to include: primary, secondary, or post-secondary education programs with a cyber focus; DoD recruitment and retention programs for civilian and military personnel, including scholarship programs; academic partnerships focused on establishing defense civilian and military cyber talent, the DoD can identify emerging trends, evaluate the effectiveness of educational initiatives, and strategically

allocate resources to areas of critical need. This data-driven approach ensures academic institutions are equipped to produce highly skilled cyber professionals and enables the DoD to adapt its strategies in response to evolving threats and technological advancements. The DoD CAEO plays a pivotal role in strengthening the nation's cyber defense capabilities by leveraging the expertise and innovation within academia while fostering a culture of continuous improvement and collaboration.

The DoD CIO administers the DoD Cyber Service Academy (DoD CSA), formerly known as the DoD Cyber Scholarship Program (DoD CySP), which awards scholarships to U.S. Citizens pursuing cyber-related degrees at designated institutions. Recipients of these scholarships are afforded experiential learning opportunities through a DoD internship, providing invaluable exposure to DoD cultures and agencies. This approach not only enhances the qualifications and capabilities of our workforce members but also initiates the clearance process, ensuring that applicants are pre-cleared before commencing full-time employment. For the 2024 cycle, 95 National Centers of Academic Excellence in Cybersecurity (NCAE-Cs) submitted proposals to support scholars under the DoD CSA. Of those 95 academic institutions, six are Historically Black Colleges and Universities, and 14 are first time participants and nominating students for the recruitment and/or retention programs. The Department is committed to supporting higher education and to prepare the DoD workforce to address threats against the Department’s critical information systems and networks. The Department is poised to bring the DoD CSA, to fruition as an additional tool to recruit and retain top cyber talent. The average cost of a DoD CSA scholarship for one academic year is $79k per student. Per law, the scholarship includes tuition, books, fees, stipend, summer internship salary support, a technology and certification allowance, as well as faculty and administrative support. The DoD CSA provided scholarship offers to more

than 165 U.S. Citizens in 2024 and aims to maintain this 17% increase per year. In order to allow a whole of government approach, we are determining the feasibility of allowing students from other Federal Agencies to take advantage of the DoD CSA on a reimbursable basis. The Department appreciates the opportunity Congress granted the Department to expand the DoD CSA to award 1,000 scholarships per year by FY 2026 and is exploring options to resource this Congressional requirement. This effort will further bolster the commitments from DoD and Congress to support higher education to prepare the DoD workforce to combat threats against the Department's critical information system and networks.

The Department is currently tracking approximately 450 designated academic institutions that are eligible to participate in the DoD CSA. Each eligible institution is invited to participate in the DoD CSA program and determines, based on their internal manpower, if they can support such a program on campus. Managing a scholarship on campus requires commitment and resources that may not be available. Any institution who achieves their designation by January 15, 2025, will be eligible to participate in the 2025 DoD CSA application cycle.

Thank you for your support on this issue. We are committed and dedicated in our combined mission of ensuring that our nation continues to be a leader in the cyberspace landscape and combat any challenges to our national security. We look forward to continuing to work with this committee. Thank you for the opportunity to testify this morning, I look forward to your questions.