TESTIMONY OF

Eric Hysen
Chief Information Officer and Chief Artificial Intelligence Officer
U.S. Department of Homeland Security

BEFORE

Committee on Homeland Security
United States House of Representatives

ON

"Finding 500,000: Addressing America's Cyber Workforce Gap"

June 26, 2024
Washington, DC

Chairman Green, Ranking Member Thompson, and distinguished Members of the Committee: thank you for the opportunity to testify at today's hearing, "Finding 500,000: Addressing America's Cyber Workforce Gap," a critical issue impacting our national security.

Every day, over 8,000 cybersecurity professionals across the Department of Homeland Security (DHS or the Department) put their skills to use defending our nation from all manner of threats and vulnerabilities. Threat hunters at the Cybersecurity and Infrastructure Security Agency (CISA) search proactively through Federal and partner networks to identify and stop suspicious activities. U.S. Secret Service Special Agents investigate complex, cyber-enabled financial crimes and combat the illicit use of digital assets. Teams from Homeland Security Investigations identify victims and catch perpetrators of child sexual exploitation and abuse by employing cutting-edge digital forensics techniques. And, Information Technology Specialists across DHS and its operational Components work to stay ahead of our adversaries and secure the Department's own networks, systems, and data.

Our cybersecurity professionals are deeply talented and dedicated to serving their country, but they are too few. The Department has nearly 2,000 vacancies for cybersecurity positions and struggles, like every government agency, to recruit and retain talent in an incredibly competitive field. As technology and our adversaries are constantly evolving, particularly with rapid advances in artificial intelligence (AI) and other emerging technologies, we must ensure our workforce continuously builds new skills to maintain its competitive edge.

I have first-hand experience when it comes to attracting private sector workers to careers in public service. After working in Silicon Valley as a software engineer and project manager, I left the private sector to co-found the United States Digital Service (USDS), which has now recruited hundreds of technologists for government "tours of duty" and will celebrate its tenth birthday later this year. At USDS, I saw how recruiting and retaining tech talent in government requires a comprehensive approach: actively reaching out to communities to build awareness of public service pathways; leveraging flexible compensation and hiring authorities; streamlining hiring and onboarding processes; and building a culture that fosters innovation and collaboration. I am honored to bring this perspective as the DHS Chief Information Officer (CIO) and its first Chief Artificial Intelligence Officer (CAIO).

We have successfully used many of the authorities passed into law under this Committee's leadership to strengthen our efforts. Today, I will highlight some of the programs and initiatives specifically designed to address our cybersecurity workforce challenges at DHS by bringing more people with diverse backgrounds and experiences into government service and by strengthening development opportunities to build skills across existing personnel.

The Department's Cybersecurity Service

Armed with authority passed into law with the strong support of this Committee, the Department, through the Office of the Chief Human Capital Officer (OCHCO), launched one of its most innovative and successful tools for attracting cybersecurity talent in November 2021—the Cybersecurity Talent Management System (CTMS). CTMS authority offers flexibilities to proactively identify, source, and recruit individuals, even if they are not active job seekers, to

create ready-made pools of pre-qualified, selectable talent when needs arise. We now maintain a talent pool of over 1,000 pre-assessed applicants. CTMS offers flexible, capability-focused career paths based upon the NICE Workforce Framework for Cybersecurity that promote career longevity, reducing costs associated with ongoing attrition and recruitment. The product of CTMS, the DHS Cybersecurity Service, offers a diverse, preeminent team working throughout DHS to protect the nation's information technology infrastructure and the American people from cybersecurity risks.

Employees in the DHS Cybersecurity Service work across our cybersecurity missions and operational Components in jobs currently spanning 17 different cybersecurity specializations. Through our authority, the Department can regularly adjust to emerging needs by expanding CTMS hiring across wide arrays of specializations, including those related to AI. Every day, DHS Cybersecurity Service employees are on the front line—protecting the systems, networks, and information Americans rely on. While a Federal employment opportunity may not bridge the salary differentials between government and private sector, CTMS combines Federal benefits with competitive market-sensitive compensation, meaningful work, and career mobility to attract a unique blend of next generation talent, technical experts, and leaders that collectively advance our dynamic cybersecurity mission.

Since its launch in November 2021, DHS received nearly 25,000 applications from persons seeking to join the Cybersecurity Service and fill high-priority jobs in my office, CISA, and the Federal Emergency Management Agency. As of May 2024, the Department issued over 345 initial job offers and onboarded 189 employees – spanning entry-level to executives and distinguished technical experts. These latest figures represent exponential growth in this program.

Employees who participate in the Cybersecurity Service produce significant results. In fewer than nine months, one DHS Cybersecurity Service employee implemented an enterprise-wide, remote penetration testing capability, resulting in a 70 percent reduction in related costs. Another employee's contributions led to a provisional patent for the Department's Unified Cybersecurity Maturity Model, which helps align cybersecurity spending and new capability requests across the Department. Other cyber employees have expanded capacity building and threat hunting capabilities, written CISA's Open Source Software Security Roadmap, and produced a decryptor for an emerging ransomware strain, among other accomplishments.

This new pool of talent represents significant geographic diversity, with employees hailing from over 29 states and the District of Columbia. Over half of current employees are at the entry and developmental level, and we are capitalizing on CTMS's flexibilities to enable these employees to move into more senior roles as their careers progress. Our two-year retention rate is currently 94 percent, compared to an average of 80 percent in the technology industry. Although we are still new and need more longitudinal data, if this rate continues, we will see reduced labor time and costs associated with recruitment and backfilling.

While CTMS is a major value-add to the Department, its rollout was not without challenges. It took us too long from receiving this authority to launch the program and begin hiring under it, and our initial rate of hires have not met our aggressive targets. Designing and launching an entirely new personnel system in the Federal Government is an extremely difficult task, and we

learned from these efforts. We are continuously improving CTMS in partnership with hiring managers to make it a more effective tool. We knew that simply eliminating a step in the hiring process or adding a pay grade would not do enough to make DHS competitive, so we designed CTMS as a true attempt at civil service reform. It is a complex, transformative, and challenging effort, but necessary to position the Department for long-term success.

Additionally, many cybersecurity positions require security clearances at various levels, and this vetting process sometimes sets the pace at which we can onboard new employees to government service. As one of the Security, Suitability, and Credentialing Performance Accountability Council (PAC) members spearheading the Trusted Workforce (TW) 2.0 initiative, DHS is working on implementing relevant policy changes to benefit from recent gains made in clearance processing.

Looking ahead, the Department has committed to expanding CTMS. In fact, one primary objective in my Fiscal Year (FY) 2024-2028 IT Strategic Plan includes implementing CTMS across all operational Components and expanding CTMS applicability as a hiring mechanism for a wider array of cybersecurity-related professionals, including those specializing in data science, AI, and other emerging technologies.

Internships and Fellowships

In addition to CTMS, the Department has established a variety of internship and fellowship programs to create pathways for students and those early in their career to begin their professional journeys at DHS. In 2021, we established the Secretary's Honors Program, modeled after a longstanding successful program at the Department of Justice, which builds cohorts of new employees in priority fields and provides them with access to training, leadership engagements, and exposure to various mission areas across the Department. To date, almost 80 employees have participated in the first three cybersecurity classes of the Secretary's Honors Program. This includes 46 CTMS employees who participated in the third class that ended in April 2024.

Last summer, we welcomed the first 16 participants into the Department's new Intelligence & Cybersecurity Diversity Fellowship program, which was authorized by Congress. Fellows worked for 12 weeks in offices across DHS and had an opportunity to engage with leaders across government, including Secretary Mayorkas and the Ranking Member of this Committee. I was impressed by the talent and passion of this inaugural cohort when I met with them last year, and I am looking forward to meeting with the fellows we are welcoming this summer.

I am also very proud of the Cybersecurity Intern Program (CSIP) launched in my office in the summer of 2022. CSIP provides internships for students ranging from high school to graduate school to bring diverse talent to fields spanning cybersecurity, data management, cloud services, and network operations. The program grew from 52 interns in seven DHS offices and operational Components in 2022 to 85 in over a dozen DHS offices and operational Components this summer. We saw over 1,000 applications in just a single day this year and had to close our application window early given the enormous interest.

AI Corps

In September 2023, the Secretary named me as the Department's first CAIO. As both the new CAIO and the current CIO responsible for strengthening the Department's cybersecurity posture, I immediately recognized the synergies between my two roles. A portion of my focus quickly turned to attracting new talent to harness AI technology in support of the Department's missions.

As AI becomes more powerful and widely used, it is evident that the Department needs AI experts to ensure we leverage this technology responsibly and safeguard against its malicious use. To meet this need, the Secretary announced the creation of the DHS AI Corps in February 2024, during a trip to Silicon Valley. Modeled after the USDS, this group will support the use of AI across DHS, working on critical efforts ranging from countering fentanyl and combating child sexual exploitation and abuse to enhancing our cybersecurity. AI Corps members will identify and mitigate safety and security considerations for AI to ensure its responsible use at DHS.

Demand for personnel with AI technical skills relevant to missions, such as cybersecurity, is immense across all sectors. When attracting such talent, the Department makes a simple argument: now is the time for technology experts to make a real difference for our nation by joining the Federal Government. Although the AI Corps and the accompanying hiring sprint to bring it to 50 personnel is still new, our straightforward message has already produced dramatic results. We received over 6,000 applications for this first-of-its-kind program and have already onboarded seven individuals with another 19 in the onboarding process. AI Corps members come from the country's top technology firms and from across government and civil society, bringing skillsets in data science, machine learning, product and program management, software engineering, and human-centered design to accelerate our efforts.

Training and Development

The Department prioritizes attracting, hiring, and retaining top technical talent, but we also understand the need to consistently train our existing workforce to confront evolving challenges in cybersecurity and technology. For this reason, the first goal of the DHS IT Strategic Plan is "Invest in the DHS IT Workforce."

We are building a DHS IT Academy to ensure every DHS IT and cybersecurity employee is competent in core skillsets and to assist employees in developing new technical skills. The DHS IT Academy will create standard technical orientations for all DHS IT employees, develop a rigorous training and rotation program for entry-level hires, and offer upskilling opportunities for employees to learn new and emerging skills. As a first step, we launched a standardized IT Immersion Program for all new DHS IT professionals. IT Immersion provides new hires with a shared understanding of how IT enables the DHS mission and instructs them in core IT concepts including zero trust implementation, cybersecurity risk management, continuous monitoring and security authorizations, privacy concerns, and customer experience. The inaugural IT Immersion Program included 140 attendees from across the Department, and a second Program held last month for employees who joined the Department after our inaugural session included an additional 72 attendees. We only expect interest to grow as we move ahead.

The DHS IT Academy effort also led to the development of role-based training minimum standards for roles with significant cybersecurity responsibility: Information Systems Security Manager, Information Systems Security Officer, System Owner, and Authorizing Official. These DHS minimum standards are aligned with the National Institute of Standards and Technology's NICE Workforce Framework for Cybersecurity and include minimum specified knowledge standards and typical tasks for each role. We anticipate launching the initial set of role-based trainings by the end of this fiscal year.

Finally, we are working to ensure all DHS employees are building basic technical awareness and skills, not just those working in securing technology and cybersecurity. We are redesigning our annual Cybersecurity Awareness Training and have launched regular phishing exercises to keep all employees sharp on their personal contributions to the Department's cybersecurity. Last year, we were the first Department to launch training for employees seeking to use commercially available generative AI tools in their work. Over 5,000 employees have taken this training and have permission to use these cutting-edge tools responsibly and safely.

Federal Cohesion and Coordination

To support the Administration's effort in modernizing Federal hiring and strengthening the Federal workforce, DHS is also aligning its cyber workforce effort with the President's Management Agenda; National Cyber Workforce and Education Strategy implementation; National Security Memoradum-3 ("Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships"); Executive Order 14119 ("Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums"); and Executive Order 14110 ("Safe, Secure, and Trustworky Development and Use of Artificial Intelligence").

Conclusion

The programs I have outlined today are just some of the tools we are using across DHS to strengthen our cybersecurity workforce. There is no single initiative or policy to address all workforce challenges, and every organization that relies on this talent across the public and private sectors is similarly looking at a combination of efforts spanning recruitment, hiring, training, and retention. I look forward to our continued partnership with Congress, and especially this Committee, to deliver flexible authorities needed to attract talent in an extremely competitive market.

I also urge the Committee to take an expansive view of cybersecurity talent. Cybersecurity is a vital part of every stage of the software and technology development lifecycle. We must ensure all employees involved in this process are equipped to understand how their role contributes to cybersecurity, from designers and program managers through network operators and help desk technicians. While cybersecurity-focused programs are critical, complementary efforts such as the DHS AI Corps, which bakes cybersecurity into programs for recruiting adjacent talent, also have an important role to play. We acknowledge the importance of diversity, equity, and inclusion in building a robust cybersecurity team. By actively recruiting from underrepresented communities and ensuring an inclusive work environment, we can leverage a wider range of perspectives and skills, which are crucial in addressing the complex challenges of cybersecurity

today.

I am proud of the progress the Department has made, but there is still work to be done. As we move forward, we remain dedicated to continuously improving our programs and learning from our challenges so that DHS remains at the forefront of our nation's cybersecurity protections.

Thank you for the opportunity to testify today. I welcome your questions.

June 26, 2024
Testimony of Seeyew Mo
Assistant National Cyber Director
Office of the National Cyber Director
Executive Office of the President
10 A.M. EST
United States House of Representatives
Committee on Homeland Security

Hearing on
"*Finding 500,000: Addressing America's Cyber Workforce Gap*"

Chairman Green, Ranking Member Thompson, and distinguished Members of the Committee, thank you for holding this important hearing to address the challenges facing the nation's cyber workforce. The White House Office of the National Cyber Director (ONCD) is leaning in to tackle persistent cybersecurity challenges, protect the nation, and foster economic prosperity.

One of these persistent challenges is the dire need for cyber talent. The problem is clear—we need more talent, not only in the Federal government, but also in state, local, tribal, and territorial governments, and the private sector. The number of open cyber jobs— approximately a half-million nationwide—is enormous and the trend line must improve.

With this challenge, there's an opportunity—we have an abundance of talented individuals in our country who can help us meet this need. They can enter a career field that—whether they work in government or in the private sector—helps secure our nation. A career with purpose. A career that offers a good-paying, meaningful job. We must remove barriers and broaden pathways for these individuals to get into cyber careers.

Many stakeholders, from Congress and this Administration to industry, academia, and civil society, have been working diligently to solve the cyber workforce challenge. Throughout our three-year history, we in ONCD have acknowledged that we are not the first to tackle the challenges to grow the cyber workforce, nor are we alone in our efforts.

As the Assistant National Cyber Director for Cyber Workforce, Education, Training and Awareness, I am honored to lead a team of cyber workforce experts to coordinate the implementation of the National Cyber Workforce and Education Strategy (NCWES), released by ONCD last July, and to align that effort with priorities such as the President's Management Agenda, recent investments in Workforce and Technology Hubs across the nation, and efforts to strengthen the workforce for in-demand industries, just to name a few.

I am pleased to testify with some of ONCD's closest Federal partners here today. The diligent work of these and many other Federal agencies is helping to expand and strengthen our nation's cyber workforce throughout every sector of the economy, including Federal, state, local, tribal, and territorial governments.

Although the problem we have is clear, the solutions are complex, and I look forward to updating the Committee on how the Administration is advancing both our national security and our economic prosperity by working to connect more Americans to good-paying, meaningful jobs in cyber. I will describe, from ONCD's perspective, the challenges we face meeting the cyber workforce demand, articulate the Administration's whole-of-nation approach, and highlight some initial implementation successes.

THE CHALLENGES FACING OUR CYBER WORKFORCE

The United States is completely reliant on a digital backbone that facilitates everything from the power, gas, and water coming into our homes to the systems that keep our roads, bridges, airports, banks, schools, hospitals, businesses, and military facilities functioning. This connectivity comes with risks, including the vulnerability of systems and networks to attacks on

that digital foundation. There's a lot we need to do—and are doing—to better protect our nation and its critical infrastructure in cyberspace.

One thing that is certain is that we need the talent to do the job. That means that we must find, hire, develop, retain, empower, and inspire more people to help us fill the approximately half-million open positions across the nation, across different industries and sectors, that are important to the security of our nation's critical infrastructure. We need cyber talent not just in information technology (IT), or finance, but also in manufacturing, utilities, agriculture, energy, healthcare, and other sectors and industries.

There are a number of issues facing our workforce:

- First, many Americans don't see opportunities for themselves in cyber, often assuming that jobs in cyber are narrow or highly technical. Further, even when we have individuals that are interested, willing, and ready to serve, there are barriers that keep them from these opportunities, such as degree requirements that may be unnecessary when job seekers have the skills and experience to fill the need.

- Next, demand for cyber workers exceeds the current capacity of workforce development and education systems. We need more opportunities and pathways to train workers to be cyber-ready. We also need educators, from K-12 to faculty with doctorates, with the knowledge to teach cyber, and support to expand hands-on learning opportunities on the latest technologies and facilities. Additionally, the training and education infrastructures that exist today need to adapt to the changing cyber skills and demands presented by the rapidly evolving technological landscape.

- Finally, there are not enough locally-driven ecosystems to develop the pipeline for cyber talent. We can't meet demand unless academia, Federal and local government, and the private sector work together to build a pipeline for cyber workers. Connecting individuals to training, helping them find jobs, providing wraparound services, and more, requires leadership and investment from a variety of local stakeholders.

This challenge is compounded by the dynamic nature of the national security environment and the rapid acceleration of global crises, new technologies, vulnerable software and systems, and novel threats. Artificial intelligence (AI), quantum computing, and technologies that have yet to be invented, will require an agile, and dynamic workforce with foundational cyber skills in every industry, sector, and occupation that can understand, leverage, develop, maintain, and protect the next generation of advanced cyber capabilities.

The only way we can defend the digital foundation of our modern way of life is to ensure that everyone has a pathway into a cyber-based career and our workforce is equipped with the skills to meet any future demands. That's why ONCD is focusing on removing barriers and broadening pathways.

NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY DEVELOPMENT

To address these enormous challenges, ONCD undertook a comprehensive approach to develop a national strategy that addresses educating, training, and employing the cyber workforce.

ONCD acknowledges that the Federal government, working alone, cannot adequately address the many challenges we face in filling current and future cyber work roles with a skilled workforce. Consequently, in the development of the strategy, ONCD collaborated with 34 Federal agencies, Executive Office of the President (EOP) components, and hundreds of key external stakeholders to identify current challenges and best practices, and grasp the true root of the issues we are facing.

These NCWES guiding principles address the challenges mentioned above:

- **First, broaden the appeal of cyber careers to more Americans** – In order to achieve the best mission outcomes, we need the best possible team. One of the most effective ways to grow our supply of cyber talent is to attract people of all ages, all demographics, and all backgrounds especially those that areunderrepresented in the cyber workforce today.

- **Second, focus on a skills-based approaches** – We must expand access to cyber skills training and education to all Americans. When individuals have the skills and abilities to learn new technologies, it creates a dynamic workforce that meets the demand of new developments and disruptions, like the rapid expansion of artificial intelligence we are seeing today. We must encourage the adoption of skills-based approaches to open up pathways to good-paying jobs for Americans with the skills to do them, regardless of how they acquire those skills.

- **Third, encourage ecosystem development** – The strategy aims to encourage partnerships between public and private stakeholders that can meet specific regional and sector-based talent needs. For example, this includes employers communicating with school systems, academia, and training programs on the skills needed to fill open jobs and meet the demand for cyber skills in the future.

To meet these cyber workforce challenges, we know that the best solutions come not solely from Washington, but from the innovative partnerships and ideas we find in communities such as those in your districts across the country. I have seen some of the best solutions come from among local government, employers, school districts, higher education institutions, and non-profits coming together to solve cyber workforce and education demands. These partnerships create pathways for potential job candidates to consider a cyber career and connect them with learning experiences to gain the skills to meet their communities' needs.

COHERENCE AND COHESION IN IMPLEMENTATION

To advance and coordinate Federal government cyber workforce and education activities, ONCD established the National Cyber Workforce Coordination Group (NCWCG), composed of ONCD and Senior Executive Service-level leadership from Federal agencies that supported the development of the NCWES. The NCWCG is chaired by ONCD and oversees three

subordinate working groups – Federal Cyber Workforce Working Group (FCWWG), the Working Group on Cyber Workforce and Education (WG-CWE), and the Working Group on Cyber Skills and Awareness (WG-CSA) – pursuing the objectives in the NCWES. Each of these working groups is co-chaired by ONCD and one or more Federal agencies.

Through these working groups, agencies are actively participating in the implementation of the NCWES by leading initiatives and producing deliverables that respond to the challenges facing cyber education and workforce development. This ensures that NCWES implementation activities are coordinated and cohesive to maximize progress and the impact of taxpayer investments.

In addition, ONCD is synchronizing its activities with the goals in the President's Management Agenda; the directives of National Security Memorandum 3, "Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships"; and ensuring that its strategy for growing and strengthening the cyber workforce is in harmony with other Federal initiatives, including Workforce Hubs, Tech Hubs, and Technology and Innovation Partnerships. ONCD is also synchronizing activities in support of President Biden's Executive Order 14119 – "Scaling and Expanding the Use of Registered Apprenticeships in Industries and the Federal Government and Promoting Labor-Management Forums," and Executive Order 14110 – "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."

The progress we have made thus far is bringing a more unified and collaborative approach at the national level and laying stronger groundwork for the development of the cyber workforce. By linking cyber workforce development with other workforce and education efforts, this approach is poised to yield a more diverse array of skilled cyber professionals through consistent and focused education and training offerings.

NCWES INITIAL IMPLEMENTATION PROGRESS

Over the past year, this interagency collaboration has yielded significant progress towards investing in cyber education and workforce development to fill jobs, and consequently have more defenders to protect our nation's most critical systems.

Strengthening the Federal Cyber Workforce

On April 29, 2024, the National Cyber Director announced that the Biden-Harris Administration is modernizing the Federal hiring process, fully embracing skills-based approaches for information technology management positions. Aligned with broader strategic hiring objectives, this modernization effort will include use of registered apprenticeships programs.

The Office of Personnel Management (OPM) is leading the transition of the Information Technology (IT) Management job series, numbered 2210, to skills-based hiring and talent development practices. The 2210 job series includes nearly 100,000 IT workers across all Federal agencies and represents a majority of the Federal IT workforce. This effort is a critical

step in removing barriers that prevent qualified job seekers from entering the Federal cyber workforce.

Furthermore, the effort extends to contractors that also play a role in our Federal cyber workforce. The Department of Energy (DOE) recently announced an effort to pivot to a skills-based approach in IT and cyber contracts. ONCD is also working with OMB to encourage wider adoption of Section 39.104 of the Federal Acquisition Regulation (FAR), which states that when acquiring information technology services, solicitations must not describe any minimum experience or educational requirements for contracted personnel.

To continue bringing cyber talent into the Federal government, the Tech to Gov Working Group (TTGWG), a workstream of the FCWWG led by OPM, held a second Tech to Gov Job Fair on April 18, 2024. More than 1,700 attendees from all 50 states registered and met with over 100 agency representatives. Since the first Tech to Gov Job Fair about a year ago , approximately 150 tentative job offers have been made and more are underway. Another Tech to Gov job fair is tentatively scheduled for the fall of 2024.

Some cyber roles require clearances, which can be a barrier to timely hiring and can cause candidates to accept other job offers due to clearance delays. Under the Trusted Workforce 2.0 initiative led by the Security, Suitability, and Credentialing Performance Accountability Council (PAC), some gains have been realized:

- The average amount of time needed to complete a security clearance background investigation has fallen from 411 to 155 days for a Top Secret clearance and from 173 to 53 days for a Secret clearance.

- In the second quarter of Fiscal Year 2024 (FY24), over 27,000 new hires were cleared using preliminary determinations, a practice by which agencies clear personnel with clean records for onboarding based on the highest value background checks.

The PAC is working to expand this practice by implementing ambitious targets of 45 days for Top Secret clearances and 25 days for Secret clearances.

Expanding and Enhancing America's Cyber Workforce

To promote cyber workforce growth opportunities, ONCD continues to hold outreach events across the country. Over the past year, events have been held in collaboration with state and local stakeholders to expand the cyber workforce in Arizona, Florida, Georgia, Illinois, Maryland, Michigan, Nevada, North Carolina, Ohio, Oklahoma, Pennsylvania, Tennessee, Texas, Virginia, and Washington. These events help amplify the Biden-Harris Administration's workforce growth priorities; highlight needs, solutions, and progress in these communities; and engage and promote cyber workforce and education ecosystems of stakeholders across all industries and sectors.

Over the course of these travels, ONCD has learned about innovative and proven best practices from local leaders, which can be shared and scaled to further enhance and expand the cyber

workforce across the nation. One of these practices is hands-on, work-based learning, primarily through apprenticeships and paid internships consistent with the Good Jobs Principles – an initiative to uplift Americans into good paying jobs, including cyber jobs.

To further increase access to registered apprenticeships in fields such as cybersecurity, in 2023 the Department of Labor (DOL) awarded approximately $108 million in grants and contracts to expand Registered Apprenticeships in high-growth and in-demand industries. DOL also worked with other Federal Agencies to conduct a registered cyber apprenticeship sprint and has served more than 13,000 cyber apprentices to date. To build on this effort, earlier this year, DOL also announced the availability of nearly $200 million in grants to continue to support public-private partnerships that expand, diversify, and strengthen Registered Apprenticeships in education, care, clean energy, IT/cybersecurity, supply chain, and other in-demand industries.

Many private-sector organizations are conducting their own voluntary initiatives in support of the NCWES. This private sector engagement has created a groundswell of additional commitments to support cyber career growth opportunities in various sectors spanning from healthcare to manufacturing, water and wastewater systems to K-12 education, agriculture and transportation to the Defense Industrial Base (DIB), and more.

Investments from both public and private sectors are key to our success. For example, the National Security Agency (NSA), through grants to National Centers of Academic Excellence in Cybersecurity (NCAE-C) institutions, launched Cyber Clinics in Louisiana, Minnesota, Nevada, and Virginia. Cyber Clinics support communities and small governments that would otherwise not have access to cyber risk assessment and planning assistance and provide an opportunity for over 200 students to develop competencies while in a supervised learning environment. The Cyber Clinics model has garnered private-sector investments of over $25 million that enabled the opening of clinics at 45 more institutions.

MOVING FORWARD

Though significant progress has been made, more work needs to be done to continue to deepen and broaden our cyber talent pool to strengthen and defend our national cyberspace. To advance NCWES implementation, we will work with our partners and stakeholders to:

- Explore innovative solutions to engage the public at different education and career levels to learn cyber skills and consider a career in cyber.

- Encourage the adoption of skills-based approaches by employers and increase work-based learning opportunities.

- Facilitate a hiring surge to fill open Federal cyber positions by conducting cyber hiring sprints to generate job offers and continue to support CyberCorps®: Scholarship for Service.

- Seek to expand foundational cyber skills learning opportunities and increase the capacity of K-12 systems and higher education institutions to provide impactful cybersecurity learning experiences.

- Look into boosting participation of students and educators in cyber scholarship programs.

- Leverage the collective strength of all Federal agencies to increase participation and promote the value of veterans, separating service members, and military spouses in the cyber workforce.

- Encourage the development of locally-driven or sector-specific systems nationwide.

- Continue to support Federal coordination of broader talent initiatives involving tech, cyber, and AI.

The Administration will strive to lead by example as we work to expand the use of skills-based hiring and talent development for Federal cyber positions and contracts. In addition, Federal agencies will work with academia to expand concurrent, credit transfer and articulation opportunities for academic credit, further integrate cyber across academic disciplines, and increase the availability of low-cost and no-cost cyber training and education curricula.

CLOSING

Let me close by quoting National Cyber Director Coker on the importance of our mission.

> *"We defend cyberspace not because it is some distant terrain on which we battle our adversaries. We defend cyberspace because it is interwoven into our very lives—because it underpins the critical systems that enable us to work, live, and play—because it is a matter of national security."*

We need more Americans to join the cyber workforce so that all Americans can benefit from the enormous potential of our interconnected future. That's why growing and strengthening the cyber workforce is a key pillar of the President's National Cybersecurity Strategy.

The Administration will continue to execute the whole-of-nation approach conveyed in the NCWES to drive change in the public and private sectors through engagement and collaboration. The Federal government is pursuing activities to respond to the critical need for cyber workers; encourage more Americans to consider cyber careers, increase skills-based hiring, talent development, and education nationwide; address barriers faced by Federal and non-Federal stakeholders; proactively analyze and monitor the changing labor demand for cyber skills; and continue to advance our cyber posture, national security, economy, and society. And ONCD will continue to monitor and report on the progress of these actions.

We are committed to working together with Congress and other partners to connect Americans to good-paying, meaningful jobs in cyber.

Thank you for the opportunity to testify today, and I look forward to your questions.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Testimony of

Rodney Petersen
Director of NICE and Interim Chief of the Applied Cybersecurity Division
National Institute of Standards and Technology
United States Department of Commerce

Before the
United States House Committee on Homeland Security

On

"Finding 500,000: Addressing America's Cybersecurity Workforce Gap"

June 26, 2024

Chairman Green, Ranking Member Thompson, and Members of the Committee, I am Rodney Petersen, Director of the National Initiative for Cybersecurity Education (NICE) Program Office at the National Institute of Standards and Technology (NIST) in the Department of Commerce. I am pleased to testify before you today on behalf of the NICE program and to illuminate our vision to *prepare, grow, and sustain a cybersecurity workforce that safeguards and promotes American's national security and economic prosperity*.

I want to briefly share three stories:

Devonie Nelson is a Junior Cybersecurity Engineer who started her journey into the cybersecurity field while a single Mom with significant personal and financial challenges. After graduating with a biology degree, she experienced a series of personal and career challenges as a young adult. She eventually enrolled in a Security Management master's degree program with a concentration in cybersecurity. Along the way, she discovered a philanthropic organization that enabled her to persist in her educational journey and eventually acquire a cybersecurity position at a healthcare company. Now, she has dedicated herself to sharing with others her experiences and the opportunities available to eliminate some of the initial hurdles faced when entering the cybersecurity field, especially as a minority first-generation student.

Jimmy Minhinnett was a truck driver who is now an Information Security Associate with a company in the financial services sector. Although he understood the impact of technology at a young age thanks to his father who worked in IT, life circumstances took him in a different direction. He left high school before completing his diploma and for the next 10 years worked hard, physically demanding shifts as a commercial truck driver. As a result of the impact of the pandemic on the trucking industry – combined with grieving the death of his father – he decided to pursue a new career and that led to the discovery of a cybersecurity certificate program that he completed on weekends while continuing to work. After acquiring that credential, he received a good job that changed his life.

Shane Wallace is the product of a military family, and he enlisted in the Army as a combat medic in 2014. Through his military service, he demonstrated a relentless commitment to excellence, concurrently pursuing a degree in Healthcare Administration. His assignments spanned the globe, where he held various leadership roles, overseeing complex logistics operations and spearheading crucial medical initiatives. As he transitioned from military service in 2023, his passion for technology led him to pursue and graduate from a training program for transitioning veterans where he developed a competency in cloud computing that led to an eventual role as a Junior Engineer with a private sector employer.

These are just three examples of individuals who have pursued a cybersecurity career through alternative pathways – and their stories help to address the focus of this hearing on how to find workers to address America's cybersecurity workforce gap. They shared their

stories earlier this month at the annual NICE Conference & Expo,[1] which was held in Dallas. However, their stories represent a growing number of Americans who are getting into good-paying, meaningful careers in cybersecurity through the many different education or training pathways available to them.

NICE's mission is to *energize, promote, and coordinate a robust community working together to create an integrated ecosystem of cybersecurity education, training, and workforce development*. This mission aligns with the Administration's broader efforts in modernizing Federal hiring and strengthening the Federal workforce. As part of this NIST is also supporting broader workforce efforts including but not limited to the President's Management Agenda, the National Cyber Workforce and Education Strategy implementation, the National Security Memoradum-3 "Memorandum on Revitalizing America's Foreign Policy and National Security Workforce, Institutions, and Partnerships" and the AI Executive Order. The NICE Program Office also actively promotes and supports the Department of Commerce Principles on Highly Effective Workforce Investments[2] and the Department of Commerce and Department of Labor's Good Jobs Principles[3]. Today's testimony will focus on signature programs led by NIST beginning with the NICE Workforce Framework for Cybersecurity (or NICE Framework).

Federal Coordination and Coherence

As part of the administration-wide effort to connect Americans to Good Jobs in cyber, NICE coordinates with the White House of Office of National Cyber Director (ONCD), Office of Management and Budget, and through the National Cyber Workforce Coordination Group to integrate and align its work with the President's Management Agenda, National Cyber Workforce and Education Strategy (NCWES) implementation, Registered Apprenticeship EO, and Workforce Hub Efforts. For example, NICE is co-chair of the Working Group on Cyber Skills and Awareness as well as the Working Group on Cyber Workforce and Education.

NICE Workforce Framework for Cybersecurity (NICE Framework)

The NICE Framework[4] provides a common taxonomy or lexicon for describing cybersecurity work. It is used by employers to assess their workforce needs and to shape workforce development, including writing job descriptions that are more consistent and effective across organizations and sectors. The NICE Framework is also used by education and training providers to develop content and provide learning experiences to ensure that students or learners can develop skills and acquire credentials that attest to their capabilities. It is also used by learners, including students, job-seekers, and employees, to identify the skills and credentials necessary to enter and advance in high quality jobs in the cybersecurity career. The NICE Program Office released version 1.0.0 of the NICE

---

[1] https://niceconference.org/

[2] https://www.commerce.gov/issues/workforce-development

[3] https://www.dol.gov/general/good-jobs/principles

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Framework components in March, which represents a comprehensive update to the core content of the NICE Framework (NIST Special Publication 800-181r1). The recently updated NICE Framework includes 52 Work Roles across seven categories, 11 new Competency Areas, and over 2,220 Task, Knowledge, and Skill Statements.

CyberSeek: Interactive Cybersecurity Jobs Heatmap and Career Pathway Tool
Another signature program of NICE is our partnership with CompTIA and Lightcast, which has resulted in the production of CyberSeek. The CyberSeek.org[5] website is a tool that can help learners discover cybersecurity careers and policymakers, such as yourself, discover the dynamics of workforce supply and demand across the United States as well as in states or major metropolitan areas. Lightcast also developed the Quarterly Cybersecurity Talent Report as a commitment to support the NCWES from ONCD. It leverages and expands upon data Lightcast provides to CyberSeek.org. The updates to CyberSeek and the Cybersecurity Talent Report earlier this month revealed that, for the past 12 months in the U.S., there were 469,930 cybersecurity job postings, 1,239,018 existing cybersecurity workers, and 85 skilled cybersecurity workers for every 100 demanded by employers. While these numbers suggest modest improvements and indicate that we are making headway, there is still a talent gap of 225,000 cybersecurity workers needed to meet employer demand. In the DC metropolitan area alone, there are 66,775 cybersecurity jobs available and 36,908 across the entire state of Texas.[6]

NICE Strategic Plan (2021-2025)
The NICE Strategic Plan[7] and corresponding implementation plan is another signature program of NICE and establishes our vision, mission, and values. It also sets forth five goals with corresponding objectives.

Promote the Discovery of Cybersecurity Careers and Multiple Pathways
The first goal is to *Promote the Discovery of Cybersecurity Careers and Multiple Pathways*. As you heard earlier, the learning pathways to a career in cybersecurity can vary from learning experiences in high school or college leading to an academic degree to training programs or bootcamps that result in an industry-recognized certification to a Registered Apprenticeship or other earn and learn experience that culminates in a certificate of completion. However, providing multiple learning pathways is not enough if learners do not understand the variety of types of careers that are available in cybersecurity. That is why during the third week of October each year, as part of Cybersecurity Awareness Month, we hold a Cybersecurity Career Week,[8] that is a campaign to promote the discovery of cybersecurity careers and share resources that increase understanding and engagement in the multiple learning pathways and credentials that lead to careers in cybersecurity. The week is typically kicked-off with a Capitol Hill event hosted by the House Cybersecurity

[5] https://www.cyberseek.org/
[6] https://www.cyberseek.org/heatmap.html
[7] https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
[8] https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week

Caucus and Senate Cybersecurity Caucus and other events throughout the week including the US Cyber Team Draft Day[9], webinars, social media campaigns, and workplace events to showcase careers in cybersecurity.

Transform Learning to Build and Sustain a Skilled and Diverse Workforce

The second goal is to *Transform Learning to Build and Sustain a Skilled and Diverse Workforce*. There are many opportunities for innovation in the learning process that will increase the likelihood that job-seekers are job-ready to enter employment. Examples include more hands-on learning experiences and the use of performance-based assessments that measure competencies and capabilities to perform NICE Framework tasks. In an era when "skills-based approaches" is the mantra of employers and educators, we need to improve the quality and transparency of available credentials that serve to demonstrate and validate the competencies of a learner. We also need to advocate multidisciplinary approaches that integrate cybersecurity across disciplines, recognizing that a basic level of cybersecurity knowledge and skills are increasingly necessary in almost every career field and in every sector of the economy. The Cybersecurity Across Disciplines Conference[10] is an example of an event that brings together community and technical college faculty from diverse disciplines to explore the intersection of cybersecurity within their specific educational program areas and the critical infrastructure sectors they serve, including but not limited to manufacturing, healthcare, retail, engineering, and finance. And, building on the NICE value to Model Inclusion, this strategic plan goal emphasizes advocating and enabling engagement of stakeholders from diverse backgrounds and experiences.

Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

The third goal is to Modernize the Talent Management Process to Address Cybersecurity Skills Gaps. It fundamentally seeks to enhance the capabilities of organizations and sectors to more effectively recruit, hire, develop, and retain the talent needed to manage cybersecurity-related risks. Building on other foundational NIST publications, such as the Risk Management Framework and Cybersecurity Framework[11], this goal helps organizations to focus on the "people" and workplace skills needed in their organizations who work alongside "technologies" or "processes" to manage cybersecurity risks. A few examples of reforms that are needed include: establishing more entry-level positions and opportunities that provide avenues for growth and advancement; aligning qualification requirements according to proficiency levels to reflect the competencies and capabilities needed to perform tasks in the NICE Framework; encouraging ongoing development and training of employees, including rotational and exchange programs, to foster and retain talent with diverse skills and experiences; and reskilling the unemployed, underemployed, incumbent workforce, and transitioning veterans or military spouses to prepare them for good jobs in cybersecurity.

---

[9] https://www.uscybergames.com/draft-day

[10] https://www.ncyte.net/about-ncyte/events/cyad-summit-cybersecurity-across-disciplines

[11] https://www.nist.gov/cyberframework

Expand Use of the NICE Workforce Framework for Cybersecurity (NICE Framework)
The fourth goal seeks to *Expand Use of the NICE Workforce Framework for Cybersecurity or NICE Framework*. This goal starts with increasing awareness of the benefits of the NICE Framework to employers, educators, and training providers. This goal goes on to ensure that the NICE Framework is aligned to other NIST resources, including the NIST Cybersecurity Framework, the NIST Privacy Framework[12], and other cybersecurity, privacy, and risk management publications or guidance. We are also keenly aware that tasks in the NICE Framework will be increasingly performed by automated techniques and will need to update knowledge and skill statements to incorporate appropriate and ethical use of artificial intelligence in the completion of cybersecurity tasks. Our international partners, especially developing nations, are increasingly looking to NIST resources, including the NICE Framework, as a model for their national efforts. That is why NICE recently partnered with the State Department to bring individuals representing over 20 countries to the NICE Conference & Expo earlier this month to learn more about their cybersecurity workforce development efforts and share how the NICE Framework is being widely used across the United States.

Drive Research on Effective Practices for Cybersecurity Workforce Development
The final goal in the NICE Strategic Plan seeks to Drive Research on Effective Practices for Cybersecurity Workforce Development. That is why each month, during our NICE Community Coordinating Council Meeting, we feature recent reports or research results that spotlight the most effective and proven practices. Similarly, we use research results to inform programs and curriculum design, foster continuous learning opportunities, impact learner success, and ensure equitable access. Again, supporting the NICE values to Challenge Assumptions, Stimulate Innovation, Act Based on Evidence, and Evaluate and Improve, we are working together as a community to pursue objective and reliable sources of information and using data to inform actions or decisions.

Foster Communication, Facilitate Collaboration, and Share and Leverage Resources
Let me conclude by just highlighting a few other ways in which NICE fulfills its mission – through its convening power and the development and dissemination of resources. On a monthly basis, NICE, convenes an interagency coordinating council of representatives from across federal government departments and agencies and the executive office of the president to coordinate and collaborate on national cybersecurity education and workforce development initiatives. We also convene a NICE Community Coordinating Council that is co-chaired by a leader from academia and industry. The Council includes working groups that correspond to each of the NICE Framework goals and communities of interest on topics such as cybersecurity apprenticeships, competitions, diversity and inclusion, K12 cybersecurity education, and more.

[12] https://www.nist.gov/privacy-framework

To promote and energize a robust community working together, NICE hosts several key events[13] each year, including the Annual NICE Conference and Expo, the Regional Initiative for Cybersecurity Education and Training Conference for the Americas, a NICE K12 Cybersecurity Education Conference, Cybersecurity Career Week, and a monthly NICE Webinar Series. These events bring together stakeholders to increase awareness and understanding, showcase effective practices and solutions, and expand our horizons by focusing on emerging and future trends. We also produce and share several resources[14], most of them developed with input from the broader community, including the NICE Framework Resource Center, the NICE Cybersecurity Apprenticeship Finder, one-pagers on topics such as Cybersecurity Workforce Demand, and a listing of Free and Low Cost Online Cybersecurity Learning Content.

Summary

In conclusion, the recent NICE Conference & Expo held in Dallas was our 15th annual conference and served to celebrate the establishment of NICE in 2008 by the Comprehensive National Cybersecurity Initiative. Over the past 15 years, we've seen considerable growth and progress towards fulfilling our mission to create an integrated system of cybersecurity education, training, and workforce development. However, the present and future promises to introduce new challenges and opportunities, and we must remain vigilant to continuously prepare, grow, and sustain the cybersecurity workforce that the public and private sector will need to safeguard our national security and promote America's economic prosperity.

Thank you for the opportunity to testify today on NIST's Cybersecurity Workforce activities, and I look forward to answering any questions.

[13] https://www.nist.gov/itl/applied-cybersecurity/nice/events

[14] https://www.nist.gov/itl/applied-cybersecurity/nice/resources

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.