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.