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.