Written Testimony of Rob Rashotte

Vice President, Fortinet Training Institute

Fortinet, Inc.

Before the U.S. House Committee on Homeland Security

Hearing on

“Preparing the Pipeline: Examining the State of America’s Cyber Workforce”

February 5, 2025

Chairman Green, Ranking Member Thompson and distinguished Members of the Committee, I appreciate the opportunity to testify before you today on "the State of America's Cyber Workforce". My name is Rob Rashotte and I serve as Vice President of the Training Institute at Fortinet.

Fortinet[1] is a U.S. company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold worldwide, our portfolio extends across nearly 60 different integrated cybersecurity and networking solutions and services, reflecting our commitment to innovation as information technology (IT) and cyber threats continue to evolve. In addition to our products and services, Fortinet operates a robust cybersecurity training institute[2] focused on helping to address the significant global cyber workforce and skill gaps and preparing the next generation of cybersecurity professionals. Our ultimate goal is to enable a more digitally secure society.

We believe teamwork is key to best defend against cyber threats. To that end, Fortinet is part of numerous collaborative activities between industry and the U.S. Government, ranging from participation in the IT sector's coordinating council to collaboration on technology development through NIST's National Cybersecurity Excellence Partnership[3] and coordinated cyber threat analysis and response via the Joint Cyber Defense Collaborative[4] (JCDC) run by the Cybersecurity and Infrastructure Security Agency (CISA). Reflecting the fact that cybercrime does not stop at country borders, Fortinet also participates in global initiatives such as the World Economic Forum Centre for Cybersecurity[5] and the Cyber Threat Alliance[6].

Our commitment to collaboration is also reflected in our training initiatives, where we've established meaningful partnerships with leading tech-focused non-profits across the globe to expand the talent pool and awareness of jobs in the field. We established a Veterans Program Advisory Council, comprised of veteran non-profit representation from across the Five Eyes, given the strong correlation between skills gained by veterans during their time in service to the needs of the cyber workforce. This council helps us gain deeper insights into the needs of the veteran community and enables us to continually evolve our programs to better serve them. These

[1] https://www.fortinet.com/corporate/about-us/about-us
[2] https://training.fortinet.com
[3] https://www.nccoe.nist.gov/news-insights/ncep-mechanism-partnering-nccoe
[4] https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative
[5] https://centres.weforum.org/centre-for-cybersecurity
[6] https://www.cyberthreatalliance.org/

collaborations are essential to broadening our impact and ensuring we attract enough talent to close the industry gap. The individuals we support will enter the cyber field across a variety of industries, like the energy or education sectors, working to safeguard corporate networks and critical infrastructures—ultimately ensuring a more secure and resilient nation. Our training could be utilized by all organizations represented here today. No one is immune and cybersecurity is all our responsibility.

State of the Cyber Workforce

As the cybersecurity landscape becomes increasingly complex, the demand for skilled professionals continues to grow with more than 500,000 cybersecurity professionals required to address the workforce gap within the U.S.[7] As part of our training initiatives, we place a strong emphasis on direct engagement with key stakeholders. Each year, we conduct a skills gap report, surveying 1,850 IT and cybersecurity decision-makers across 29 countries, with the U.S. contributing a significant 300 respondents. The findings are compiled into our annual *Cybersecurity Skills Gap Global Research Report*, now in its fourth year of publication. Our latest 2024 report revealed that 70% of global organizations believe the shortage of skilled cybersecurity professionals is escalating security risks. That statistic rises to 75% for U.S. respondents.[8]

In the past year, nearly 90% of organizational leaders said their enterprise experienced a breach that they can partially attribute to a lack of cyber skills. Despite many organizations adopting creative strategies to recruit, hire, and retain qualified cybersecurity professionals to fill positions, 51% of leaders say the talent pools for their needed skill sets are generally lean. These ongoing recruitment challenges represent a significant and dangerous supply problem for the industry, with 54% of enterprises noting that they continue to struggle to recruit cybersecurity talent.

While there are numerous hurdles associated with recruitment and hiring, leaders also noted that the retention of skilled cybersecurity practitioners is also a challenge. Half of respondents said that offering employees sufficient training and upskilling opportunities was the biggest hurdle to keeping qualified practitioners on staff.

[7] https://homeland.house.gov/2024/09/24/chairman-green-introduces-cyber-pivott-act-to-tackle-government-cyber-workforce-shortage-create-pathways-for-10000-new-professionals/
[8] https://www.fortinet.com/content/dam/fortinet/assets/reports/2024-cybersecurity-skills-gap-report.pdf

Barriers to Entry

The cybersecurity workforce gap has been exacerbated by several interconnected challenges ranging from lack of standardization and awareness of cybersecurity roles to competition for skilled professionals in adjacent fields. Among the most significant challenges, however, are the barriers to entry for both newcomers to the field and existing professionals seeking career advancement. Based on our research and insights from numerous partnerships, the most pressing and widespread issue in this regard is access to education and training. While financial constraints are often a factor for those looking to start a career in the field, a major obstacle remains the persistent reliance of companies and government agencies on traditional four-year degrees as a primary requirement for cybersecurity roles. This outdated requirement should no longer serve as a default filtering mechanism in the hiring process.

Through our collaborations with hundreds of academic institutions, we have observed a growing number of technical schools, colleges, and universities launching two-year degree programs that effectively prepare students for a range of cybersecurity roles. Additionally, many industry stakeholders have made significant strides in providing high-quality cybersecurity industry training at little or no cost to aspiring professionals. Since the beginning of 2020, Fortinet has been offering its entire catalog of self-paced cybersecurity certification training free of charge to all individuals looking to enter the field or advance their careers. Other organizations, both within and beyond the cybersecurity sector, have taken similar steps to expand access to industry-recognized training.

While not a substitute for formal academic education, industry training and certification play a crucial role in equipping new entrants with the practical knowledge and hands-on skills-based experience that isn't always available through traditional degree programs. Our top level of certified professionals, who have earned the title of Fortinet Certified Experts (FCX), tell us repeatedly that their expertise was mostly obtained through hands-on experience. To address the cybersecurity workforce gap effectively, we all need to remove as many barriers to education as possible, while hiring organizations must recognize and embrace alternative pathways to competency and expertise.

The Needed "Spark": Awareness of Cybersecurity as a Career

Cybersecurity has evolved from an obscure technical concept to become part of our household vocabulary, often happening for all the wrong reasons. However, we must seize this newfound

visibility and use it as an opportunity to inspire young students to pursue careers in cybersecurity. Just as children come home from school and talk to their parents about becoming a doctor, firefighter, or police officer, we must challenge ourselves to make “Cyber Threat Hunter" a part of that conversation. In many instances, waiting until high school or college to influence career decisions is too late.

This goal is not only achievable but already yielding results. We have seen firsthand the impact of early engagement through our extensive work with K-12 schools across the United States. In 2022 Fortinet participated in the White House’s National Cyber Workforce and Education Summit. This initiative brought together government and private industry leaders to discuss how we could collectively address the pressing issue of workforce development in cybersecurity. We were grateful for this opportunity to participate, as it challenged us to rethink the approach and responsibility of the Fortinet Training Institute.

In response, our experienced team of cybersecurity curriculum content developers began adapting our enterprise security awareness and training service for the education sector with a focus on equipping K-12 staff and faculty with the knowledge to become more cyber-aware. We offered this training at no cost to school districts and private schools across the U.S., and the feedback was overwhelmingly positive.

To demonstrate the selfless nature of the educators in this country, many asked if we could also develop a curriculum to teach cybersecurity directly to K-12 students. Recognizing the urgent need for this type of education, we once again were tasked with evolving our role and responsibility at the Fortinet Training Institute. We immediately hired a dedicated team of K-12 curriculum developers - former educators - who now focus exclusively on creating age-appropriate cybersecurity content for students, teachers, and parents while leveraging the expertise of the cybersecurity professionals in our organization.

Our programs now introduce cybersecurity concepts as early as kindergarten and evolve into more career-oriented content as students progress through later grades. To date, this program is active in 43 states, and has issued more than 700,000 licenses to our content. Taking a holistic approach - engaging students, teachers, parents, and staff - is critical to fostering a cybersecurity-aware culture and sparking interest in cyber careers at an early age.

We are seeing many states across the U.S. take a leadership role in this as well. States, such as Nevada, Nebraska, North Carolina, Rhode Island, South Carolina and Tennessee, are bringing cyber education to younger students by requiring a credit in computer science to be eligible for high school graduation. Tennessee has taken it a step further by including a credit in cybersecurity as an alternative to the requirement. We believe these efforts are highly appropriate and necessary to expand awareness, and hope additional states take similar action.

Beyond inspiring the next generation, we must also do more to attract existing underutilized talent pools, particularly individuals transitioning into new careers. A key example is military veterans moving into civilian roles. Many veterans possess highly relevant skills—including situational awareness, leading in a crisis, and the ability to perform under pressure—that are invaluable in cybersecurity. While technical skills can be taught, these innate attributes are critical in many cyber roles. However, our partner organizations that support veterans, such as VetSec Inc. and Hire Heroes USA, frequently report that their members lack awareness or confidence in how their military experience translates into cybersecurity careers. Addressing this gap is essential to unlocking a wealth of talent that is both capable and well-suited for the field.

Lack of Clarity on Career Paths and Roles

While some traditional cybersecurity roles—primarily technical roles—are relatively well-defined, the field has evolved to encompass a vast and increasingly complex range of roles and required skill sets. This rapid evolution has led to significant ambiguity, making it challenging for individuals seeking education and training to navigate their path into a cybersecurity career.

Organizations such as NIST and the National Initiative for Cybersecurity Education (NICE) have made great strides in developing cybersecurity career pathways. As cybersecurity roles evolve at a rapid pace, these efforts must continue and evolve to ensure these frameworks remain current and, more importantly, that they serve as a benchmark for standardizing cybersecurity roles across government and industry.

Clearly defined career pathways are not only essential for individuals entering the field but also for current professionals looking to advance. Establishing standardized career pathways is crucial in efficiently upskilling the existing workforce and creating a pipeline of experienced professionals for senior and leadership roles as part of long-term succession planning. By creating greater clarity and consistency in cybersecurity career paths, we can better equip both new entrants and

seasoned professionals to meet the growing demands of the industry. At Fortinet, we have seen increasing interest over the last few years in courses in security operations (SecOps) and cloud-based security architecture. In response, we updated our entire certification program in 2023 to meet the needs of the rapidly evolving threat landscape and job market needs.

Recruitment and Retention

Recruiting and retaining cybersecurity professionals remain significant challenges in addressing the cyber workforce shortage. Unlike well-established fields such as accounting—where hiring for a CPA, for example, follows a clear and standardized process—cybersecurity is still a relatively young profession with roles and responsibilities that are constantly changing. This ongoing evolution makes the recruitment process uniquely difficult.

Many recruiters struggle to develop accurate job descriptions or identify the appropriate skills needed for cybersecurity roles. As a result, they often rely on arbitrary requirements, such as mandating a traditional four-year degree, which unnecessarily excludes a large pool of highly qualified candidates. This underscores the critical importance of efforts by organizations like NIST and the NICE[9] initiative, which is making significant strides in standardizing cybersecurity roles and career pathways. Establishing clearer role definitions and hiring frameworks will be essential in improving both recruitment and retention across the industry.

Retention efforts are just as critical as recruitment in addressing the cybersecurity workforce gap. Attracting new talent is only part of the solution – organizations must also focus on keeping skilled professionals engaged, motivated, and growing within their careers. High turnover rates not only exacerbate the workforce gap but also lead to knowledge loss, increased training costs, and disruptions in cybersecurity operations, all of which can weaken an organization's security posture.

Moreover, cybersecurity professionals often face high levels of stress, burnout, and job dissatisfaction due to long hours, intense workloads, and the ever-evolving threat landscape. Without clear career pathways, opportunities for advancement, and continuous upskilling, many professionals may leave for better-defined roles in other industries.

Investing in retention strategies, such as competitive compensation and professional development, ensures that organizations maintain a strong, experienced cybersecurity workforce.

[9] https://www.nist.gov/itl/applied-cybersecurity/nice/about

Ultimately, addressing retention challenges is key to building a sustainable and resilient cybersecurity talent pipeline.

Ongoing Progress to Address the Cyber Workforce Gap

While there is work to be done to develop the future cybersecurity workforce, it's encouraging that there are significant efforts already underway across industry, academia, and government to address this challenge. Many industry-leading organizations are working to meet the challenge head on. Fortinet, for example, has committed to training 1 million people over a five-year period (2021-2026) through our Fortinet Training Institute. We are slightly ahead of our goal with more than 630,000 trained as of Dec. 31, 2024.[10] By providing free, self-paced cybersecurity training and working with academic institutions, non-profits, global organizations and government agencies, Fortinet is helping to equip individuals with the skills needed to enter and advance in the field.

Additionally, through our many academic partnerships, Fortinet has seen several innovative post-secondary institutions recognize the importance of alternative education pathways. Some of our academic partners, such as Northeast State Community College in Tennessee, Sinclair Community College in Ohio, and Mohave Community College in Arizona have introduced two-year cybersecurity degree programs that provide students with skills based, relevant knowledge and hands-on training and industry certifications. These programs are effectively preparing students for entry-level cybersecurity roles. Effective degree programs, along with government-backed workforce initiatives, apprenticeship programs, and veteran transition efforts, are making cybersecurity careers more accessible to a broader talent pool. While these initiatives represent meaningful progress, continued investment and collaboration will be essential to closing the cybersecurity workforce gap at scale.

What More Can Be Done?

Despite ongoing efforts to close the cybersecurity workforce gap, more comprehensive solutions are needed to address systemic challenges. First, organizations and policymakers must expand and embrace alternative pathways into cybersecurity roles beyond traditional four-year degrees. Increased investment in shorter degree programs, vocational training, industry-recognized certifications, and apprenticeship programs can help individuals enter the field quickly and

[10] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-announces-progress-towards-mission-to-tackle-cybersecurity-skills-shortage

transition from adjacent fields into cybersecurity. Additionally, upskilling and reskilling of existing employees must be prioritized. This is necessary in order to provide clear career progression opportunities to retain critical talent and ensure robust succession planning.

Stronger partnerships between industry, academia, and government agencies can also enhance workforce development. Businesses should collaborate with educational institutions to ensure curricula align with real-world cybersecurity needs. Governments should continue to provide incentives for companies and academic institutions that invest in cybersecurity training, education and workforce development. These public–private partnerships can help to ensure portability of experienced cybersecurity professionals between government and private sector roles and help to bridge the workforce gap at scale.

The work of this Committee is also key to expanding awareness of cyber roles in the workforce and closing the cyber workforce gap. If enacted, the proposed Cyber PIVOTT Act would have a positive impact across both the public and private sector with its emphasis on cybersecurity scholarships for students in partnership with community colleges and technical schools, as well as developing internships and Federal job opportunities for graduates of this program.

Finally, the cybersecurity profession must improve awareness and branding. Many potential candidates are unaware of the range of cybersecurity careers available. Public awareness campaigns, starting at the high school level, can help attract more individuals to the field, ensuring a sustainable and resilient workforce for the future.

Conclusion

Our digital ecosystem is constantly under attack by hackers, cyber criminals and nation-state actors. Teamwork across the public and private sector is crucial to ensure strong national cyber resilience. A robust and skilled workforce is foundational to this resilience – making today's discussion both about jobs and our national security.

I have spent my career focusing on empowering others with the skills to successfully enter or advance within the cybersecurity workforce. I am confident that with the right tools, incentives, and partnerships we can ensure the cyber workforce pipeline is strengthened and that today's skills gap becomes yesterday's issue. To achieve this, we need bold and consistent action that can scale – ranging from early training of our children on cyber awareness through to technical training

on secure coding practices. Efforts like the Cyber PIVOTT Act are critical examples of how private and public sector collaboration can ensure this workforce pipeline is strengthened.

Thank you for the opportunity to be part of this hearing and I stand ready to assist the Committee on this important topic. I look forward to today's discussion and I welcome your questions.