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.

Testimony for the Record

Submitted to the

U.S. House of Representatives Committee on Homeland Security

For the Hearing

Preparing the Pipeline: Examining the State of America's Cyber Workforce

February 5, 2025
310 Cannon House Office Building
Washington, DC

David J. Russomanno, Ph.D.
Executive Vice President for Academic Affairs and Provost
Professor of Electrical and Computer Engineering
360 Administration Building
The University of Memphis
Memphis, TN 38152

INTRODUCTION

Chairman Green, Ranking Member Thompson, and distinguished members of the committee, thank you for the opportunity to appear before you today. I express my gratitude to Chairman Green for your overall leadership on cybersecurity workforce priorities and for introducing the Cyber PIVOTT Act.

My name is David Russomanno. I am an electrical and computer engineer by training and have the honor of serving as Executive Vice President for Academic Affairs and Provost at the University of Memphis. The University of Memphis is a Carnegie R1 university, which is a prestigious designation meaning we are a high-performing, comprehensive research institution. Before becoming an academic more than thirty years ago, I worked as an engineer for corporations in the defense, automotive, and computer sectors.

I have conducted fundamental research with support from various sponsors, including the National Science Foundation (NSF), Army Research Laboratory (ARL), state and local governments, and the private sector to advance the state-of-the-art in some areas and apply the state-of-the art in other areas. Most importantly, I have devoted a significant portion of my career as an engineering professor, department chair, and dean of engineering and technology, before assuming my role as Provost, to advance Science, Technology, Engineering, and Mathematics (STEM) education focused on initiatives to grow the student pipeline and produce successful student outcomes aligned with workforce needs. For example, I have served as principal investigator or co-principal investigator on NSF-administered Scholarships for STEM (S-STEM) [1] and CyberCorps Scholarship for Service (SFS) Defending America's Cyberspace [2] projects.

Per the U.S. Department of Commerce, about 500,000 cybersecurity positions are open. Those vacancies place our nation's digital infrastructure, intellectual property, and privacy at significant risk from threat actors who are looking to exploit our vulnerabilities. The Cyber PIVOTT Act is an important contribution toward addressing this deficiency.

In addition, we at the University of Memphis are implementing an additional and needed contribution so that 4-year universities are doing even more by strengthening pathways from applied technology programs, including applied cybersecurity, to appropriate baccalaureate programs.

BACKGROUND

Rightly so, prior testimony to this and other Congressional committees has focused on various cyber threats to the U.S. presented by a variety of threat actors, including nation-states, criminal organizations, and individuals. A parallel threat, which has been noted in prior hearings, is the loss of human intellectual capital that could be marshalled toward strengthening our cybersecurity infrastructure. I am pleased that this 119th Congress is considering steps to address this threat through the Cyber PIVOTT Act, which will expand support for education and training programs at community colleges and technical schools. These institutions, to the best of my knowledge, are eligible only as sub-awardees of the partnering 4-year CyberCorps (SFS) institutions. Therefore, the Cyber PIVOTT Act will broaden and strengthen the workforce and contribute toward forming a panoply of cybersecurity readiness at scale desperately needed by our nation.

CHALLENGES

There are significant challenges to forming that comprehensive cybersecurity readiness to which I just referred, with many opportunities for post-secondary education, as well as the public and private sector to work collaboratively to address the challenges.

Higher Education

As summarized last week in the American Society for Engineering Education's (ASEE) *First Bell* publication [3], data shows that many colleges are struggling to align education with workforce needs. As referenced by ASEE *First Bell* and described in Forbes by Perna [4]: "Historically, institutions of higher learning have been slow to pivot their offerings to meet current workforce needs. The inertia is real. The problem is, Gen Z is smart enough to know it." I add that with respect to our cybersecurity readiness, adversaries are smart enough to know it too.

Although the focus of the Perna article is Artificial Intelligence (AI), many of the highlighted issues are relevant to the applied cybersecurity workforce. For example, Perna cites a survey conducted by Hult International Business School in which 85% of recent college graduates who participated in the survey agreed with the statement [4]: “I wish my college had better prepared me for the workplace.” The Perna article goes on to state [4]: “The call here is simply for the higher education system to better align with what today’s students and employers need—before it’s too late.”

The Perna article could understandably be interpreted as the higher education system is solely responsible for preparing its graduates to meet workforce needs. However, in high demand areas, most notably and critically in cybersecurity, the private sector may prefer to recruit experienced employees from other companies rather than creating entry-level positions and hiring new graduates. Such an approach contributes toward an unsustainable “race for talent” rather than developing deep and sustained partnerships with educational institutions and the public sector to grow the talent pipeline at scale and in a sustainable manner. Such a “race for talent” scenario may also have the unintended consequence of presenting significant barriers to entry to the profession for new graduates who may have interest but limited experience in cybersecurity.

Examples of sustained private sector and higher education best practices include “invested” program advisory boards that provide input to academic programs to guide their educational objectives, curriculum, and student learning outcomes. The advisory input is then supplemented with ample opportunities for students to augment their program of study with compensated and meaningful experiential learning opportunities, including internships sponsored by advisory board members, to become better prepared applicants upon graduation.

A service commitment proportionate to student sponsorship as incorporated into CyberCorps (SFS) and the Cyber PIVOTT Act should serve as an important model for the private sector to strengthen its commitment toward contributing to a sustainable cybersecurity workforce at scale. Opportunities for incentivizing such a private sector commitment at the federal and state levels are encouraged, especially given the

dependencies of the U.S., including the U.S. military, on private sector infrastructure maintained with insufficient levels of cyber resilience as noted by Rear Admiral (Ret.) Montgomery in his recent testimony to this Committee [5].

By focusing on retaining cybersecurity professionals, the federal government can avoid the high costs of continually recruiting and training new employees. Cybersecurity experts in critical infrastructure roles are costly to train, and turnover disrupts operations while forcing taxpayers to bear the expense of new hiring and training processes. Additionally, when private companies invest in collaborative training programs, they help bridge the skills gap, easing the financial burden on the federal government by sharing the responsibility for workforce development.

Traditional Pathways to and Barriers preventing joining the Cybersecurity Workforce

Although many comprehensive universities across the U.S. offer a 4-year program of study in cybersecurity and closely related fields, there are often barriers for student entry into such programs. For example, rigorous computer science and engineering programs, which incorporate cybersecurity education into their curricula, require extensive mathematics and basic sciences preparation, such as including Calculus in the first year of a 4-year program of study. These programs are based on foundational knowledge acquired through courses with substantial prerequisite chains. First-principle-based programs are critically important to our nation to prepare students to advance the-state-of-the-art in a variety of fields. However, these types of programs may not always be the most appropriate educational pathway for students interested in applying the-state-of-the-art versus acquiring foundational knowledge at the baccalaureate level, which may be required for graduate programs in computer science and engineering focused on research to advance the state-of-the-art.

Moreover, the time required to earn a 4-year degree, particularly for students who may be working during their program of study, may also present a hurdle that is too high. Therefore, the opportunity to earn cyber security credentials through community colleges and technical schools will present an attractive option to both traditional

students and those who may be considering career change. The Cyber PIVOTT Act is appropriately focused on community colleges and technical schools as a component for increasing the cybersecurity workforce at scale.

Given the appropriate focus of the Cyber PIVOTT Act on community colleges and technical schools, it is important for 4-year institutions, including comprehensive R1 institutions, to strengthen pathways from applied technology programs, including applied cybersecurity, to appropriate baccalaureate programs.

A vitally important aspect of the Cyber PIVOTT Act is the DELAYED SERVICE clause in which students who immediately after completion of their community college or technical school program enroll in a 4-year program may delay their service obligation until after receiving the 4-year degree. This clause will be an attractive incentive for many students as they are considering career goals. I encourage that both the public and private sectors be incentivized in some appropriate manner to consider continued support of Cyber PIVOTT Act recipients to pursue a 4-year degree at a later stage of their career if students do not pursue a 4-year degree immediately after completing their community college or technical school program.

By partnering with universities, community colleges, and technical schools, the federal government can create tailored cybersecurity programs that build upon students' prior learning experiences such as military service and technical certifications. This collaborative approach allows the government to leverage existing skills and expertise without having to start from scratch, ultimately maximizing the return on its investment in workforce development.

Although significant progress has been made in many states with articulation agreements from community colleges to 4-year universities, especially for general education courses, arguably the same progress has not been made with respect to articulation agreements with programs offered by technology schools.

Per a report by the Education Commission of the States, at least 31 states have policies requiring a transferable core of lower-division courses and statewide guaranteed

transfer of an associate degree [6]. However, my experience is that these articulations primarily focus on a general education core, which is a component of most associate of science (AS) and associate of arts (AA) degrees or very similar programs, and may exclude or not optimally articulate courses, knowledge, and skills acquired through associate of applied science (AAS) programs creating a barrier to baccalaureate degree completion. For example, within the State of Tennessee, there are limited articulation agreements between programs offered by Tennessee Colleges of Applied Technology (referred to as TCATs) to baccalaureate programs offered by 4-year universities. However, progress is being made, especially with articulations from AAS to Bachelor of Applied Science (BAS) programs. The University of Memphis (UofM) is striving to be a national leader to accelerate the AAS-to-BAS transfer pathway through **The Polytechnic @ UofM** initiative.

SUPPORTNG WORKFORCE GROWTH AT SCALE

The Polytechnic Model

A polytechnic [7] may be regarded as an educational institution or unit within an institution that primarily focuses on applied sciences, applied technology, and career pathways.

Although polytechnic has several definitions and a variety of implementations, some recurring themes are as follows:

- Offer real-world experiences and industry partnerships
- Provide hands-on training with emphasis on practice and applying the state-of-the-art versus advancing it
- Serve as a complement to first-principle-based curricula (e.g., traditional computer science and engineering programs) in which the fundamental concepts or assumptions on which a theory, system, or method is based [8] are foundational to progression in the curriculum

To attain their ideal definition, polytechnic programs must align with workforce needs and demonstrate the ability to pivot to meet rapidly changing knowledge and skillset demands by the workforce (arguably requiring a more rapid feedback loop with respect to assessing student and workforce needs for continuous improvement than programs that have strong foundations in first principles).

While dean of the Purdue School of Engineering and Technology at Indiana University-Purdue University Indianapolis (now part of Purdue in Indianapolis), I enthusiastically supported the development of an application-oriented Bachelor of Science degree in Cybersecurity and a Master of Science degree in Cybersecurity and Trusted Systems. Distinguishing features of these programs included: i) minimization of extensive course prerequisite chains; ii) team-based and project-based courses and labs; iii) “invested” advisory boards as previously mentioned; iv) significant student participation in experiential learning opportunities, including paid internships; and v) flexibility in accommodating transfer from 2-year institutions for the BS program and accommodating a variety of undergraduate BS degrees in preparation for admission to the MS program. Moreover, both the BS and MS programs incorporated student participation in NSF CyberCorps (SFS), which served as a model to enhance partnerships with the programs’ advisory board and other entities from the private sector.

Now as Provost at the University of Memphis, with strong support from the President of the University and our Board of Trustees, we are launching **The Polytechnic @ UofM** as an important component of the UofM’s *Ascend* strategic plan [9] to better prepare our students for workforce needs with emphasis on a successful outcome for every student.

The Polytechnic @ UofM will serve as the organizational sub-unit within our Herff College of Engineering to host several existing applied technology programs, as well as to launch new applied technology programs to rapidly respond to workforce needs. Implementation includes a Bachelor of Applied Science (with concentrations such as Applied Cybersecurity, Applied AI, and Advanced Manufacturing Supervision) to expand support for student matriculation pathways from the following: i) Tennessee Colleges of

Applied Technology; ii) Community Colleges with associate of applied science programs; iii) private sector training and certification programs; iv) credit for prior learning, including experience gained through military service; and v) other applied technology and vocational institutions across the U.S., all of which are well positioned to benefit from the Cyber PIVOTT Act and to contribute to building a cybersecurity workforce at scale.

CONCLUSION

I am honored to testify today in strong support of the Cyber PIVOTT Act under consideration by the 119th Congress as it will broaden and strengthen the workforce toward forming the panoply of cybersecurity readiness at scale desperately needed by our nation. Moreover, consideration of the Cyber PIVOTT Act highlights the urgency for 4-year institutions to develop and align a portion of their STEM academic portfolio to provide a seamless pathway to baccalaureate programs for students pursuing applied technology programs, including applied cybersecurity, from community colleges and technical schools.

The Polytechnic @ UofM is an important new initiative leveraging partnerships within the State of Tennessee and beyond to contribute toward a national model for addressing workforce needs in applied technology areas and as an important complement to first-principle-based baccalaureate and graduate programs in computer science, engineering, and closely related fields of study.

REFERENCES

1. NSF Scholarships in Science, Technology, Engineering, and Mathematics Program (S-STEM): https://new.nsf.gov/funding/opportunities/s-stem-nsf-scholarships-science-technology-engineering-mathematics (link active as of February 1, 2025)

2. NSF CyberCorps Scholarship for Service (SFS): https://new.nsf.gov/funding/opportunities/sfs-cybercorps-scholarship-service (link active as of February 1, 2025)

3. ASEE First Bell: https://www.asee.org/publications/NEWSLETTERS/First-Bell (link active as of February 1, 2025)

4. M.C. Perna, “New Data Reveals Just How Deep The College Crisis Goes,” *Forbes*, January 28, 2025: https://www.forbes.com/sites/markcperna/2025/01/28/new-data-reveals-the-depth-of-college-crisis/ (link active as of February 1, 2025)

5. RADM (Ret.) Montgomery, “Unconstrained Actors: Accessing Global Cyber Threats to the Homeland,” A House Committee on Homeland Security hearing, January 22, 2025, https://homeland.house.gov/wp-content/uploads/2025/01/2025-01-22-FC-HRG-Testimony.pdf (link active as of February 1, 2025)

6. Education Commission of the States: “50-State Comparison: Transfer and Articulation Policies - Education Commission of the States,” https://www.ecs.org/50-state-comparison-transfer-and-articulation/ (link active as of February 1, 2025)

7. “Polytechnic,” Merriam-Webster.com Dictionary, Merriam-Webster, https://www.merriam-webster.com/dictionary/polytechnic (link active as of February 1, 2025)

8. “First Principles,” Oxford Learner’s Dictionary, https://www.oxfordlearnersdictionaries.com/us/definition/american_english/first-principles (link active as of February 1, 2025)

9. Office of the President of the University of Memphis, Ascend strategic plan 2023-2028, https://www.memphis.edu/president/strategic-plan/index.php (link active as of February 1, 2025)

Testimony of Mr. Chris Jones
President and Chief Executive Officer
Middle Tennessee Electric

To the United States House of Representatives, Committee on Homeland Security

"Preparing the Pipeline: Examining the State of America's Cyber Workforce"

Wednesday, February 5, 2025

Introduction

Chairman Green, Ranking Member Thompson, and Members of this Committee: Thank you for the opportunity to testify before you today. My name is Chris Jones, and I serve as President and CEO of Middle Tennessee Electric (MTE). I am testifying today to provide my own insights as a co-op leader, but also representing the National Rural Electric Cooperative Association (NRECA) and nearly 900 electric cooperatives across the country.

MTE is the largest electric cooperative in the Tennessee Valley Authority (TVA) region and the second largest in the United States, serving more than 750,000 Tennesseans. Our service territory includes 15,000 miles of distribution lines over 2,200 square miles – or more than double the landmass of Rhode Island – across 11 Middle Tennessee counties, primarily Rutherford, Cannon, Williamson, and Wilson. MTE employs around 540 people in six local offices and its Murfreesboro headquarters.

NRECA is the national trade association representing nearly 900 rural electric cooperatives across the country. Electric co-ops are not-for-profit, at-cost electric utility providers focused on delivering affordable, reliable, and secure electricity to over 42 million Americans in 48 states. We are unique in the electric utility sector in that we are private sector, operate without profit incentives, and are owned and governed by the people we serve.

Electric co-ops were created with a mission to address the distinct challenges associated with providing electric service to rural communities, which typically have lower population densities, are more residential, and less affluent than the industry average. This means that cooperatives are constantly asked to do more with less, and they deliver. Cooperative members give their utilities the highest customer satisfaction scores, on average, in the electric sector.

Electric co-ops are owners and operators of some of our nation's most critical infrastructure, such as power plants, electrical substations, and transmission and distribution lines. This also includes infrastructure to generate or provide power for more than 150 military facilities and

installations across the United States. We also serve as economic drivers and lifelines for critical industries and services in rural communities, including hospitals, schools, emergency services, and food and agriculture production.

Protecting America's electric grid from cyber and physical threats is a top priority for the nation's electric cooperatives. Accomplishing this important task presents its own set of challenges. The same circumstances that made it difficult to invest in electrifying rural America nearly a hundred years ago, including being isolated from the larger customer bases and diverse talent pools available in urban areas, persist today. These challenges add difficulty in investing in the people, processes, and technologies needed to secure the grid in rural communities.

We have a saying in our industry: If you have met one electric co-op, then you have met exactly one electric co-op. The nearly 900 electric co-ops across the country all come in different shapes and sizes. Although MTE does not fit the profile of the typical electric cooperative, all our challenges share similar themes. MTE is fortunate to not have to wrestle with some of the more intense challenges of the rural cyber workforce issue. However, with my over two decades of experience working for the cooperative, I have seen how MTE has tackled those issues and can share how co-ops are impacted across the broader community.

I will share some of the challenges electric co-ops face in securing the grid, specifically in recruiting, retaining, and developing cybersecurity professionals. I also will highlight how electric cooperatives are overcoming these challenges through the help of resources developed by NRECA and the smart investment of federal dollars.

Threat Landscape

Cyber threats jeopardize electric reliability and pose a significant risk to the nation's safety, security, and economic well-being.

The cybersecurity threat landscape for electric utilities is increasingly complex and perilous. Electric utilities are prime targets for cyberattacks due to their pivotal role in both national security and daily life. Threat actors, ranging from state-sponsored groups to cybercriminals, exploit vulnerabilities for geopolitical or monetary gains. These attacks have the potential to disrupt the power supply, causing widespread outages and economic damage. The rise of sophisticated malware, ransomware, and phishing attacks further exacerbates the risk.

Additionally, smart grids, distributed energy resources (DER), and Internet of Things (IoT) devices – while improving efficiency – introduce new targets. Defending our infrastructure against new challenges and evolving cybersecurity threats requires strong cybersecurity measures, continuous monitoring, proactive threat intelligence, and a skilled workforce capable of safeguarding these critical assets against increasingly sophisticated attacks.

Workforce Challenge

As cyber threats grow more complex and prevalent, particularly those targeting critical infrastructure like electric utilities, the demand for cybersecurity professionals will continue to grow. In 2023, the National Institute of Standards and Technology (NIST) reported that only 20% of business leaders at energy utilities surveyed felt confident that they had the cyber talent they needed. These experts are essential for developing and implementing advanced security measures, conducting threat assessments, and responding to incidents swiftly and effectively.

Despite the evolving and complex threat environment, there are still around 450,000 cybersecurity vacancies in the United States. We need more cyber professionals to safeguard critical infrastructure across the country. While no sector or region is immune to the underlying difficulties of recruiting and retaining skilled cyber professionals, these challenges are exacerbated by the unique and inherent characteristics of electric cooperatives and rural areas.

Electric cooperatives are not-for-profit, at-cost utility providers, meaning we operate without a profit incentive. This model allows co-ops to serve more remote areas with low population density, averaging only 25% of the customers and revenue per mile of line, compared with the rest of the industry. Unlike investor-owned utilities, electric cooperatives operate without shareholders. Because of this, financing costly investments often requires reliance on debt, which must be approved by each cooperative's Board of Directors and ultimately paid back through rates paid by their members. Boards are careful stewards of their members' resources and mindful of the economic impact of rate increases to end-of-line consumer-members, particularly given that cooperatives provide service to 92% of the nation's persistent poverty counties.

Therefore, investing in the most sophisticated security technologies and competing for skilled cyber professionals can be a challenge. Recruitment and retention for these professionals are complicated by competitive salaries and benefits offered by larger, urban-based firms, which can lure away skilled workers. Cooperative staff, whether in IT, cyber, or non-technical roles, often wear multiple hats within the organization.

Since electric cooperative service areas are often largely rural, they can be seen as less attractive to professionals seeking vibrant social and professional networks, further complicating recruitment efforts. Rural areas also face significant challenges in developing a robust cybersecurity talent pool. One of the primary issues is the limited access to specialized education and training programs. Many rural regions lack institutions that offer advanced cybersecurity courses, making it difficult for residents to acquire, and keep up to date on, the necessary skills and changing techniques and tactics locally. Additionally, the overall awareness of cybersecurity careers is often lower in these areas, leading to fewer individuals pursuing this field.

Cyber PIVOTT Act

We want to thank and acknowledge Chairman Green's leadership on introducing the Cyber PIVOTT Act during the last Congress. This proposed legislation was a positive step toward addressing the complex and multifaceted difficulties surrounding the cyber workforce in general, and particularly in rural areas.

NRECA was particularly pleased with the inclusion of language that would extend cybersecurity internship opportunities to critical infrastructure providers in rural communities. We hope this provision will raise the visibility of electric co-ops as a viable and rewarding career path in cyber. Developing a talent pipeline with off-ramps into rural communities will help grow a local, skilled cybersecurity workforce to protect critical infrastructure in these communities. The Cyber PIVOTT Act will bridge the skills gap, enabling rural communities to strengthen their cyber defenses and secure their critical infrastructure.

Electric Cooperatives Solutions

Electric cooperatives are identifying innovative ways to address cyber workforce challenges. Co-ops are increasingly focused on building local talent through partnerships with educational institutions and providing opportunities for remote work and professional development. We are also seeing partnerships between large generation and transmission cooperatives, statewide associations, and distribution co-ops to share tools, equipment, and expertise across shared systems to bolster cyber defenses. In the Tennessee Valley, we have a long history of collaboration and partnership among TVA and its 153 local power companies, which are electric cooperatives and municipally owned electric systems. This partnership extends into the cybersecurity arena. Our state and Valley wide associations have made cybersecurity a top priority, from conferences and training to work groups and webinars.

Additionally, NRECA is leveraging members' fees and federal dollars to build a robust cybersecurity program to assist cooperatives in attracting cybersecurity talent, building professional and mentoring networks, and providing skill development and training opportunities.

The Rural Cooperative Cybersecurity Capabilities (RC3) Handbook is a series of comprehensive guides designed for specific roles within cooperatives to help enhance their cybersecurity posture. Last year, NRECA published the final handbook in the series targeted toward HR managers to provide practical advice on implementing recruitment and retention strategies and employing ongoing professional development.

NRECA and electric cooperatives are also utilizing funds through the Department of Energy's (DOE) Rural and Municipal Utility Cybersecurity Program, or RMUC, to make investments in cybersecurity technology, training, and educational opportunities. RMUC is a generational opportunity to improve the cybersecurity posture of electric cooperatives by providing resources to critical infrastructure operators with the greatest need of support.

Through RMUC, more than 200 personnel from 123 cooperatives participated in an intensive, three-day training program last year, hosted by DOE. The program was designed to advise attendees on how to improve cybersecurity for industrial control systems and operational technology.

Additionally, NRECA was awarded $9 million in RMUC funds to strengthen peer-to-peer information sharing, boost mutual assistance, promote cybersecurity awareness, and build

internal expertise through the expansion of the NRECA Threat Analysis Center (TAC) and the development of the Cyber Champions Program.

Finally, NRECA hosts an annual technical conference, known as Co-op Cyber Tech, that brings together cybersecurity professionals from rural electric cooperatives to collaborate, share knowledge, and develop skills. The event features hands-on content and sessions on the latest cybersecurity trends and technologies.

Conclusion

Cyber threats endanger electric reliability and present a major risk to the nation's safety, security, and economic stability. Electric cooperatives have a mission to safeguard the electric grid of the communities we serve and live in ourselves.

While electric cooperatives are making smart investments and building strategic partnerships to develop our cyber professionals, more work needs to be done. Initiatives like those in the Cyber PIVOT Act bring much-needed focus to the cyber workforce needs of rural America. Creating a talent pipeline that includes pathways into rural areas will foster a local, skilled cybersecurity workforce to safeguard critical infrastructure in these regions. Co-ops and our rural communities have a lot to offer in protecting America's critical infrastructure.

I thank the Committee for its bipartisan work on this issue and look forward to answering your questions.

PARTNERSHIP
FOR PUBLIC SERVICE

Max Stier

President and CEO

Partnership for Public Service

Written statement prepared for

The House Committee on Homeland Security

Hearing entitled,

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

February 5, 2025

Introduction

Chairman Green, Ranking Member Thompson and members of the committee, thank you for the opportunity to participate in this discussion on strengthening America's cyber workforce. My testimony today will focus on the cyber workforce needs of the federal government.

I am Max Stier, the President and CEO of the Partnership for Public Service, a nonpartisan nonprofit which, over the last 24 years and across administrations of both parties, has been dedicated to building a better government and stronger democracy.

The Partnership was founded on the premise that any organization's best asset is its people and that the federal government needs dedicated, skilled talent to deliver on promises to the American people.

Our organization over the years has produced a number of reports on cyber talent that speak to the themes relevant to today's hearing – developing a comprehensive cyber workforce strategy, improving federal hiring and developing better pipelines into cyber positions encouraging the nationwide development of technology skills.[1] We also help place recent graduates in cyber and artificial intelligence fellowships at federal agencies.[2]

We believe that the federal government should continually modernize its practices and earn the trust of the public. We've recently outlined five key areas for reform in our Vision for a Better Government:[3] develop better government leaders; make it easier to hire and keep great public servants; hold poor performers accountable; unleash the power of data and technology to achieve better public outcomes; and provide efficient, constituent-friendly services to the public.

The Partnership is gravely concerned about escalating actions that undermine the capabilities of the executive branch to carry out mandates from Congress, including protecting our national security with a skilled cyber workforce. The list is growing by the hour – freezing of federal funds, mass firings of federal employees, threatened coercion of all federal employees to leave the workforce and disturbing decisions on access to government systems that impact the private information of your constituents. Collectively, these actions only increase the cyber threat to our country.

By contrast, the committee's approach today is the right one. With respect to the federal cyber workforce, this committee for years has focused on key workforce issues: How do we identify and fill cyber skills gaps throughout the federal government? What is working and not working for the numerous efforts across the federal government – which often are carried out in silos – and how do we leverage success stories across the broader governmentwide cyber workforce? What are ways

[1] Partnership for Public Service, "Cyber In-Security: Strengthening the Federal Cybersecurity Workforce" (July 2009), "Cyber In-Security II: Closing the Federal Talent Gap" (April 2015), "Leading Ambitious Technology Reforms in Government" (Aug. 2017).
[2] Partnership for Public Service, Cybersecurity and Artificial Intelligence Talent Initiative, https://gogovernment.org/fellowship/cybersecurity-ai-talent-initiative/
[3] Partnership for Public Service's "Vision for a Better Government" (Aug. 15, 2024), available at https://ourpublicservice.org/publications/vision-for-a-better-government/

to best foster federal, state/local and private sector coordination in strengthening the cyber workforce?

As members of this committee have noted in past hearings, the cyber responsibilities of the federal government are vast – not only protecting the systems of federal agencies but working in partnership to protect the cyber spaces of our nation's critical infrastructure, the public at large, and all levels of government. This hearing today provides a thoughtful forum on how to equip the federal workforce to address these urgent challenges.

Status of the Federal Cyber Workforce

While attention to cyber needs has increased greatly across the federal government over the last decade, the gaps in agencies' needs remain vast. The Partnership's analysis of data over the last five years shows that overall, the federal cyber workforce grew from over 101,000 in 2019 to over 114,000 in 2024.[4] This is far short, though, in meeting the government's overall needs.

For example, the Department of Homeland Security reported to your committee last June that the Department had over 8,000 cyber employees but still had over 2,000 cyber vacancies.[5] That's exactly the type of skills gap analysis – updated regularly – that we need from each federal department and agency so that we can best determine how to fill those gaps and how to align federal efforts with the overall cyber workforce needs of the entire country.

As discussed in your previous hearings on the cyber workforce, we need skills at all levels – entry-level, mid-level (who either already have cyber skills or are good candidates for reskilling) and senior professionals willing to bring their years of expertise into the government. I want to call particular attention to the age demographics in the federal cyber workforce. The percentage of federal cyber workers under age 30 is just under 8%, while those age 50 and over represent 48% of the federal cyber workforce.[6] My recommendations today will offer ways to improve the talent pipeline at all levels, with particular attention to developing the pipeline of future leaders as so many current cyber employees approach retirement.

The committee is well familiar with these challenges and the many studies on the cyber workforce. Notably, the Government Accountability Office first designated information security as a governmentwide High Risk area in 1997 and subsequently expanded it to include the cybersecurity of critical infrastructure and the privacy of personally identifiable information. GAO then identified strategic human capital management within the federal government as a high-risk area in 2001.[7] In

[4] Based on Office of Personnel Management's FedScope data from Sept. 2019 through Sept. 2023, and March 2024, for occupational categories 0854 (Computer Engineering), 1550 (Computer Science), 2210 (Information Technology Management), and 2230 (DHS Cybersecurity Specialist).
[5] House of Representatives Committee on Homeland Security, hearing entitled "Finding 500,000: Addressing America's Cyber Workforce Gap" (June 26, 2024), available at https://homeland.house.gov/hearing/finding-500000-addressing-americas-cyber-workforce-gap/
[6] Analysis based on Office of Personnel Management's FedScope data as of March 2024.
[7] Government Accountability Office, "High Risk Series: An Update" (Jan 1, 2001), available at https://www.gao.gov/products/gao-01-263

a 2024 High Risk update, GAO identified the need to address cybersecurity workforce management challenges as one of ten critical cybersecurity action areas.[8]

In its most recent report on the cybersecurity workforce, GAO reviewed the cybersecurity workforce planning efforts of five federal agencies.[9] GAO found that the Department of Homeland Security had fully implemented most practices that are central to effectively managing the cybersecurity workforce. These practices included (1) setting the strategic direction for the workforce, (2) conducting workforce analyses, (3) developing workforce action plans, (4) implementing and monitoring workforce planning, and (5) evaluating and revising these efforts. The other agencies reviewed, however, were not as consistent in their implementation. Importantly, efforts to destabilize the broader federal workforce will put these hard-earned gains and strategic planning efforts at risk.

Agencies struggling to implement effective cybersecurity workforce practices identified several challenges they faced including:

- Pay disparity between federal agencies and the private sector
- Department budget limitations
- Maintaining an adequate cybersecurity workforce
- Recruiting well-qualified applicants
- Time-to-hire cybersecurity personnel for vacant positions
- High attrition due to cybersecurity employees choosing different career paths

This hearing today is a welcome opportunity to discuss how the federal government addresses these challenges.

Recommendations

The Partnership's recommendations on strengthening the federal cyber workforce largely mirror our broader recommendations for ensuring that our government has the capabilities and capacity to meet its mission and more effectively deliver services to your constituents. Our overall recommendations are reflected in the Partnership's Vision for a Better Government, mentioned above, which highlights five priorities: leadership, federal hiring and retention, performance management, data and technology, and constituent experience with government services.

Much of the federal government's civil service legal framework dates back decades – in the case of our pay and classification system, over 75 years. The passage of the Civil Service Reform Act of 1978 marked the last broad overhaul of governmentwide laws governing personnel management. Our overall framework for human capital is built for a bygone age when a great bulk of the federal

[8] Government Accountability Office, "High Risk Series: Urgent Action Needed to Address Critical Cybersecurity Challenges" (June 2024), available at https://www.gao.gov/assets/gao-24-107231.pdf
[9] Government Accountability Office, "Cybersecurity Workforce: Departments Need to Fully Implement Key Practices" (Jan. 2025), available at https://www.gao.gov/assets/gao-25-106795.pdf

workforce was clerical, not for this day when highly specialized skills such as cybersecurity are critical for protecting the health and safety of the people our government serves.

To its credit, Congress – and this committee in particular – has worked on a bipartisan basis over the years to provide programs and authorities to bolster our nation's cybersecurity defenses and attract cyber talent into government.

Here are ways Congress can build on those efforts:

Maintain nonpartisanship as a bedrock principle of the civil service: Throughout our nearly 25-year history, the Partnership has highlighted the need for updating the ways that the government should manage its workforce, to align with the modern economy. Our 2014 report, Building the Enterprise: A New Civil Service Framework,[10] is just as relevant today as when we issued the report over a decade ago. The report includes recommendations for modernizing the federal pay system to attract top talent, streamlining the process through which agencies deal with poor performers, and strengthening the Senior Executive Service – all recommendations aimed at increasing the accountability of civil servants. As I have said many times in the past, good government starts with good people, and our nation is fortunate to count some of the brightest, most dedicated professionals among its ranks. But too often they succeed in spite of the current system, not because of it.

At the same time, the Partnership has staunchly defended the nonpartisan nature of our civil service. Recent executive actions take us farther from, not closer to, a civil service system that prizes merit, expertise and professionalism free from political interference. A civil service staffed by people chosen for their political loyalty rather than their skill will result in a government less capable of serving the public and more likely to become a tool for retribution and actions counter to democratic principles. A more political government is not a better government for the American people, and it does not help make our country safer.

We welcome a conversation on improving the effectiveness of the civil service framework. Politicizing the workforce and freezing budgets, though, will be extremely damaging to the federal government's current capacity to address our national security needs and to recruit and retain talent to fill critical skills gaps, including in the area of cybersecurity.

Create high expectations for leaders within government: Good leaders create the conditions necessary for employees to perform at their best. In 2019, the Partnership developed the Public Service Leadership Model,[11] recognizing the unique nature of leadership in government, centered on stewardship of public trust and commitment to public good. We believe this model should be the standard for all leaders across the federal government.

Federal leaders—both political and career—should be held accountable for the organizational health of the organizations they helm, including the workforce. Congress should hold leaders responsible for recruiting and retaining highly qualified talent, developing future leaders, engaging

[10] Partnership for Public Service, "Building the Enterprise: A New Civil Service Framework" (April 10, 2024), available at https://ourpublicservice.org/publications/building-the-enterprise/
[11] Available at https://ourpublicservice.org/public-service-leadership-institute/public-service-leadership-model/

employees, and holding subordinate managers accountable for addressing performance. The Partnership recommends Congress require political appointees to have transparent performance plans to drive this accountability at the highest levels of leadership.

Congress also should urge agency leaders to use the annual Federal Employee Viewpoint Survey and the Partnership's Best Places to Work in the Federal Government® rankings[12] to drive better results in their agencies. Employee engagement is not just about happy employees. Higher scores in employee engagement equate to better performance and higher quality service, which in turn become valuable recruiting and retention tools and help agencies better serve the public.

Undertake a comprehensive analysis of existing tools: Congress and the Office of Personnel Management have created a number of tools to better position the government to recruit, hire, train and retain the cyber workforce. These include direct hire authorities, special cyber personnel authorities at the Departments of Defense and Homeland Security, a federal cyber rotation program, the National Institute of Standards and Technology's National Initiative for Cybersecurity Education (NICE), and numerous agency programs such as the National Security Agency's support for cyber clinics in various states and the Department of Labor's country-wide cyber apprenticeship program.

Within the jurisdiction of this committee, of course, is the DHS Cybersecurity Talent Management System (CTMS), authorized by Congress in 2014 and envisioned as a forward-thinking model that would allow DHS to be more flexible in hiring and managing its cyber workforce. The program was not officially launched, though, until 2021, and as of the date of your June 2024 hearing on the cyber workforce, only 189 hires had been made at DHS under this new authority – a tiny fraction of the DHS cyber workforce.

While reports such as the Office of the National Cyber Director's National Cyber Workforce and Education Strategy have put out broad visions for cyber talent,[13] we still need a comprehensive review of existing efforts to give Congress the information it needs to assess the effectiveness and implementation of these different tools, assess why some authorities (such as the DHS CTMS) have been challenging to implement, and determine what adjustments might be warranted. We need a concerted effort to not only assess the effectiveness of different programs and authorities but also to know whether special flexibilities for some agencies put other agencies at a disadvantage in recruiting cyber talent. And undoubtedly there are many success stories that could be replicated throughout the government and with other levels of government and the private sector.

For the federal sector as a whole, this effort needs to be undergirded by careful, regularly updated human resource planning to know specifically which cyber skills and positions agencies and their subcomponents need. Also, as agencies also look to scale the effective use of AI and other emerging technologies, Congress and the White House need to make sure these efforts are aligned with cybersecurity efforts.

---

[12] Available at https://ourpublicservice.org/performance-measures/best-places-to-work-in-the-federal-government/

[13] For a summary of the National Cyber Workforce and Education Strategy, see Center for Security and Emerging Technologies, "Highlights from the National Cyber Workforce and Education Strategy" (Aug. 10, 2023).

Continue to promote innovative talent pipelines: The commitment of this committee to addressing the government's cyber workforce needs, as exhibited by this hearing today, has a profound impact on driving priorities within agencies. Further actions the committee can take include:

- Focus on getting young people into government. Members of Congress routinely use their intern programs as a pipeline for hiring, and federal agencies should do the same. In addition to leveraging and coordinating existing cyber-specific programs, Congress on a governmentwide basis could make it easier for agencies to hire young people, including by increasing the cap on direct hire authority for students and recent graduates. Congress should also authorize so-called conversion authority for agencies to hire interns or fellows sponsored by third parties, so that the government can move quickly to hire high-performing interns or fellows and not lose them to other job offerors.
- Promote ROTC-like opportunities to encourage young people to enter public service – an idea shared by Chairman Green in his bill in the last Congress, the Cyber PIVOTT Act.[14] The Partnership has long endorsed a ROTC-like model as a pipeline for the whole federal civil service.
- Use your oversight capacity to ensure effective implementation of the bipartisan Chance to Compete Act,[15] passed into law late last year to ensure agencies are identifying the skills they need, using technical assessments to identify highly qualified applicants, and removing barriers such as degree requirements to open the door to technologists with alternate qualifications, backgrounds and experiences.
- Promote public-private talent exchanges. Providing formal opportunities for individuals from the private sector to temporarily work in the public sector, and vice versa, is an effective way to cross-fertilize knowledge across the sectors and increase each sector's understanding of the other. Congress should extend government-wide the talent exchange authority already authorized for the Department of Defense.[16]

These types of strategies will better equip federal agencies to find and hire cyber talent across the country. This is important because over 80 percent of the entire federal workforce is outside the D.C. area. Moreover, used smartly and with proper oversight, telework and remote work are strategic business tools used by both the public and private sectors to enhance an organization's ability to recruit and retain top talent, increase productivity and reduce the real estate footprint. Just over 64 percent of the federal cyber workforce is outside of D.C., Maryland and Virginia.[17] We need to ensure that our policies recognize this is a nationwide effort.

Elevate the human resource functions of agencies: There are outstanding and innovative HR professionals across the government, but there are also skills gaps in their offices. They are often overwhelmed by responsibilities and the complexities of federal human capital law. Often, HR specialists are not familiar with the authorities they have available to them, and do not have the

[14] H.R. 9770, 118th Congress.
[15] Pub. L. 118-188 (Dec. 23, 2024).
[16] Section 1104 of the National Defense Authorization Act for Fiscal Year 2017, Pub. L. 114-328 (Dec. 23, 2016).
[17] Analysis of FedScope data as of March 2024.

technologies, data and analytical skills that would better enable them to recruit and hire while also engage in strategic workforce planning for the future. Ways Congress could strengthen the HR function include ensuring that agencies undertake strategic workforce planning and that Chief Human Capital Officers have a voice in the strategic and budget planning processes so that agency leaders will be informed of the HR needs necessary to carry out their policies and programs.

Congress also should jump-start efforts to increase the skills and professionalism of the federal HR community by requiring OPM to re-start technical training for HR specialists, conduct a review of overall training needs and how those needs can be met, and fund IT needs of the HR community.

Conclusion

Federal agencies face frenetically growing needs to protect our nation's cybersecurity as threats from external actors escalate. To do so, we need the talent, skills and capacity to meet these needs. This calls for a governmentwide strategic human capital planning effort coordinated between Congress and the White House to ensure agencies have necessary authorities and resources.

As we enter a period where arbitrary moves to reduce the size of the federal workforce are occurring, there is an increased risk that we lose the exact cyber talent we need. I commend the committee for its continued focus on this critical issue and look forward to working with you on reforms to hiring, performance management, leadership development, and other improvements that will make our federal workforce systems modernized to meet the needs of the future.