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)