

# Maryland's Cybersecurity Talent Strategy



# Table of Contents

<b>Executive Summary</b> .....	<b>2</b>
<b>Goals</b> .....	<b>5</b>
<b>Letter from Cyber Maryland Program</b> .....	<b>7</b>
<b>Letter from Governor’s Workforce Development Board</b> .....	<b>8</b>
<b>Maryland’s Cybersecurity Workforce – Supply, Demand, and Challenges</b> .....	<b>9</b>
<b>Existing State Investments in Cybersecurity</b> .....	<b>11</b>
<b>Maryland Experiences a Persistent Cybersecurity Workforce Gap</b> .....	<b>12</b>
<b>Employer Categories and Pathways to Access Cybersecurity Talent</b> .....	<b>15</b>
<b>Summary of Pain Points by Employment Pathway</b> .....	<b>16</b>
<b>GOAL 1: Equip Every Marylander with Foundational Skills to Grow the Pipeline of Potential Cyber Talent</b> .....	<b>17</b>
STRATEGY 1.1 Building Foundational Digital Skills and Cyber Literacy for Marylanders of All Ages .....	<b>17</b>
STRATEGY 1.2: Providing Career Coaching to Learners Interested in Cyber Fields .....	<b>19</b>
<b>GOAL 2: Transform Postsecondary Cybersecurity Education to Align with Industry Needs</b> .....	<b>21</b>
STRATEGY 2.1: Realign Curricula to Support Cybersecurity Skill Development .....	<b>22</b>
STRATEGY 2.2: Integrate Experiential Learning into Postsecondary Degree Pathways in Cybersecurity .....	<b>24</b>
STRATEGY 2.3: Increase Access to Postsecondary Degree Pathways in Cybersecurity .....	<b>26</b>
<b>GOAL 3: Expand Pathways into Cybersecurity Beyond Traditional Higher Education</b> .....	<b>28</b>
STRATEGY 3.1: Expand Registered Apprenticeships and Work-Based Learning in Cybersecurity .....	<b>28</b>
STRATEGY 3.2: Support Employer Adoption of Skills-First Hiring and Advancement Practices .....	<b>30</b>
STRATEGY 3.3: Boost to Cyber Talent Supply and Diversity Through Targeted Programs and Supports .....	<b>31</b>
<b>GOAL 4: Strengthen the Federal, State, and Local Government Cyber Workforce</b> .....	<b>34</b>
STRATEGY 4.1: Develop and Expand Federal Partnerships .....	<b>35</b>
STRATEGY 4.2: Develop New State & Local Government Cyber Talent Initiatives .....	<b>37</b>
<b>Cyber Maryland Board Members</b> .....	<b>39</b>
<b>Governor’s Workforce Development Board Members</b> .....	<b>40</b>
<b>Acknowledgments</b> .....	<b>Back Cover</b>

## Executive Summary

**Cybersecurity is fundamental to modern life, ensuring the security of critical infrastructure, data, and personal information across our society and economy.** With proximity to federal cybersecurity agencies, world-class academic institutions, and a vibrant private-sector tech ecosystem, Maryland has unmatched assets that position it to lead the nation in cybersecurity workforce development. However, Maryland also had tens of thousands of cyber jobs opening each year and, according to estimates performed by Lightcast, roughly 6,500 of those jobs were going unfilled as of the start of 2024.<sup>1</sup> The need is only expected to grow across our region – in Maryland alone, cybersecurity jobs are expected to grow by almost 40% over the next 10 years. Maryland must act decisively to grow and diversify its cybersecurity talent pipeline.<sup>2</sup>

Maryland’s vision is to build a sustainable, inclusive talent pipeline that meets industry needs of today while driving continued growth and innovation across the state. The **Cyber Maryland Program and Board** were established by statute under **TEDCO** in 2023 to accomplish this vision by developing and implementing a bold strategic action plan for cybersecurity workforce development.<sup>3</sup> Specifically, the Cyber Maryland Program, with the guidance and support of the Cyber Maryland Board, was established to:

1. **Create and execute a talent pipeline that materially reduces workforce vacancies by July 1, 2026;**
2. **Serve as a one-stop shop for employers seeking to leverage cyber workforce development programs offered by the state and its partners;**
3. **Inform cybersecurity training and education programs operated by public or private entities with industry-driven needs; and**
4. **Build the most advanced local and state information technology workforce in the nation, which, to the maximum extent possible, reflects the racial, gender, ethnic and geographic diversity of the state.**

---

1 <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>

2 <https://labor.maryland.gov/lmi/iandoproj/wias.shtml>

3 <https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0801/?ys=2023rs>

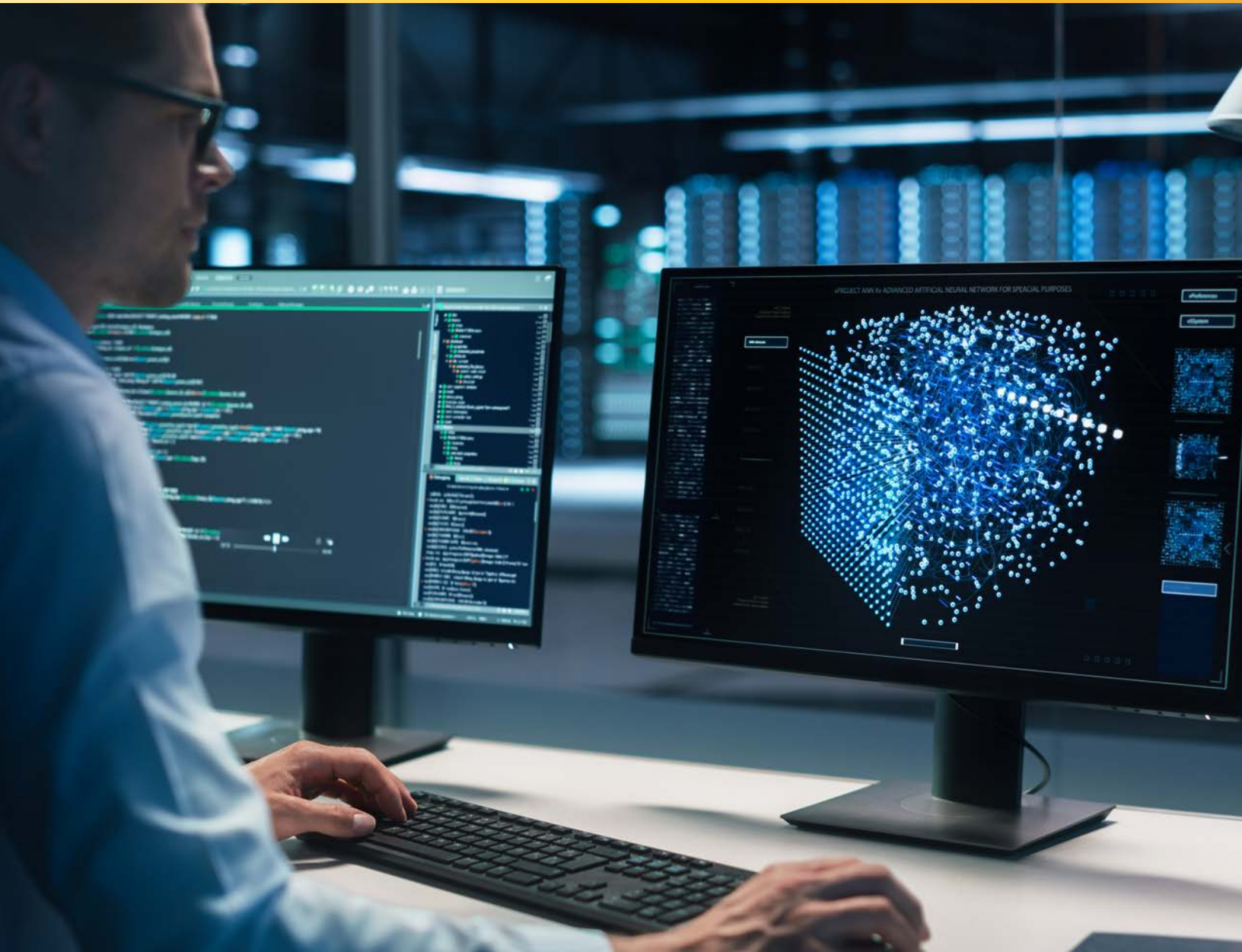
In early 2024, to better understand the state's robust, but fragmented ecosystem, the Cyber Maryland Program under the guidance of the Cyber Maryland Board commissioned and released '*Cybersecurity Workforce Analysis and Strategy*' which provided an analysis of the current state of Maryland's cybersecurity workforce ecosystem. Building off the findings of the report, later that year, the Cyber Maryland Board partnered with the **Governor's Workforce Development Board** to engage over 65 industry leaders, educators, as well as other state and local stakeholders across Maryland in developing the comprehensive strategic action plan that follows.

This plan is anchored in four goals that build on the state's strengths, address workforce gaps for employers, and expand economic opportunities for Marylanders:

- 1. Equip every Marylander with foundational skills to grow the pipeline of potential cyber talent:** Ensure Marylanders of all demographics are able to develop foundational digital skills and cybersecurity literacy skills that enable them to participate in public life and equip them to enter into cybersecurity education or training programs.
- 2. Transform postsecondary cybersecurity education to align with industry needs:** Ensure curricula and experiential learning opportunities are developed in alignment with industry needs, and expand access and affordability of degree pathways into cybersecurity careers.
- 3. Expand new pathways into cybersecurity careers beyond traditional higher education:** Develop and scale new, less "traditional" pathways into cybersecurity careers, creating opportunity for a more diverse talent pool by leveraging tools and models beyond the traditional postsecondary education system.
- 4. Strengthen the federal, state, and local government cybersecurity workforce:** Strengthen partnerships with government agencies to cultivate talent pipelines for the public sector, and help individuals leverage public sector experience into career advancement opportunities across sectors.

Meeting these goals will require industry leaders, state agencies, and local partners to take shared ownership of the goals in this plan, coordinating actions and accelerating implementation by leveraging partner strengths and assets. The Cyber Maryland Program, with the support of the Cyber Maryland Board, must provide the important connective tissue that drives synergy between industry, federal, local, academic and philanthropic partners towards a shared vision of the future of the cybersecurity workforce development ecosystem in Maryland.

Given Maryland's standing as the national epicenter for cybersecurity, the global significance of developing Maryland's cybersecurity workforce pipeline cannot be overstated. Developing a robust workforce pipeline that meets the demands of Maryland's cybersecurity ecosystem will require extensive resources and staff capacity. The execution of this strategic action plan can be achieved most efficiently and effectively through strong mission alignment. The Cyber Maryland Board therefore proposes that, during the 2025 session of the Maryland General Assembly, the Cyber Maryland Program be re-established in statute under the Maryland Department of Labor, where it will have strategic alignment with the mission of the department.



In 2025 and beyond, the Cyber Maryland Program will continue its work to develop, promote, support, and invest in cybersecurity talent pipelines throughout the state. Guided by the recommendations outlined in this talent strategy the program will support coordination and collaboration throughout the ecosystem, facilitating alignment between industry, federal, local, academic and philanthropic partners to advance the development of the state's cybersecurity talent, promoting the state's economic growth, and ensuring the safety of our nation's digital infrastructure.

## GOAL 1: Equip Every Marylander with Foundational Skills to Grow the Pipeline of Potential Cyber Talent

<b>1.1: Build Foundational Digital Skills and Cyber Literacy for Marylanders of All Ages</b>	<b>1.1.1:</b> Leverage opportunities to invest in foundational digital skills that can prepare learners of all ages for pathways in cybersecurity
	<b>1.1.2:</b> Introduce K-12 cyber literacy integration, starting in elementary school
<b>1.2: Provide Career Coaching to Learners Interested in Cyber Fields</b>	<b>1.2.1:</b> Coordinate career coaching for middle and high school students on cybersecurity career pathways and associated credentials as part of <i>Blueprint</i> implementation
	<b>1.2.2:</b> Build industry-specific career coaching into all cyber training and education programs

## GOAL 2: Transform Postsecondary Cybersecurity Education to Align with Industry Needs

<b>2.1: Realign Curricula to Support Cybersecurity Skill Development</b>	<b>2.1.1:</b> Integrate cybersecurity skills and curriculum requirements into related degree programs
	<b>2.1.2:</b> Improve conditions for community college cyber graduates to seamlessly transition to four-year colleges and universities
<b>2.2: Integrate Experiential Learning into Postsecondary Degree Pathways in Cybersecurity</b>	<b>2.2.1:</b> Scale and build upon cyber ranges across Maryland
	<b>2.2.2:</b> Establish industry-specific cyber clinics at Maryland's community colleges and universities
	<b>2.2.3:</b> Integrate certificates, internships, and work rotations into degree pathways
<b>2.3: Increase Access to Postsecondary Degree Pathways in Cybersecurity</b>	<b>2.3.1:</b> Realign Maryland's scholarships and other investments to employer demand

## GOAL 3: Expand Pathways into Cybersecurity Beyond Traditional Higher Education

<b>3.1: Expand Registered Apprenticeships and Work-Based Learning in Cybersecurity</b>	<b>3.1.1:</b> Expand career and technical education through registered apprenticeship and other work-based learning opportunities in K-12
	<b>3.1.2:</b> Provide support and incentives for cyber employer exploration of registered apprenticeship
	<b>3.1.3:</b> Tailor registered apprenticeship requirements and branding for cyber careers
<b>3.2: Support Employer Adoption of Skills-First Hiring and Advancement Practices</b>	<b>3.2.1:</b> Develop tools and resources to collaborate with employers' human resources teams on real-world skill, competency, and credential needs to better fill cyber roles
<b>3.3: Boost Cyber Talent Supply and Diversity Through Targeted Programs and Supports</b>	<b>3.3.1:</b> Expand access to short-term non-degree training and credentialing programs
	<b>3.3.2:</b> Leverage existing and/or develop new incentives for incumbent worker training
	<b>3.3.3:</b> Increase engagement of transitioning veterans within Maryland who have cyber skills, adjacent skills, and/or relevant clearances acquired during their service
	<b>3.4.4:</b> Build on programs that cultivate racial and gender diversity in the cyber workforce

## GOAL 4: Strengthen the Federal, State and Local Government Cybersecurity Workforce

<b>4.1: Develop and Expand Federal Partnerships</b>	<b>4.1.1:</b> Work with NSA, US Cyber Command and other cyber-focused federal agencies to promote internships, registered apprenticeships, and other early job pathways that incorporate clearance processes where feasible
	<b>4.1.2:</b> Explore partnership with State/ NSA and US Cyber Command on a multi-purpose cyber workforce center
	<b>4.1.3:</b> Support partnerships between Maryland universities and federal agencies for cybersecurity research and development
	<b>4.1.4:</b> More effectively market existing federal scholarship programs
<b>4.2: Develop New State &amp; Local Government Cyber Talent Initiatives</b>	<b>4.2.1:</b> Coordinate State agency action to fill cybersecurity roles
	<b>4.2.2:</b> Explore a service-based learning program for cybersecurity training



Dear Cybersecurity Partners and Stakeholders,

Maryland stands at a critical crossroads. As cyber threats grow increasingly sophisticated and relentless, our position as a national cybersecurity leader demands that we respond with urgency and purpose. These threats jeopardize not only our critical infrastructure and economy but also the safety and prosperity of all Marylanders. Yet, within this challenge lies an opportunity: to build a more resilient economy.

The Cyber Maryland Program is uniquely positioned to lead this charge, backed by strong public and private support. Our strategy is centered on four transformative goals:

- **Expand cyber literacy and skills** across all age groups—integrating cybersecurity education statewide.
- **Create diverse pathways to cyber careers** through apprenticeships, credentialing, and skills-based hiring.
- **Strengthen partnerships** with federal, state, and local entities—leveraging Maryland's position as home to the NSA, U.S. Cyber Command, and NIST.
- **Foster inclusive growth**, ensuring underserved communities, veterans, and their families can access high-demand cyber roles.

As we work towards these goals, it is essential that we remain vigilant about the promise and risks of emerging technologies like AI and quantum technologies. Maryland must lead in crafting adaptive cybersecurity frameworks that maximize the potential of these advancements while mitigating their risks.

Achieving our vision requires all of us—educators, employers, policymakers, and professionals—to collaborate. Whether mentoring, updating curricula, or embracing hiring practices that prioritize skills over traditional credentials, your role is essential.

I extend my deepest gratitude to Governor Wes Moore, my fellow Cyber Maryland board members, TEDCO, the Governor's Workforce Development Board, and our federal, state, and private sector partners. Your contributions are the foundation of our ability to protect and innovate.

Strategies and goals are only as impactful as the actions they inspire. The Cyber Maryland Program remains steadfast in its accountability and commitment to delivering results. The time to act is now. Let's work together to protect Maryland's future—and set a national standard.

Thank you for your partnership and commitment to this vital effort.

Sincerely,

A handwritten signature in black ink that reads 'Roger Austin' in a cursive script.

Roger Austin  
Chair  
Cyber Maryland Board





Dear Partners and Stakeholders,

On behalf of the Governor's Workforce Development Board (GWDB), I am pleased to share our support for Maryland's Cybersecurity Talent Strategy and the critical work it represents. The GWDB has been proud to partner with TEDCO and the CyberMaryland Board on this important initiative, which aligns closely with our mission to develop a thriving, competitive workforce across Maryland.

Maryland's Cybersecurity Talent Strategy provides a valuable framework for addressing Maryland's evolving cybersecurity workforce needs. By encouraging collaboration among public and private partners, the plan focuses on initiatives to support the development of a skilled and adaptable cyber workforce. Through thoughtful investments and employer-driven strategies, this effort seeks to address the dynamic needs of the industry while laying a pathway for continued growth and resilience in this critical sector.

This alignment with the GWDB's ongoing priorities strengthens our shared goal of making Maryland a national leader in cybersecurity talent development. As we continue to support businesses in identifying workforce needs and bridging skill gaps, we look forward to seeing Maryland's Cybersecurity Talent Strategy enhance opportunities for individuals and businesses alike.

Thank you to everyone who has contributed to this effort. Together, we are ensuring Maryland remains at the forefront of workforce development and cybersecurity excellence.

A handwritten signature in black ink, appearing to read "Carim Khouzami".

Carim Khouzami  
*President & CEO*  
Baltimore Gas & Electric  
*Chair, Governor's Workforce Development Board*



## Maryland's Cybersecurity Workforce – Supply, Demand, and Challenges

### INTRODUCTION

Maryland has long been a leading hub in America's cybersecurity industry. The cybersecurity industry includes all capabilities critical to protecting systems, networks, and data from cyber threats, such as hacking from malevolent actors, data breaches, and malware. As cyber threats continue to evolve, cybersecurity—and an appropriately skilled workforce that can deliver on this security – is increasingly critical to ensuring the confidentiality, integrity, and availability of digital assets and information while ensuring continuity of operations.

Maryland is a leading state for cybersecurity talent; nationally, Maryland has the second highest concentration of cybersecurity jobs, with the District of Columbia, Maryland, and Virginia region (DMV) holding all the top spots across a number of talent statistics.<sup>4</sup>

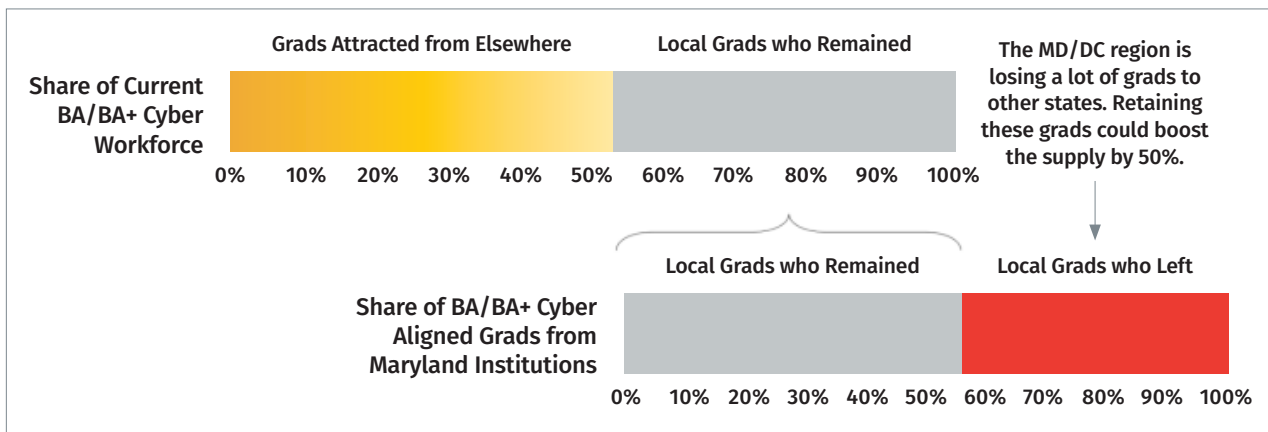
<sup>4</sup> As measured by "Information Security Analyst" employment; <https://www.bls.gov/oes/current/oes151212.htm#nat>

**TABLE 1: Employment of Information Security Analysts per thousand jobs within the state.** SOURCE: BLS

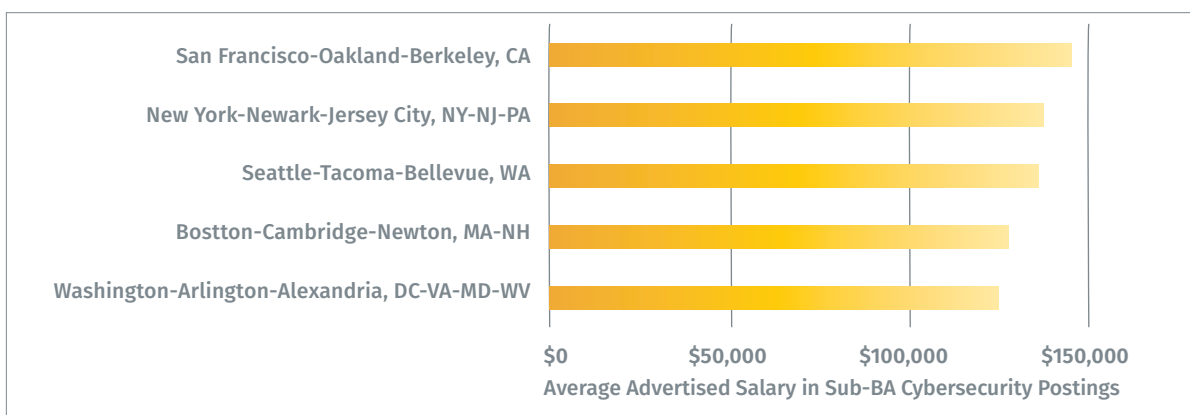
State	Employment per thousand jobs
Virginia	4.64
Maryland	2.95
District of Columbia	2.28
New Mexico	1.98
Colorado	1.94

Maryland both attracts and sheds highly educated cyber talent. Over 50 percent of Maryland's current cybersecurity workforce earned their bachelor's or advanced degree out of state before moving to Maryland. This helps to offset the fact that Maryland is only retaining around 55 percent of its cyber-aligned graduates from Maryland institutions, who sometimes pursue more lucrative job opportunities or lower costs of living in other geographies.

**FIGURE 1: In-flows and out-flows of cybersecurity talent in Maryland and Washington, D.C.** SOURCE: LIGHTCAST



**FIGURE 2: Avg. advertised salary in cybersecurity job posting at the Bachelor's and above level, '21-'23.** SOURCE: LIGHTCAST



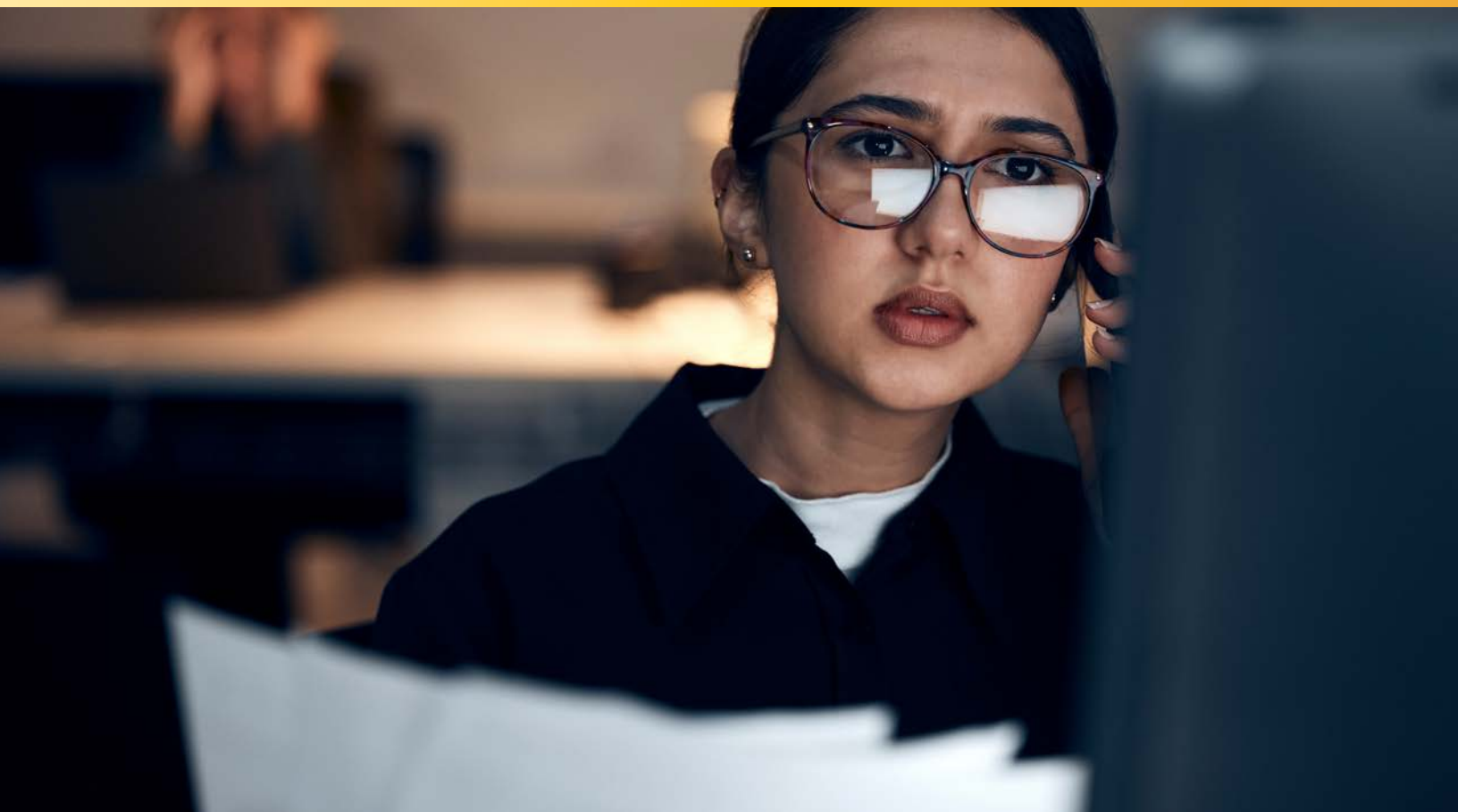
## Existing State Investments in Cybersecurity

To support its growing cybersecurity industry, Maryland has continued to make significant investments in programs to develop the state's workforce. The table provided below provides a snapshot of state investments between FY 2024 and FY 2025.

	Program	Fiscal 2024	Fiscal 2025
MDL	MDL (Employment Advancement Right Now)	\$3,833,086	\$3,833,086
Commerce	Cybersecurity Investment Tax Credit	\$2,000,000	\$2,000,000
Commerce	Buy Maryland Cybersecurity Tax Credit	\$4,000,000	\$4,000,000
TEDCO	CyberSecurity Investment Fund (TEDCO)	\$900,000	\$900,00
MSDE	P-TECH	\$2,272,295	\$2,062,133
MHEC – Student Financial Assistance	Cyber Public Service Scholarship	\$1,000,000	\$1,000,000
MHEC	Cyber Warrior Diversity Program	\$2,500,000	\$2,500,000
UMBC	MTIP	\$356,372	\$1,056,372
UMBC	UMBC Institute for Innovative Computing	\$500,000	\$500,000
UMBC	MD Cyber Range	\$1,200,000	\$1,200,000
UMBC	UMBC Center for Cybersecurity	\$3,000,000	\$3,000,000
Commerce	Build Our Future Grant Pilot Program	\$9,000,000	\$9,000,000
MDL	Registered Apprenticeships in Cybersecurity		
MDL	Accelerating Cyber Careers – (through Talent Innovation Fund)		\$2,000,000

Investments through Workforce Development Initiative			
University	Program	Fiscal 2019 and 2020	
UMBC	Establish Computer Science/Cyber/Data Science at USG	\$1,311,973	funding for these initiatives was incorporated into base funding for the institutions after fiscal 2019 and 2020
UMCP	Cybersecurity Enhancements at iSchool	\$1,270,000	
SU	Expand Information & Decision Science Program	\$365,000	
UMCP	Increase Capacity in Computer Science Programs	\$1,560,000	
BSU	Cybersecurity Certificate Development	\$225,000	
TU	Computer Science and Cybersecurity Program Development	\$281,163	
Ubal	Cybersecurerity Management Program Development	\$260,000	
UMCP	Cybersecurity Enhancements at iSchool at USG	\$340,000	
Ubal	M.S. in Cyber Forensics Development	\$332,000	
SU	Computer Science Enrollment & Retention Efforts	\$292,000	

While these investments have had a meaningful impact on the growing Maryland cybersecurity sector, including the development of a workforce to support the sector, the supply of cyber talent in the region consistently falls short of demand.



## Maryland Experiences a Persistent Cybersecurity Workforce Gap

Despite Maryland's visible strengths as a leader in the cybersecurity sector, nearly all employers of cybersecurity professionals indicate that it is challenging to find the talent that they need.

***“The reality is, we are extremely short on cyber professionals now. Our company could hire 100 people tomorrow, based on our needs.”***

***– Manager of Strategic Initiatives at a large government contractor***

Maryland is home to many leading cybersecurity employers, including major federal agencies, state and local government entities, government contractors, and non-contractor private companies. They choose to locate in Maryland to leverage the unique strengths of Maryland's cybersecurity ecosystem: collectively, they generate more demand than the current cybersecurity talent pool in Maryland supplies.

Lightcast estimates that, between December 2023 and January 2024, over 6,500 open public and private cybersecurity positions in Maryland and Washington, D.C. (and over 15,000 when including Virginia) were left unfilled because employers were unable to locate suitable talent. This combined cybersecurity talent gap is the largest in the country, preventing agencies and contractors from fully protecting national infrastructure and prevents private companies from fully protecting their own systems.

Cybersecurity talent needs will only grow greater over time, as technology systems grow in complexity and the sophistication of cyber threats increases. The Maryland Department of Labor estimates that over the next 10 years, cybersecurity employment in Maryland will increase by 37 percent.<sup>5</sup> This growth will occur across the state, and for many occupations—such as information security analysts—will be greatest within Frederick, Prince George's, and Montgomery Counties.

## TABLE 2: Forecasted growth in employment of Information Security Analysts, 2022 to 2032.

SOURCE: LOCAL WORKFORCE DEVELOPMENT AREA OCCUPATIONAL PROJECTIONS 2022-2032<sup>6</sup>

Region	Forecasted growth in employment
Frederick	41%
Prince Georges	41%
Montgomery	39%
Howard	38%
Susquehanna	38%
Carroll	38%
Anne Arundel	37%
Southern MD	36%
Baltimore	34%
Baltimore City	34%
Western Maryland	20%

Maryland must create new and expanded pathways for the state talent to pursue careers in cybersecurity, along with a more robust ecosystem for cyber talent and cyber tech entrepreneurship and investment. Failing to do so will prevent Maryland companies from growing their businesses and protecting their data and technology systems. Maryland additionally risks losing its position as a leader in the cybersecurity sector, ceding opportunities to Virginia or other states that have made significant investments in cybertalent, such as Florida, Georgia or Texas. Cyber Florida received a \$16M annual budget and a one-time \$20M grant for cyber education and workforce development; Cyber Georgia was funded at \$100M, with \$60M granted in capital expenditures and \$40M in operational expenses.<sup>7</sup>

<sup>5</sup> <https://labor.maryland.gov/lmi/iandoproj/wias.shtml>

<sup>6</sup> Projections data for information security analysts is not available for the Upper Shore and Lower Shore Workforce Development Areas, so those two areas are not included in Table 2.

<sup>7</sup> [Cyber Maryland Presentation](#)



***“Our ecosystem today is much more robust than other places, but the states of Georgia and Texas are investing significant amounts of funding to catch up. Large centers of cybersecurity activity – such as the Sixteenth Air Force (Air Forces Cyber) in San Antonio – will continue to attract growth.”***

***– CEO of a leading Maryland nonprofit focused on the cybersecurity workforce***

However, if Maryland can rise to meet this persistent challenge, the state will unlock the potential of its cybersecurity-focused employers and ensure that all enterprises—public and private—remain protected from cyber threats. In addition, Maryland can support entrepreneurship and the development of new cyber capabilities and products, leading to thousands of new, quality jobs. Finally, Maryland can continue to protect its leadership position at the forefront of our national security, protecting our nation from foreign cyber threats.

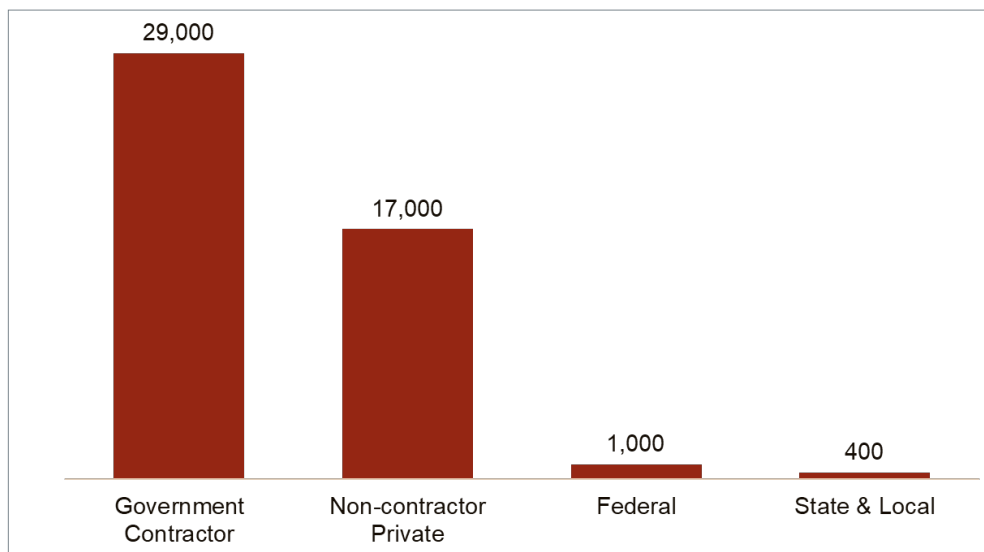
## Employer Categories and Pathways to Access Cybersecurity Talent

This report examined four specific groups of employers to understand their challenges recruiting and retaining talent:

- **Non-contractor private employers of cybersecurity talent**, including companies developing cybersecurity products, such as Minerva Cyber Technologies, and companies hiring cybersecurity talent to protect their own systems, such as T Rowe Price.
- **Government contractors**, such as Northrop Grumman, Accenture, and AT&T, provide essential cybersecurity and technology services to government agencies and must also protect their own networks.
- **Federal agencies**, including the National Security Agency (NSA), U.S. Cyber Command, the Defense Information Systems Agency (DISA) and many others.
- **State and local government employers**, including the State of Maryland, city and county governments for Maryland and D.C. communities, and public school systems.

During 2023, these employer types collectively accounted for over 47,000 unique cybersecurity job postings in Maryland and Washington, D.C..<sup>8</sup> Contractors and non-contractor private employers accounted for the jobs postings. It is important to note, however, that because some recruiting does not occur through public job postings (such as on-campus recruiting of students, and direct hiring of military talent), it is likely that these statistics undercount true cybersecurity job demand.

**FIGURE 3: Public job postings for cybersecurity positions, 2023. SOURCE: LIGHTCAST<sup>8</sup>**



Summary of

### Pain Points by Employment Pathway

Conversations with employers, including government contractors, federal agencies, and private

























<sup>8</sup> TEDCO & Lightcast, Cyber Maryland: Cybersecurity workforce strategy (p. 7). Lightcast Occupational Taxonomy defines three categories of roles: Cybersecurity-Forward Roles (central to the creation, analysis, and management of cybersecurity technologies), Downstream Cybersecurity Implementers (other IT roles that use the tools or strategies developed by cyber-forward occupations), and Diffuse Cybersecurity Roles (include all other, non-IT roles that employ cybersecurity skills or tools in the performance of their responsibilities)



companies, illuminated varying challenges in sourcing cybersecurity talent. These challenges often stem from barriers experienced by the talent themselves, such as differing degree requirements that make it harder for workers to secure employment.

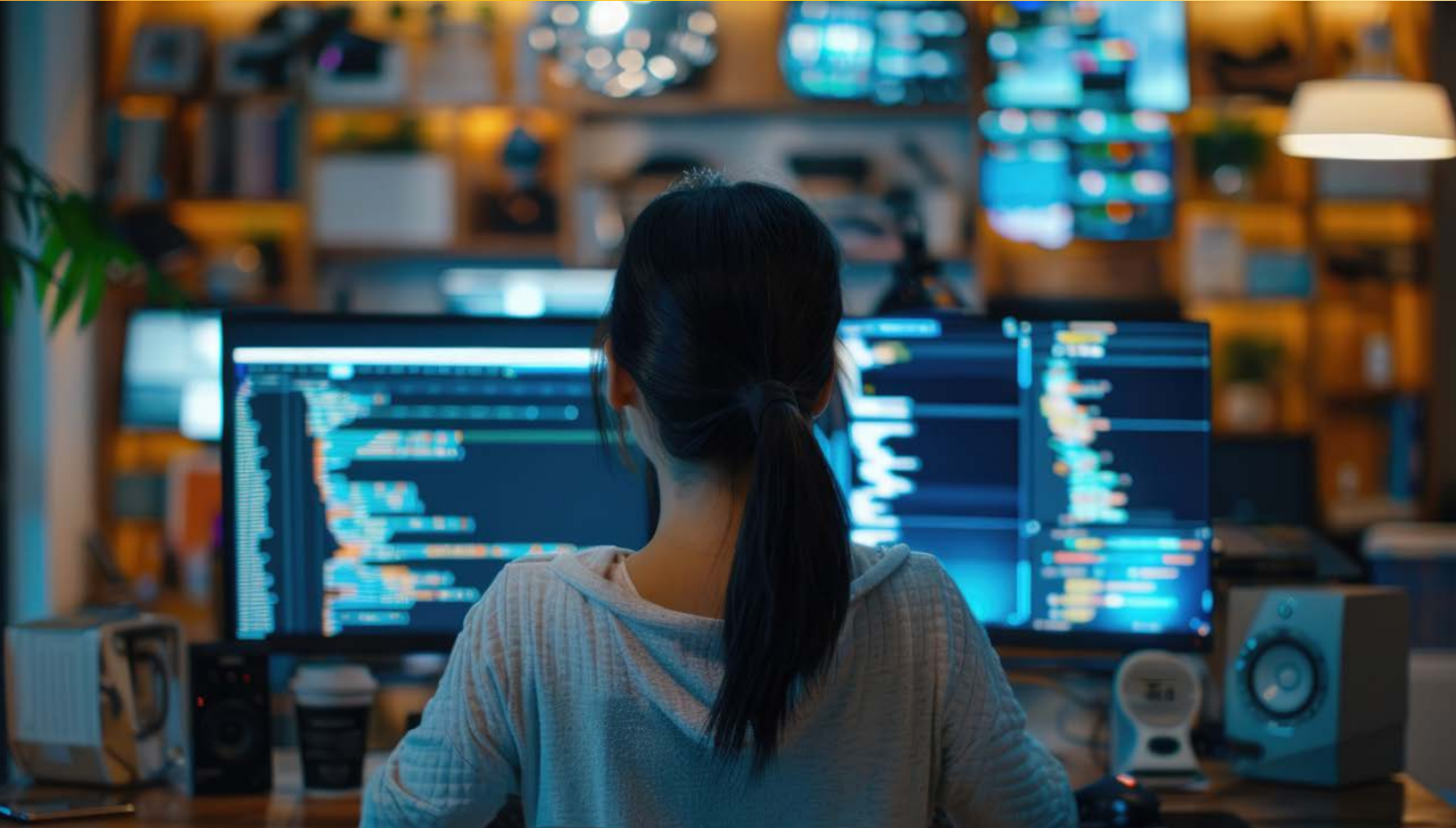
The table below summarizes pain points experienced by each employment pathway:

- Green:** Minimal barrier – easy to overcome for any given employer
- Yellow:** Moderate barrier – required dedicated employer focus to overcome
- Red:** Very significant barrier – significantly hard for any one employer to “move the needle,” required systemic change to differentially improve hiring conditions

	Private Employers		Government Contractors		Federal Agencies	
	Entry-Level	Mid-Career	Entry-Level	Mid-Career	Entry-Level	Mid-Career
<b>Security Clearances</b>						
<b>Degree requirements</b>						
<b>Demonstrated experience (incl. via work-based learning such as apprenticeships, internships)</b>						
<b>Certification requirements</b>						

To directly address these pain points while building stronger and more accessible talent pipelines in cybersecurity, the Cyber Maryland Board and Governor’s Workforce Development Board identified the following four goals around which to center Maryland’s cyber talent strategy:

1. Equip every Marylander with foundational skills to grow the pipeline of potential cyber talent
2. Transform postsecondary cybersecurity education to align with industry needs
3. Expand pathways into cybersecurity careers beyond traditional higher education.
4. Strengthen the federal, state and local government cybersecurity workforce:



## **GOAL 1: Equip Every Marylander with Foundational Skills to Grow the Pipeline of Potential Cyber Talent**

Expanding Maryland's cybersecurity talent pipeline begins with equipping more residents with foundational information technology and cybersecurity skills. Additionally, because information networks are essential to every type of business and sector of the economy, individuals who may not specialize in cybersecurity but use the internet, access networks, or work with data or operational technology must understand and exercise basic cyber hygiene practices.

### **STRATEGY 1.1: Building Foundational Digital Skills and Cyber Literacy for Marylanders of All Ages**

Maryland cannot build a consistent, reliable cyber talent pipeline without ensuring all Marylanders develop the foundational digital skills and cyber literacy needed not only to thrive in the modern age, but to have the option of entering a cyber career. By investing in foundational skills, Maryland will capitalize on available opportunities to embed digital skills across communities, incorporating these essential competencies in programs that reach K-12 students, adult learners, and job seekers.

The state should leverage existing funding sources across agencies (e.g., the Maryland Department of Labor and the Maryland State Department of Education) to support broad

access to digital skills and cyber literacy training. By aligning resources and efforts, the state can ensure that Marylanders of all ages have the skills necessary to pursue cybersecurity pathways.

### **To accomplish this, Maryland should:**

#### **1.1.1: Invest in foundational digital skills that can prepare learners of all ages for pathways in cybersecurity**

---

Building foundational digital skills will require meeting learners where they are and leveraging existing outreach and connections with technology. Existing programming and investments can be used to support expanded digital literacy which should incorporate cybersecurity awareness and foundational concepts. For example, the Department of Housing and Community Development (DHCD) and the Maryland Department of Labor should support leveraging of BEAD (Broadband, Equity, Access, and Deployment Act) investments, as outlined in the Maryland Digital Equity Plan. That plan seeks to address critical gaps in digital access and literacy by prioritizing connectivity for underserved areas, and coordinating digital equity and inclusion activities.

Beginning in FY 2026, the Governor's Workforce Development Board (GWDB) and Cyber Maryland Board will replace with the Maryland Department of Labor to assess and evaluate digital skills-offerings to adults through existing training programs (including those offered by local workforce development boards (LWDBs), adult education providers, correctional education facilities, and more). After the assessment, the GWDB, Cyber Maryland Board, and Maryland Department of Labor can determine how to best align existing offerings to support cyber career pathways.

#### **1.1.2: Introduce K-12 cyber literacy integration, starting in elementary school**

---

Strategic investments in early education are key. By introducing cyber skills starting in elementary school and embedding cyber literacy across K-12, Maryland can lay a strong foundation, exposing students to critical cybersecurity concepts and career opportunities. Many industry and education leaders agree that Maryland could strengthen efforts to inspire young people to consider a career in cybersecurity. Early exposure is crucial, not only to demystify the cybersecurity industry, but also to create pathways for students who might otherwise overlook this essential field. This exposure should include a multidisciplinary approach to cybersecurity, with a focus not only on technical skills, but also law and policy (e.g., privacy concerns), and applications of psychology, economics, and other social sciences and their implications on cybersecurity risks. Currently, computer science is not part of the required K-8 curriculum – investments in introducing K-12 cyber literacy should include requiring computer science in earlier grades.

Maryland must build on existing resources, such as its computer science standards<sup>9</sup>, and foundational investments being made by the Maryland State Department of Education and the Maryland Center for Computing Education (MCCE) in developing four new pathways into the computer science workforce and draft learning standards for computer literacy for PK-12 students. Maryland can also leverage resources provided by multiple national and regional training organizations, to increase youth interest in cybersecurity careers, creating pathways to prepare Maryland's future cybersecurity professionals.

### **ACTION HIGHLIGHTS:**

Beginning in FY 2026, Maryland State Department of Education and other state agency partners should assess and, as appropriate, embed cybersecurity content into STEM and Computer Science curricula across K-12. This integration should ensure that students can engage with cybersecurity concepts early on.

## **STRATEGY 1.2: Providing Career Coaching to Learners Interested in Cyber Fields**

As Maryland invests in foundational cyber skills and integrates cyber literacy into K-12 education, the state should foster early awareness of the cybersecurity industry, creating pathways that spark interest, build understanding, and lay the foundation for future careers in cybersecurity. A significant driver of these efforts is the *Blueprint for Maryland's Future* ("the Blueprint"), which mandates comprehensive career coaching for all public middle and high school students (grades 6-12).<sup>10</sup> This requirement emphasizes individualized guidance to help students align their educational pathways with career aspirations, ensuring they are prepared for high demand fields like cybersecurity.

Effective career coaching, informed by the *Blueprint*, will ensure that students understand the skills, credentials, and opportunities necessary to pursue cybersecurity careers. By embedding cybersecurity-focused career coaching into both educational and workforce programs, Maryland can provide learners with a roadmap to enter and succeed in this field.

**To support this goal, Maryland should:**

### **1.2.1: Coordinate career coaching for middle and high school students on cybersecurity career pathways and associated credentials as part of *Blueprint* implementation**

Beginning in FY 2025, in consultation with the Cyber Maryland Board, the Governor's Workforce Development Board (GWDB) should collaborate with the Maryland State Department of Education, the Maryland Department of Labor, and other state and local partners tasked with supporting the Career Coaching program being piloted under the

<sup>9</sup> <https://www.cs4md.com/annotations>

<sup>10</sup> Blueprint for Maryland's Future Accountability and Implementation Board, *Blueprint for Maryland's Future: Comprehensive Implementation Plan*, 2023, <https://drive.google.com/file/d/1PsYQGhld5Qwk7PgK2cEubr68SSKrG5dH/view>.

**Blueprint.** This partnership should focus on equipping **Blueprint** career coaches in middle and high schools, starting in fifth grade, with comprehensive training and resources on career pathways and associated credentials for in-demand occupations, including cybersecurity.<sup>11</sup> Cybersecurity is inherently a complex and nuanced industry: Maryland can enhance the effectiveness of its career coaches through partnerships with industry and philanthropy so students can learn about the specifics of the industry. Maryland can increase student participation in career and technical education programs, industry-recognized credential attainment, dual enrollment opportunities, and registered apprenticeships (RAs) in cybersecurity. These efforts would ensure students are positioned for long-term success.

### **1.2.2: Build industry-specific career coaching into all cyber training and education programs**

---

Beyond K-12, Maryland should ensure that industry-specific career coaching is integrated into all Cyber Maryland-funded cybersecurity training and education programs. This work builds on the foundations that the MCCE has laid. This must include key actions such as:

Beginning in FY 2026, the GWDB, in consultation with the Cyber Maryland Board, and partner agencies such as MCCE, should facilitate the development of a comprehensive resource library to be publicly accessible and available to educational institutions, local workforce boards, and other organizations. These tools would enhance career coaching services, equipping learners with the specialized support they need to navigate and succeed in cybersecurity careers. These tools may be a new development or build on the existing vision from the 2020 Maryland Statewide Computing Alignment to Locate your Education pathway (SCALE) project. The project called for (1) a comprehensive online computing education portal that will include self-assessments, aptitude assessments, virtual training, mentoring, apprenticeships, and internships; (2) connections to education pathways, certification pathways, and job opportunities; (3) support for collaboration between education and industry; and (4) integration into a Learner Credential Network (LCN).

Leveraging philanthropy, innovative national delivery models, and private sector engagement, supports widespread delivery of career services to aspiring cybersecurity professionals—such as resume development, technical interview preparation, skills, and other requirements depending on employer (such as security clearances) tailored to the unique demands of the cybersecurity industry.

---

<sup>11</sup> For instance, professional skills include communication, time management, teamwork, problem-solving, creativity and adaptability.



## **GOAL 2: Transform Postsecondary Cybersecurity Education to Align with Industry Needs**

Maryland's colleges and universities graduate more than 8,000 students annually with cybersecurity-related degrees, from associate to doctoral levels. Despite the demand for skilled professionals, many of these students struggle to transition into cybersecurity roles upon graduation, particularly those from community colleges. This is further complicated by the complex ecosystem of work role categories that fall under the "cybersecurity" umbrella – for example, the National Institute of Science and Technologies (NIST)'s Workforce Framework from Cybersecurity (NICE) outlines 52 work roles all under cybersecurity. Furthermore, employers articulate the driving barrier as workforce-readiness, which includes core cybersecurity skills, credentials, and hands-on experience. Higher education institutions express a willingness to adapt to industry needs, which underscores the opportunity for the State to help align this pathway for postgraduate employment.

Maryland is distinctly positioned to capitalize on the growth that the cybersecurity industry demands. Educating the volume of needed cybersecurity hires and delivering cutting-edge, practical training for all students is a once-in-a-generation challenge that Maryland's higher education institutions are already tackling, and the state will set conditions to meet the occasion. Ensuring that students at higher education institutions are able to move seamlessly into cybersecurity careers will require foundational shifts in academic program design and curriculum, as well as expansion of internships and other experiential learning opportunities. Such innovations will require strong engagement from employers and entrepreneurs, support and involvement from community and philanthropic organizations, and creative approaches from workforce and educational institutions. Taking these steps would strengthen the bridge between education and employment to maximize the impact of Maryland's higher education institutions on the cybersecurity talent pipeline.

## **STRATEGY 2.1: Realign Curricula to Support Cybersecurity Skill Development**

Maryland ranks seventh in sub-bachelor's completions and tenth in bachelor's degree completions in cybersecurity-aligned postsecondary programs<sup>12</sup>. However, gaps in coordination between education providers and employers have led to curricula that do not emphasize the critical skills and knowledge most needed in the field. Compounding this issue is the limited integration of cybersecurity training into related disciplines, which narrows students' exposure to diverse career paths and the interdisciplinary expertise employers increasingly expect. In addition, although students in four-year programs experience higher rates of postgraduate employment compared to students in two-year programs, both groups face challenges securing employment. Two-year program graduates often lack critical theory learnings while four-year program graduates cite a lack of skills upon completion of their degree, resulting in a fragmented pathway for all students seeking advanced qualifications<sup>13</sup>. These systemic challenges undermine students' ability to transition seamlessly into the cybersecurity workforce.

**To support this goal, Maryland should:**

### **2.1.1: Integrate cybersecurity skills and curriculum requirements into related degree programs**

One of the most critical structural changes that must be made to ensure that Maryland has the cybersecurity protections in place to safeguard its businesses, government, and the economy is to integrate cybersecurity into related degree programs. This is a national problem; as the White House and Cybersecurity and Infrastructure Security Agency (CISA) Secure by Design initiative launched in 2024 indicate, many higher education institutions have still failed to incorporate cybersecurity into their curricula. In a piece early in

<sup>12</sup> Lightcast Report - Pg. 40

<sup>13</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>; insights gathered during interviews of over 30 employers by GWDB, TEDCO and Fierce Outcomes staffs between June - August 2024

2024 noting that 23 of the top 24 universities in computer science still do not require cybersecurity, a senior advisor at CISA notes:

***“Cybersecurity is viewed as a subdiscipline, much like graphics or human-computer interaction – not essential knowledge that every future software developer should be equipped with as they enter the workforce. This is unacceptable....To foster long-term cybersecurity, we must ensure that software developers and business leaders can build in security from the onset.”<sup>14</sup>***

To implement a comprehensive cybersecurity approach, Maryland's higher education leaders must work together to assess opportunities to ensure every Computer Science or Information Technology degree program incorporates basic cybersecurity knowledge (e.g., penetration testing, security operations centers (SOC), and other key skills on the outside.) This should extend beyond computer science and technical degrees and should encompass degree programs in critical industry sectors – healthcare, energy, transportation – as well as increased general education offerings on the importance and basics of cybersecurity.

### **2.1.2: Improve conditions for community college cyber graduates to seamlessly transition to four-year colleges and universities**

Many of Maryland's two-year community college programs focus on applied programs such as Computer and Information Sciences to gain practical skills. In contrast, four-year institutions prioritize theoretical degrees, such as Computer Science. Employers cite the importance of both credentials and experience for their workforce, however there are limited pathways for students to transfer credits seamlessly. While the 2021 Transfer with Success Act empowered the Maryland Higher Education Commission to strengthen articulation agreements, progress has been limited and transferability must still be negotiated institution by institution, program by program. This creates barriers for students wishing to attain higher-level education and credentials.

Cybersecurity is an example of a rapidly evolving field that is ripe for more expedited and system-wide transfer options. Such mechanisms would maximize students' opportunities to continue to upgrade their skills and attain four-year degrees and provide employers with a broader talent pool. The Cyber Maryland Board should work with the Maryland Higher Education Commission to identify the competencies, skills, and knowledge needed for a bachelor's degree that leads to an entry-level position in the cybersecurity industry. Once identified, the Maryland Higher Education Commission should work with Maryland's colleges and universities to implement relevant bachelor-level degree programs, with special attention to support students transferring from existing associate degree programs.

<sup>14</sup> “We Must Consider Software Developers a Key Part of the Cybersecurity Workforce,” Jack Cable, Senior Technical Advisor, CISA  
<https://www.cisa.gov/news-events/news/we-must-consider-software-developers-key-part-cybersecurity-workforce>



## STRATEGY 2.2: Integrate Experiential Learning into Postsecondary Degree Pathways in Cybersecurity

Cybersecurity employers emphasize the need to translate classroom knowledge into real-world application through practical work experiences. Internships and (RAs) provide intensive opportunities for hands-on learning, and expanding their availability is key to bridging the gap between education and employment. Training environments, such as cyber ranges and cyber clinics, allow students to collaborate as teams to respond to cyber threats, bridging the gap between theoretical knowledge and practical application.

In 2017, Maryland opened a first-of-its-kind cyber range – the Baltimore Cyber Range (BCR)<sup>15</sup> – which offers an interactive platform that simulates real-world cybersecurity scenarios to provide hands-on experiential learning in a controlled, secure environment. Cyber clinics take experiential learning a step further into the “real world” of work by enabling students to assist local businesses or organizations in securing their networks and data, under the guidance of a cybersecurity professor or practicing expert. The White House’s National Cyber Workforce and Education Strategy also prioritizes the expansion of cyber clinics.<sup>16</sup> Maryland has hosted one cyber clinic at Prince George’s Community College<sup>17</sup>, but challenges remain in making these proven models for experiential learning widely accessible to meet growing student demand.

**To support expansion of these types of experiential learning, Maryland should:**

### 2.2.1: Scale and build upon cyber ranges across Maryland

Cyber range models that reach students across Maryland and are integrated with ongoing learn-and-earn opportunities, including registered apprenticeship, need to be expanded across the state. Work has already begun on this effort: In November 2024, Governor Moore announced a grant of \$1.8 million to the Maryland Association of Community Colleges (MACC), the Maryland Workforce Association (MWA), and the BCR.<sup>18</sup> This \$1.8M investment will allow all 16 community colleges to offer cutting-edge experiential training through cyber ranges. Through this investment and ongoing work, it will be crucial to build upon the cyber range experiences by expanding to additional settings, adding operational technology training, simulations, and assessment of cyber skills, as well as direct connections to apprenticeship and employment in cyber roles. Continuous evolution of cyber ranges and related experiences will require routine engagement and feedback from industry experts to

15 Defense Daily, First U.S. Public Cyber Security Training Facility Opens In Baltimore, 2017, <https://www.defensedaily.com/first-u-s-public-cyber-security-training-facility-opens-baltimore/international/>

16 The White House, FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America’s Cyber Talent, 2023, <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-%E2%81%A0harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/>

17 <https://www.pgcc.edu/about-pgcc/news/2024/prince-georges-community-college-national-cyber-security-center-announces-new-cyber-clinic-and-roundtable-highlighting-microsofts-cyber-skilling-grant-to-support-students.php>

18 <https://governor.maryland.gov/news/press/pages/governor-moore-announces-18-million-investment-to-bolster-cybersecurity-training-at-every-maryland-community-college.aspx>

ensure up-to-date relevant experience.

### **2.2.2: Establish industry-specific cyber clinics at Maryland's community colleges and universities**

---

Cyber clinics gather local small businesses and students to solve current cybersecurity issues faced by business owners. Clinics bolster the cybersecurity ecosystem by engaging local communities, bringing in expertise and leadership from community college faculty and senior students, providing hand-on, low-risk training for cybersecurity students, and acting as a primer to generate interest in students who are not currently focused on cybersecurity career paths. Maryland should invest in funding one or more pilots to establish industry-specific cyber clinics. These clinics would provide relevant, industry-based training to support local community members and businesses in developing cybersecurity infrastructure and processes to protect their businesses – providing cybersecurity services to a local business that might not otherwise have it. Cyber clinics can leverage the existing Centers of Academic Excellence (CAEs) in Maryland, which are linked to local feeder schools and can be leveraged for internships and cybersecurity career pathways. Investments in cyber clinics are underway at the University of Maryland, Baltimore County (UMBC) and by Gula Tech Adventures. Pilot programs could include incentives for local businesses to hire postsecondary students to work on cybersecurity projects.

### **2.2.3: Integrate certifications, internships, and work rotations into degree pathways**

---

Key cyber ecosystem leaders, including representatives of higher education institutions, Chief Information Security Officers (CISOs) from state, local Maryland government, and private employers emphasized a need to expand work-based learning programs for both entry-level students and mid-level students.

Maryland needs a robust set of work-based learning experiences that can be woven into degree programs and that support the full career journey of the cybersecurity workforce. This continuum must start from foundational IT training, such as data science or IT administration before entry-level cybersecurity roles. Moving along the continuum, students can gain cyber specialization through work-based learning. The continuum should include identification of concrete opportunities to weave industry-relevant certifications, internships and work rotations into degree programs. The Cyber Maryland Board should convene Maryland higher education institutions, Maryland-based employers, Maryland Department of Labor, and the Maryland Higher Education Commission to develop strategies and programs to incorporate work-based learning opportunities into degree programs.



## **STRATEGY 2.3: Increase Access to Postsecondary Degree Pathways in Cybersecurity**

Maryland employers are seeking specialized talent to meet the growing demands of their cybersecurity operations, but the state's financial aid and investment structures often fail to connect learners with the opportunities they need. While Maryland boasts a strong cybersecurity ecosystem, many learners and potential workforce entrants are unaware of the pathways available to develop the precise skills employers require. One industry leader noted, "Employers are asking for very specific skills, but the state's funding often goes to general programs that don't prioritize these requirements." This underscores the importance of targeted outreach rather than creating new, narrowly focused programs. By strategically connecting learners with existing opportunities, including certifications, apprenticeships, and specialized degrees, Maryland can better align talent development with workforce needs, ensuring both students and employers achieve their goals.



**To address this disconnect, Maryland should:**

### **2.3.1 Realign Maryland's scholarships and other investments to employer demand**

In 2025 and 2026, the Cyber Maryland Board, the Governor's Workforce Development Board, and Maryland High Education Commission's Office of Student Financial Assistance (OSFA) should review Maryland's scholarships and investments to ensure they effectively align with employer demands and support learners pursuing cybersecurity careers. This review should focus on identifying gaps in funding for certifications, hands-on training, and specialized degree pathways while emphasizing strategic outreach to connect learners with these opportunities.

Existing programs such as the Cybersecurity Public Service Scholarship, which ties funding to in-state service commitments, and the Maryland Technology Internship Program (MTIP), which reimburses employers for hiring interns, provide valuable models for further development. Instead of creating new programs, targeted outreach can better inform learners of these resources, helping to bridge gaps between talent and opportunity. Maryland can strengthen its efforts to retain skilled graduates and build a robust local workforce by exploring incentives – such as retention bonuses or scholarships tied to post-graduation work commitments – that align with proven initiatives like the Kansas Promise Act or the Michigander Scholars program.

## **GOAL 3: Expand Pathways into Cybersecurity Beyond Traditional Higher Education**

Degree requirements have consistently been a signal commonly used by employers to indicate readiness – but employers have cited credentials, as well as experience, as even more important requirements for many in-demand cyber roles. Moreover the cybersecurity sector has already set a precedent for prioritizing credentials and certifications, for hiring applicants.<sup>19</sup>

While investments in higher education represent one pathway to narrowing these statewide talent gaps, Maryland’s strategy must extend beyond traditional postsecondary degrees to build new pathways into cyber roles for adult learners and jobseekers that focus more on skills, competencies, and credentials than traditional postsecondary degrees. By diversifying the types of pathways available into cybersecurity skills, Maryland will expand the pool of talent and ensure talent can be developed quickly for key roles where doing so is feasible, including those with clear certification pathways such as Penetration Testers, Support Technicians, and Cybersecurity Analysts.<sup>3</sup>

### **STRATEGY 3.1: Expand Registered Apprenticeships and Work-Based Learning in Cybersecurity**

Currently, Maryland’s limited apprenticeships and work-based learning opportunities in cybersecurity roles – targeting roles such as SOC analysts and penetration testers impact the development of a robust entry-level talent pipeline. In 2023, 14 organizations hosted a combined 249 cybersecurity registered apprentices statewide. Key barriers to expansion include administrative complexities in establishing RA programs; below-market wages and reimbursements for entry-level cybersecurity apprenticeships; and participation requirements, such as the one-to-one supervisor-to apprentice ratio, which – while pertinent for hazardous occupations, does not align with how cybersecurity workplaces operate best.

**To support this goal, Maryland should:**

#### **3.1.1: Expand career and technical education through registered apprenticeship and other work-based learning opportunities in K-12**

Preparing students for cybersecurity careers must begin before postsecondary education. The state should enhance cybersecurity learning within K-12, including Career and Technical Education (CTE) programs. To advance this effort, beginning in FY 2026, the Governor’s Workforce Development Board’s Career and Technical Education Committee should collaborate with school districts, Maryland State Department of Education and

<sup>19</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>

Maryland Department of Labor to design and implement an investment that pilots the development of registered apprenticeship or pre-apprenticeship in cybersecurity, and expand CTE-connected cybersecurity offerings in high school.

### **3.1.2: Provide support and incentives for cyber employer exploration of registered apprenticeship**

---

To expand the number of cybersecurity RAs, Maryland should invest in the development, adoption, and expansion of RAs for cyber roles such as cybersecurity analyst, information systems security engineer, SOC analysts, and penetration testers. Beginning in FY 2026, the Maryland Department of Labor should engage intermediaries with a proven track record in creating cybersecurity apprenticeships. Maryland Department of Labor should invest in the creation of incentives for employers, such as tax credits and “pay-per-apprentice” incentives to further encourage cybersecurity employer participation in RAs.

### **3.1.3: Tailor registered apprenticeship requirements and branding for cyber careers**

---

While Maryland has successfully grown RAs statewide and in multiple sectors, many cybersecurity occupations and employers have needs that do not easily conform to traditional registered apprenticeship and require a tailored approach. Recognizing the unique demands of cybersecurity, Maryland should maximize registered apprenticeship requirements and support branding that better aligns with industry standards.

Beginning in FY 2026, Maryland Department of Labor should take steps to educate the industry on the ability for registered apprenticeship programs with non-hazardous occupations to request an expansion of the 1:1 journeyworker (mentor)-to-apprentice ratio requirements for non-hazardous occupations like cybersecurity. Requests for expanded ratios in cyber occupations have previously been approved but the industry is generally not aware of this. The education of the industry regarding this shift could make cybersecurity RAs more accessible and scalable for employers, expanding opportunities for apprentices without compromising the quality of mentorship, safety, or training.

Additionally, many employers acknowledge that terminology and branding matter to both employers and jobseekers in their industry, and that the “apprenticeship” branding may not always align to their interests. RAs in cybersecurity must be branded using industry-relevant terminology that resonates with cyber employers. Maryland Department of Labor should invest in an intermediary familiar with cyber terminology and promote RAs with a tailored brand.

## STRATEGY 3.2: Support Employer Adoption of Skills-First Hiring and Advancement Practices

In 2022, Maryland became the first state in the country to issue a commitment to removing postsecondary degree requirements from a large share of state government jobs that require specific skills and competencies that are not necessarily conferred solely by postsecondary degrees.<sup>20</sup> In the years since, over a dozen states have followed suit.<sup>21</sup> In addition to exploring greater adoption of skills-first approaches to hiring and advancement within government agencies, states and thought-leaders across the country are increasingly exploring methods to encourage adoption of skills-first approaches by private sector employers. This coincides with increasing recognition that many employees may be appropriately skilled for a wide range of good jobs through “alternative routes” to postsecondary degree programs, particularly in light of the reality that nearly 70% of Americans do not have – and often cannot afford to obtain – a postsecondary degree.<sup>22</sup>

At the same time, cybersecurity employers in Maryland have articulated that their greatest unmet talent needs center around specific skillsets and experiences. Historically, credentials have been viewed by employers as an important addition to degrees, even though cybersecurity has a number of robust and clearly-articulated certification pathways.<sup>23</sup> This information combined suggests that several demand gaps may be filled more readily with employer adoption of skills-first hiring and advancement approaches that allow credentials and experience to more readily substitute for degrees.<sup>24</sup>

**To support this goal, Maryland should:**

### 3.2.1: Develop tools and resources to collaborate with employers’ human resources teams on real-world skill, competency, and credential needs to better fill cyber roles

Several cybersecurity employers interviewed during this study cited a disconnect in their human resources department’s knowledge and understanding of required skillsets for cybersecurity roles, which impacts the effectiveness of their recruitment practices. Additionally, recent research has underscored that even when an employer proclaims an intent to focus on skills over degrees, actual hiring practices and corporate cultures are often slow to catch up.<sup>25</sup> Maryland can leverage early work pioneered by national organizations and other states to develop and deploy tools and resources to educate

20 <https://www.americanprogress.org/article/the-benefits-of-skills-based-hiring-for-the-state-and-local-government-workforce/>

21 <https://www.nga.org/news/commentary/governors-leading-on-skills-based-hiring-to-open-opportunity-pathways/>

22 <https://opportunityatwork.org/wp-content/uploads/2022/01/Rise-with-the-STARs.pdf>

23 <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf> p. 27

24 <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>; insights gathered during interviews of over 30 employers by GWDB, TEDCO and Fierce Outcomes staffs between June-August 2024.

25 <https://www.hbs.edu/managing-the-future-of-work/Documents/research/Skills-Based%20Hiring.pdf>

employers' human resources teams on the skills, competencies, and credentials needed to fill cyber roles and on practices to support greater adoption of skills-based hiring and advancement within organizations.

Beginning in FY 2025, the GWDB should complete a study on advancing skills-based approaches to recruitment, hiring, and advancement in both public and private sector employment.<sup>26</sup> The GWDB should collaborate with the Cyber Maryland Board to explore feasible applications of its recommendations within the cyber field.<sup>27</sup>

## **STRATEGY 3.3: Boost to Cyber Talent Supply and Diversity Through Targeted Programs and Supports**

In addition to diversifying the types of education and training pathways available in cybersecurity, addressing regional talent gaps will require diversification of the workforce itself, by engaging untapped talent pools in communities across the state. Targeted programs that broaden access to training, incentivize employer engagement of hires with diverse educational backgrounds, and support transitioning veterans and underrepresented groups are vital.

A wider talent net can be cast by investing in proven programs that deliver valuable, industry-recognized credentials and skills in a shorter time frame than traditional postsecondary degrees. Moreover, there are significant and underutilized opportunities for many employers to re-skill current employees with skill adjacencies into cyber roles within their organizations. Finally, Maryland can better engage transitioning veterans who possess relevant skillsets and clearances, and can build on existing programs that cultivate greater demographic diversity within the cybersecurity workforce.

**To support these goals, Maryland should:**

### **3.3.1: Expand access to short-term non-degree training and credentialing programs**

Short-term training and credentialing programs offer an efficient and accessible pathway for individuals to gain the skills needed for in-demand cybersecurity roles.<sup>28</sup> While employers generally indicated that work experience was most important, several shared that it was important for entry-level staff to hold key certifications. Investments in non-degree training programs can create multiple accessible pathways for skills development and credential attainment. Maryland College Promise Scholarship ("Promise") is a critical tool that can now support non-degree credentials and certificates, as well as related instruction for registered apprenticeship. However, it is not yet happening at scale. The Maryland Higher

<sup>26</sup> <https://mgaleg.maryland.gov/Pubs/BudgetFiscal/2024rs-budget-docs-jcr.pdf> p. 159-160

<sup>27</sup> <https://www.markle.org/skillful/>

<sup>28</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>; insights gathered during interviews of over 30 employers by GWDB, TEDCO and Fierce Outcomes staffs between June-August 2024.



Education Commission and the Maryland Department of Labor should collaborate to ensure that community colleges institutionalize processes for students to access Promise dollars for these purposes, given that the scholarships are managed locally in a decentralized fashion.

Maryland Department of Labor should prioritize investing in programs and credentials that leverage private-sector offerings and engage key federal and state agencies, so that the results meet the needs of employers and learners alike. These programs should be designed to be accessible statewide, ensuring equitable opportunities for participation.

### **3.3.2: Leverage existing and/or develop new incentives for incumbent worker training**

---

Employers cite the importance of prior work experience in cybersecurity roles, yet it is difficult for candidates to gain entry-level experience: only 31% of cyber job postings in Maryland and DC are open to candidates with less than two years of experience.<sup>29</sup> This gap presents an opportunity for employers to prioritize internal training programs that build cybersecurity expertise among existing employees. Employers may not be aware that state resources are available to support upskilling efforts.

To bridge this gap, the Governor's Workforce Development Board, the Maryland Department of Labor, local workforce development boards (LWDBs), and the Maryland Higher Education Commission should encourage employers to leverage resources, such as Workforce Innovation and Opportunity Act (WIOA) and EARN Maryland funds, to support training for qualifying employees transitioning from IT to cybersecurity roles. Maryland Department of Labor should pursue additional chances to expand these opportunities via private, philanthropic or other funding opportunities. By providing employers with the tools and support needed to invest in incumbent worker training, Maryland will strengthen its cybersecurity workforce while retaining valuable talent. The Partnership for Workforce Quality in the Department of Commerce may serve as a model to replicate.<sup>30</sup>

### **3.3.3: Increase engagement of transitioning veterans within Maryland who have cyber skills, adjacent skills, and/or relevant clearances acquired during their service**

---

Maryland's veteran population represents a valuable talent pool for the cybersecurity industry, with many veterans possessing transferable skills, clearances, and technical expertise acquired during their service.<sup>31</sup> Several government contractors indicated that they found exiting veterans to be an attractive talent pipeline and that they specifically worked to engage veterans in their recruiting processes.

---

<sup>29</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf> P. 30-31

<sup>30</sup> <https://commerce.maryland.gov/grow/partnership-for-workforce-quality-pwq>

<sup>31</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf>; insights gathered during interviews of over 30 employers by GWDB, TEDCO and Fierce Outcomes staffs between June-August 2024.

Given the strong alignment between veterans' skills and the needs of the cybersecurity industry, Maryland should focus on developing additional resources to support transition into the industry. The Governor's Workforce Development Board, in partnership with the Maryland Department of Labor, the Department of Veterans Affairs, and the Cyber Maryland Board, should explore the development of a state-level program, modeled after initiatives like Cyber Vets Virginia, to provide transitioning veterans with career guides, advisement, and connections to training and employment opportunities. This program could complement existing efforts, including DoD SkillBridge, [CyberVets.org](https://www.cybervets.org), and Maryland Department of Labor's Jobs of Veterans State Grants program, to ensure that veterans are equipped to transition seamlessly into cybersecurity roles.

### 3.3.4: Build on programs that cultivate greater diversity in the cyber workforce

---

Developing a diverse cybersecurity workforce is essential to addressing the field's challenges and fostering equitable opportunities.<sup>32</sup> The cybersecurity sector in Maryland and DC demonstrates stronger gender and racial diversity compared to the broader tech industry, with women holding 35% of roles and significant representation of Black and Hispanic professionals compared with other regions.

#### **ACTION HIGHLIGHTS:**

Establish partnerships with organizations such as Girls Who Code and Black Girls CODE to expand local chapters and create mentorship and training opportunities for underrepresented groups.

Philanthropic and private sector actors should partner with higher education institutions to help students of all backgrounds complete cybersecurity and computer science degrees at the associate's and bachelor's levels and beyond.

These initiatives will not only increase representation in the cybersecurity workforce but also provide ongoing career advancement support, ensuring that Maryland's workforce reflects the diversity of its communities.

---

<sup>32</sup> <https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf> P. 43-44



## **GOAL 4: Strengthen the Federal, State, and Local Government Cyber Workforce**

As the home to key federal agencies like the National Security Agency (NSA) and US Cyber Command, as well as state and local entities responsible for protecting critical infrastructure, Maryland is optimally positioned to lead in building a robust public-sector cybersecurity workforce. However, government employers face persistent challenges in filling cybersecurity roles, due to complex hiring processes, high demand for security clearances, and a competitive private-sector job market. At the state and local levels, Chief Information Security Officers and smaller government entities struggle with limited capacity to upskill or train entry-level hires, small IT teams with limited available roles, and constrained budgets. This hampers their ability to maintain a pipeline of hires and effectively address growing cyber threats.

As cyber threats grow in complexity and digital infrastructure becomes central to government operations, addressing workforce barriers is critical to national security and the protection of public infrastructure. Strengthening cybersecurity talent pipelines at the federal, state, and local levels will position Maryland as a leader in public-sector cyber workforce development while expanding high-quality career pathways for its residents. By investing in skilled talent and fostering cross-sector collaboration, Maryland can build a resilient workforce capable of responding to evolving cyber risks.

## **STRATEGY 4.1: Develop and Expand Federal Partnerships**

Federal agencies and government contractors face significant challenges in securing the cybersecurity talent necessary to protect national security. Delays in obtaining security clearances—often taking 12–24 months—prevent timely onboarding of new hires, particularly entry-level talent. Sensitive roles have rigorous requirements for experience, credentials, and certifications, but limited pathways exist for graduates to gain these qualifications. Contractors struggle with high onboarding costs, contract restrictions that exclude interns and apprentices, and retention challenges as cleared professionals command premium salaries in a competitive market. These systemic issues leave many critical cybersecurity positions unfilled and hinder the development of a robust public-sector workforce.

Maryland must support partnerships between federal agencies (such as the NSA, US Cyber Command, US Office of Personnel Management, other government agencies, etc.), contractors, and higher education institutions to address these barriers and streamline the talent pipeline to ensure the state is producing workforce-ready graduates while addressing critical security gaps in government agencies and contractors.

### **To support this goal, Maryland should:**

#### **4.1.1: Work with NSA, US Cyber Command, and other cyber-focused federal agencies to promote internships, RAs, and other early job pathways that incorporate clearance processes where feasible**

The Governor's Workforce Development Board, in collaboration with the Cyber Maryland Board, Maryland Department of Labor, Maryland Higher Education Commission, and Maryland State Department of Education, should collaborate with federal intermediaries, government contractors, and agencies to advocate for the creation and expansion of skill-based job codes within federal contracts. This would enable student interns and apprentices to contribute to billable work while gaining experience, even without meeting traditional requirements like degrees or years of experience. By incorporating entry-level labor categories, contractors can reduce payroll costs during clearance processing and develop a direct pipeline to full-time hires. The state should focus on scaling successful apprenticeship models that incorporate security clearance, such as the Howard Community College's IT Apprenticeship Program in partnership with AT&T, and prioritizing work with NSA, given its heightened security requirements and significant share of cybersecurity contracts. The GWDB should work with sister agency partners, such as Maryland Department of Labor and Department of Information Technology, to facilitate collaboration between federal intermediaries, contractors, and federal agencies to design new work-based learning programs through which students can gain experience working at both federal agencies and contractors as part of a single program.

These efforts can support recommended actions under Goals 1 - 3 of this report. At employer focus groups convened during 2024, different exploratory models were raised:

**Talent Bridge Program:** Students are assigned non-sensitive, cybersecurity-relevant tasks at entities such as government contractors while awaiting clearance. After clearance is granted, students transition to working at a federal agency for a predetermined period.

**Rotational Program:** Students join a centralized work-based learning pool and are assigned to non-sensitive work based on demand, rotating between agencies and contractors as needs arise. This dynamic, market-clearing mechanism maximizes the time students spend on cybersecurity-relevant tasks while exposing them to both types of employers.

#### 4.1.2: Explore partnership with State / NSA and US Cyber Command on a multi-purpose cyber workforce center

---

Building a strong cybersecurity ecosystem requires a consistent physical presence. To address this need, the Maryland Department of Labor, Cyber Maryland Board, and Maryland Department of Commerce are exploring the creation of a dedicated physical site to support a wide range of workforce development initiatives focused on cybersecurity. This center would serve federal, state, and local employers and would be developed in collaboration with US Cyber Command, the Fort Meade Alliance, and private sector and nonprofit organizations like the Technology Advancement Center (TAC), which already plays a significant role in similar efforts. Ideally, the cybersecurity talent pipeline components of multiple federal agencies (DoD, NSA, CISA, FBI, Treasury, SSA, HHS, NASA, FDA, CIA, DIA) would co-locate along state programs at the center.

The proposed cyber workforce center would function as a hub for work-based learning, secondary and post-secondary cyber education, and resources to support entry into the cybersecurity workforce at all levels. It would host conferences, provide training and job placement services, and act as a one-stop shop for cybersecurity businesses, contractors, and returning veterans. Additionally, the center would include secure facilities for innovation and entrepreneurship, fostering a dynamic environment for advancing cybersecurity initiatives. While exploring spaces for a physical location, a website should be created – a one stop shop which lists all public and as many private cyber jobs in Maryland.

This aligns with the recent recommendations from “Cyber Command 2.0” which acknowledges that U.S. Cyber Command must streamline its partnerships with industry and envision a new system for how the military services recruit and retain talent. The proposals include a cyber training center which “probably piggybacks on the innovation hub, with the command’s own instruction curriculum beefed up by the private sector.”<sup>33</sup> Maryland should partner with the Office of the National Cyber Director to connect Maryland with federal agencies who are willing to partner on developing a physical facility. Furthermore, the state could pilot a trial period with students from schools across the state prior to the development of a physical space with existing resources (e.g., at the TAC).

---

33 <https://therecord.media/cyber-command-2-0-project-progress-military-congress/>

### 4.1.3: Support partnerships between Maryland universities and federal agencies for cybersecurity research and development

---

Growing the cybersecurity ecosystem in Maryland will also require cultivating research and development which, in turn, can fuel entrepreneurship. Maryland should explore the development of the Maryland Cybersecurity Research Collaborative, to promote industry-relevant research, further collaboration between Maryland institutions, and cutting-edge intellectual property and research and development created by the state of Maryland. This would build on existing partnership infrastructure including the National Defense University, in DC;<sup>34</sup> the National Security Agency (NSA) Research Science of Security Virtual Institute,<sup>35</sup> and strengthening individual and collective ties with the Cybersecurity & Infrastructure Security Agency (CISA).

### 4.1.4: More effectively market existing federal scholarship programs

---

Existing federal scholarship programs, such as the Department of Defense (DoD) SMART Scholarship for Service Program or the CyberCorps Scholarship for Service Program, can fund either graduate or undergraduate level education. Recipients must agree to serve for a period equivalent to the length of the scholarship.

The DoD SMART Scholarship allows applicants to pursue degrees in 24 STEM disciplines, including:

- Computer Science and Engineering
- Cybersecurity
- Data Science and Analytics
- Information Sciences
- Software Engineering

The CyberCorps Scholarship is designed to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

## STRATEGY 4.2: Develop New State & Local Government Cyber Talent Initiatives

Maryland's state and local governments face unique challenges in maintaining a steady pipeline of talent and scaling their cybersecurity workforce. State and local government IT teams are often resource constrained and believe they cannot afford the productivity loss associated with mentoring new graduates. Additionally, many recent graduates pursue industry over government roles due to more competitive compensation and limited awareness of government roles.

---

<sup>34</sup> <https://www.google.com/url?q=https://cic.ndu.edu/About/Fact-Sheet/&sa=D&source=docs&ust=1733457115935695&usg=AOvVaw37Yddse-dwbNQhLBafpk3C>

<sup>35</sup> <https://www.google.com/url?q=https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3796389/nsa-and-universities-partnering-to-advance-cybersecurity-research/&sa=D&source=docs&ust=1733457115936047&usg=AOvVaw2Hfw8ewOJBp0qjRjKXfve7>

Maryland's strategy should focus on expanding pathways to public-sector cybersecurity employment by addressing financial and logistical barriers for both governments and students. Investments should prioritize developing work-based learning programs tailored to state and local government needs, while also supporting financial incentives to encourage student participation. The establishment of these types of initiatives would position Maryland's public sector as a viable and attractive option for cybersecurity graduates, ensuring a steady pipeline of talent to address critical workforce gaps.

**To support this goal, Maryland should:**

#### **4.2.1: Coordinate State agency action to fill cybersecurity roles**

---

The State should take a coordinated approach to decreasing agency barriers to fill cybersecurity roles, including improved adoption of skills-based hiring. Agencies should work in FY 2026 to launch a registered apprenticeship program in state government for one or more cybersecurity occupations. Lastly, the State should build processes and infrastructure to prioritize filling state IT procurement contracts with vendors who have developed strong cybersecurity apprenticeship programs. Positive examples include Minnesota's "Whole of State Cybersecurity Plan" which focuses on a united front against cyber threats across state, local, tribal governments, as well as school districts and key government vendors.

#### **4.2.2: Explore a service-based learning program for cybersecurity training**

---

In FY 2026, the Cyber Maryland Board in collaboration with the Maryland Department of Service and Civic Innovation (DSCI), should consider a feasibility study to explore the design and implementation of a service-based program for cybersecurity training. This program could incorporate key aspects of models in other regions, such as the Ohio Digital Academy, whose inaugural January 2024 cohort filled 26 entry cybersecurity roles in Ohio state and local governments. The Department of Service and Civic Innovation (DSCI) and key state agencies should explore a service program pilot to achieve a three-pronged goal of providing high quality cybersecurity jobs for Marylanders, filling state and local government cyber job openings, and building the base of entry-level cyber talent in the state of Maryland. In addition, the Governor's Workforce Development Board and Cyber Maryland Board can support DSCI in identifying opportunities to incorporate cybersecurity roles into the existing Service Year Option and Maryland Corps programs.

# Cyber Maryland Board Members

(AS OF DECEMBER 31, 2024)

**Roger Austin**

*Security and Risk Director*

Boston Consulting Group

*\*Board Chair*

**Greg Rogers**

*Chief Information Security Officer*

Maryland Department of Information  
Technology

*\*Board Vice Chair*

**Supro Ghose**

*Chief Information Security Officer*

Graphene Security, Inc

*\*Board Vice Chair*

**Kenneth Allman**

*Assistant Professor of Cybersecurity*

Garrett Community College

**Loyce Best Pailen**

*Sr. Director, Center for Security  
Studies*

University of Maryland Global  
Campus

**Thomas Byrd**

*VP & Enterprise Security, Senior Cyber  
Security Manager*

T. Rowe Price

**Derrek B. Dunn**

*Dean, School of Business and  
Technology*

University of Maryland Eastern Shore

**Hon. Katie Fry Hester**

*Senate co-chair Joint Committee on  
Cybersecurity, IT, and Biotechnology*

Maryland Senate

**Allen Kachalia**

*Senior Vice President, Patient Safety  
and Quality*

Johns Hopkins Medicine

**Hon. Anne Kaiser**

*House co-chair Joint Committee on  
Cybersecurity, IT, and Biotechnology*

Maryland House of Delegates

**Troy LeMaile-Stovall**

CEO

TEDCO (Maryland Technology  
Development Corp.)

**Kim Mentzell**

*Director of Cybersecurity and  
Aerospace*

Maryland Department of Commerce

**Kirkland Murray**

*President and CEO*

Anne Arundel Workforce  
Development Corporation

**Laura Nelson**

CEO

National Cryptologic Foundation

**Gregg Smith**

CEO

Technology Advancement Center  
(TAC)

**Rachael Stephens Parker**

*Executive Director*

Governor's Workforce  
Development Board

**Tami Watkins**

*Director of Government &  
Regulatory Affairs*

Comcast

**Hon. Anthony Woods**

*Secretary*

Maryland Department of  
Veterans Affairs



# Governor's Workforce Development Board Members

(AS OF DECEMBER 31, 2024)

**Hon. Wes Moore**

*Governor*

**Carim V. Khouzami**

*President & CEO*

BGE

*\*Board Chair*

**Delali Dzirasa**

*Founder & CEO*

Fearless

*\*Board Vice Chair*

**A. Ferris Allen, III**

*Thoroughbred Horse Trainer*

Warwick Stable

**Hon. Kevin Anderson**

*Secretary*

Maryland Department of Commerce

**Hon. Vanessa Atterbeary**

*State Delegate, District 13*

Maryland House of Delegates

**Alexander Austin**

*President & CEO*

Prince George's Chamber of Commerce

**Marco V. Ávila**

*Vice President*

WSP

*President/CEO*

Maryland Hispanic Chamber of Commerce

**Hon. Calvin Ball, III**

*County Executive*

Howard County

**John D. Barber, Jr.**

*President of Local 177*

Northeast Regional Council of Carpenters

**Hon. Joanne C. Benson**

*State Senator, District 24*

**Jody Boone**

*Acting Assistant State Superintendent*

Division of Rehabilitation Services Maryland State  
Department of Education

**Donald Boyd**

*Supervisor of Strategic Initiatives*

Dorchester County Public Schools

**Jennifer W. Bodensiek**

*Chief Development Officer*

Junior Achievement of Greater Washington

**Brian S. Cavey**

*International Vice President*

International Association of Heat and Frost Insulators  
& Allied Workers

**Annesa Cheek**

*President*

Frederick Community College

**Donna Edwards**

*President*

MD State and DC AFL-CIO

**Mackenzie Garvin**

*Director*

Baltimore Mayor's Office of Employment Development

**Steven W. Groenke**

*CEO*

Himmelrich Associates, Inc.

**Kevin D. Heffner**

*President and CEO*

LifeSpan Network

**Stacey Herman**

*Assistant Vice President, Neurodiversity and  
Community Workforce Development*

Kennedy Krieger Institute

**Matthew R. Holloway**

*Owner & Operator*

Quantico Creek Sod Farms, Inc.

# Governor's Workforce Development Board Members

(AS OF DECEMBER 31, 2024)

**Roderick King**

Chief Diversity, Equity and Inclusion Officer  
University of Maryland Medical System

**Larry Letow**

CEO US  
CyberCX

**Robert "Rob" Limpert**

Regional Manager for Maryland and Virginia  
iCEV Multimedia

**Aminah "Amie" J. Long**

Human Resources Director  
Chaney Enterprises

**Jessica Mente**

Director of Training  
Royal Farms

**Kirkland J. Murray**

President and Chief Executive Officer  
Anne Arundel Workforce Development Corporation  
Maryland Representative for NAWDP

**Stephen Wayne Neal**

President/CEO  
K. Neal International Trucks, Inc  
K. Neal Idealease

**Myra W. Norton**

Senior Director  
Johns Hopkins Technology Ventures

**Sanjay Rai**

Secretary  
Maryland Higher Education Commission

**Edward C. Rothstein**

Commissioner Carroll County  
Commissioners Office

**Martin "Marty" Schwartz**

President  
Vehicles for Change

**Michelle B. Smith**

President & CEO  
1st Choice, LLC

**Brian Stamper**

Executive Director  
Cell Therapy Operations AstraZeneca

**Inez Stewart**

SVP-CHRO  
Johns Hopkins Medicine

**Teaera Strum**

Chief Executive Officer  
Strum Contracting Company Inc.

**Michael D. Thomas**

Vice President  
Workforce Development & Continuing Education  
Baltimore City Community College

**Perketer Tucker**

Director  
Office of Adult Education and Literacy Services, DWDAL  
Maryland Department of Labor

**Charles T. Wetherington**

President  
BTE Technologies, Inc.

**Carey Wright**

State Superintendent of Schools  
Maryland State Department of Education

**Portia Wu**

Secretary  
Maryland Department of Labor

**Charnetia V. Young**

Director, Workforce Initiatives  
CVS Health

## NON-VOTING MEMBERS

**Carol Beatty**

Secretary  
Maryland Department of Disabilities

**Jacob "Jake" Day**

Secretary  
Maryland Department of Housing and Community Development

**Rafael López**

Secretary  
Department of Human Services

**Paul Monteiro**

Secretary  
Maryland Department of Service and Civic Innovation

**Carmel Roques**

Secretary  
Maryland Department of Aging

**Vincent "Vinny" Schiraldi**

Secretary  
Department of Juvenile Services

**Laura Herrera Scott**

Secretary  
Maryland Department of Health

**Carolyn Scruggs**

Secretary  
Maryland Department of Public Safety and Correctional Services

**Paul Wiedefeld**

Secretary  
Maryland Department of Transportation

**Anthony "Tony" Woods**

Secretary  
Department of Veterans Affairs





## Acknowledgements

The Cyber Maryland Board and the Governor's Workforce Development Board extend their sincere gratitude to Fierce Outcomes for facilitating focus groups and research, their generous supporters at the Lumina Foundation, and the experts at Lightcast for their invaluable contributions to the data and recommendations presented in this action plan.

 **MDTEDCO**

 **MDTEDCO**

 **MDTEDCO**

 **TEDCO**

[tedcomd.com](http://tedcomd.com)

 **MDGWDB**

[gwdb.maryland.gov](http://gwdb.maryland.gov)