

## MARYLAND DEPARTMENT OF LABOR TESTIMONY ON SENATE BILL 241

TO: Education, Energy, and the Environment Committee Members  
FROM: Maryland Department of Labor  
DATE: January 30, 2025  
BILL: Cyber Maryland Program - Revisions

### MDL POSITION: SUPPORT WITH AMENDMENT

SB241 makes several enhancements to the *Cyber Maryland Program (Program)* to ensure that Maryland is a leader in this competitive industry. The legislation moves the *Program* and the associated *Cyber Maryland Board (Board)* and *Cyber Maryland Fund (Fund)* from the Maryland Technology Development Corporation (TEDCO) to the Maryland Department of Labor (MD Labor).

### Investing in Cybersecurity Workforce is Critical for Economic Growth

Growing Maryland's economy will rely on playing to the state's unique strengths. Cybersecurity is undoubtedly one of those strengths, and thus, our cybersecurity workforce must be at the heart of that strategy.

In March 2024, The Cyber Maryland Board issued a [report](#) analyzing the Maryland/DC Cybersecurity workforce landscape. That analysis showed that the Maryland-DC area has nearly the highest demand for cybersecurity jobs in the nation, second only to Virginia, with a level of demand for cyber talent over 3 times the national average. What is more — the DMV has the largest talent gap in the nation — with several thousand open cybersecurity jobs in Maryland and DC at any given time. The analysis estimated that only a third of the gap can be met with available workers. This means it's not just about connecting people to high-demand cybersecurity jobs, it's about preparing more people for these jobs.

Maryland's cybersecurity talent ecosystem is unique, shaped by the presence of the NSA, NIST, and other critical federal agencies. Not surprisingly, a significant portion of open cybersecurity roles are at government contractors, meaning the roles often require specialized skill as well as security clearances.

Growing Maryland's cybersecurity talent pipeline is paramount, not only because the industry is an area of key competitive advantage for the state but also because cybersecurity is increasingly necessary to every aspect of business operations. The new federal cyber incident requirements on the horizon for all critical infrastructure sectors will require these sectors—energy, finance, health, national security—to ensure they have the processes and personnel in place to meet the requirements of the law.

The potential for generative AI to radically reshape the nature of both cybersecurity attacks and tools for combatting cybersecurity threats are just two examples of the need for much stronger coordination.

[www.labor.maryland.gov](http://www.labor.maryland.gov)

Efforts to make software and technology tools “secure by design” also will require greater knowledge of cybersecurity by all IT developers, engineers and architects. Cybersecurity will also need to be incorporated into all technology jobs, and many jobs outside of tech, to make sure our workforce can develop the skills demanded by a shifting threat and opportunity landscape,

The vision of Cyber Maryland was that it would catalyze, develop, and sustain Maryland’s cyber workforce to support a thriving cybersecurity ecosystem. It is more imperative than ever that this vision be realized, and that we have a state workforce strategy that both provides pathways for individuals into cybersecurity and establishes the infrastructure to ensure our existing workforce can continue to evolve.

For these reasons, Governor Moore’s Budget, in addition to shifting the Cyber Maryland program to Labor, also proposes a significant investment of \$5M in Cyber Maryland.

TEDCO/Cyber Maryland and the Governor’s Workforce Board will be releasing the Maryland Cybersecurity Talent Strategy in February 2025. This strategy was developed through engagement with over 65 leaders in industry, government, academia, and workforce, and extensive involvement by members of the Cyber Maryland Board. The strategy is anchored in four key areas:

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 new pathways into cybersecurity careers beyond traditional higher education;*
4. *Strengthen the federal, state, and local government cybersecurity workforce.*

### **Moving the Cyber Maryland Program will enable the Department to leverage existing resources and infrastructure.**

The Department has a strong foundation of industry partnership and supporting skills programs to meet employers’ needs. Initiatives like the Maryland Works for Wind consortium—which brought together a robust sectoral partnership of 19 organizations, and has thus far supported 1,750 individuals to enroll in training programs—demonstrate MD Labor’s ability to drive strategic industry collaboration. The Department has already made significant investments in cybersecurity skills including:

- \$5.4 million during the Moore-Miller Administration through the EARN program to support 13 different organizations that provide cybersecurity occupations training, including \$1.6 million in FY25 alone;
- Cybersecurity Registered Apprenticeships in four occupations: Cyber Security Level I (18 apprentices), Cyber Security Support Technician (5 apprentices), Certified Cyber Analyst Operator (1 apprentice), and Junior Software Developer (89 apprentices); and
- A \$1.8 million award to BCR Cyber and the Maryland Association of Community Colleges from the Talent Innovation Fund to install and train over 1,100 Marylanders on cyber ranges.

Shifting the program to MD Labor will enable the Department to leverage its existing resources, grants and fiscal infrastructure, and expertise in workforce and industry partnerships to accomplish the bold goals of the action strategy.

At the same time, the Department envisions continued close collaboration with TEDCO, particularly around opportunities to engage business leaders and entrepreneurs, as well as the Department of Commerce as it invests in cybersecurity/IT as a lighthouse sector.

[www.labor.maryland.gov](http://www.labor.maryland.gov)

The changes proposed in SB241 partnered with the Administration's investments in the cybersecurity ecosystem will help to establish Maryland as the premier hub for cybersecurity in the nation.

### **Proposed Amendment**

The Department is seeking one (1) amendment to add the Adjutant General of Maryland to the composition of Cyber Maryland Board. This addition would ensure that the Maryland Military Department, the MD Defense Force, the MD National Guard, and their related assets are included and can contribute to the ongoing state cybersecurity policy efforts of the state.

**The Department respectfully requests a Favorable Report on SB241.** For questions, please contact Andrew Fulginiti, at [Andrew.Fulginiti@maryland.gov](mailto:Andrew.Fulginiti@maryland.gov)

[www.labor.maryland.gov](http://www.labor.maryland.gov)