

SB0867-EEE_MACo_SUP.pdf

Uploaded by: Dominic Butchko

Position: FAV



Senate Bill 867

Cyber Maryland Program - Revisions

MACo Position: **SUPPORT**

To: Education, Energy, and the Environment
Committee

Date: March 6, 2025

From: Karrington Anderson and Dominic J. Butchko

The Maryland Association of Counties (MACo) **SUPPORTS** SB 867, which expands and strengthens the Cyber Maryland Program by increasing funding eligibility and ensuring sustained investment in Maryland's cybersecurity workforce and infrastructure.

Beginning in FY 2026, the Cyber Maryland Program will award competitive grants and contracts for information technology and operational technology, reinforcing the State's commitment to cybersecurity workforce development and economic growth. SB 867 clarifies in law that local governments, workforce development boards, and economic development entities can access program funds. The bill ensures sustained and increased investment by allowing the Governor to include a \$3 million appropriation for FY 2026 and requiring an annual appropriation in the budget beginning in FY 2027.

By strengthening workforce development, SB 867 incorporates talent improvement strategies, such as those leveraging the U.S. Chamber of Commerce's Talent Pipeline Management approach, to ensure Maryland's cybersecurity workforce is well-prepared to meet evolving industry needs. Additionally, SB 867 reallocates unspent funds from multiple workforce and cybersecurity programs, including the Cybersecurity Investment Tax Credit, the Maryland Technology Internship Program, and the Cyber Public Service Scholarship, into the Cyber Maryland Program to maximize effectiveness.

As cyber threats continue to grow in sophistication and scale, local governments remain critical in safeguarding essential services and public safety. By expanding access to resources and ensuring sustainable funding, SB 867 empowers counties to develop a robust cybersecurity workforce and enhance digital resilience across Maryland.

For these reasons, MACo urges a **FAVORABLE** report on SB 867.

MML- FAV-SB 867.pdf

Uploaded by: Iris Ibegbulem

Position: FAV



Maryland Municipal League
The Association of Maryland's Cities and Towns

TESTIMONY

March 4, 2025

Committee: Senate -Education, Energy, and the Environment Committee

Bill: SB 867- Cyber Maryland Program-Revisions

Position: Favorable

Reason for Position:

The Maryland Municipal League (MML) respectfully supports Senate Bill 867, as it alters the Cyber Maryland Fund requirements for municipal entities, providing increased access to grants for local governments to support the state's cybersecurity workforce developments. More specifically, it allows for municipalities to operate cybersecurity programs cohesively with the Cyber Maryland Program's strategic plan with the opportunity for additional financial support.

The alteration to the requirements for the Cyber Maryland Fund additionally means increased economic development as local communities in the state of Maryland start and continue their own cybersecurity workforces. Expanding the requirements of the Cyber Maryland Fund and its funding opportunities to "local workforce boards, local government, local or regional economic development entities and other relevant partner entities" also means continued progress of the state's cybersecurity efforts, allowing for a diverse and inclusive workforce that reflects the diversity of the state itself.

For these reasons, the Maryland Municipal League respectfully requests a favorable report on SB 867. For more information, please contact Iris Ibegbulem, Senior Associate, Advocacy and Public Affairs at irisi@mdmunicipal.org or 443-295-9457. Thank you in advance for your consideration.

The Maryland Municipal League uses its collective voice to advocate, empower and protect the interests of our 160 local governments members and elevates local leadership, delivers impactful solutions for our communities, and builds an inclusive culture for the 2 million Marylanders we serve.

47 State Circle, Suite 403 Annapolis, Maryland 21401
(410) 295-9100 www.mdmunicipal.org

SB 867

Uploaded by: Katie Fry Hester

Position: FAV



THE SENATE OF MARYLAND
ANNAPOLIS, MARYLAND 21401

Testimony in Support of SB867 - Cyber Maryland Program - Revisions

March 6, 2025

Chair Feldman, Vice-Chair Kagan, and members of the Education, Energy, and Environment Committee:

Thank you for your consideration of **SB867 - Cyber Maryland Program – Revisions**, which transfers the CyberMaryland Program and CyberMaryland Fund from the Maryland Technology Development Corporation (TEDCO) to the Maryland Department of Labor.

For context, the state has a pressing need to fill currently open jobs. A [2024 report published by Lightcast](#) in collaboration with the CyberMaryland Board revealed that the Maryland/DC region has one of the highest demands for cybersecurity professionals in the country. Between December 2023 and January 2024, there were 9,781 cybersecurity job openings in the area.¹ At the same time, the region faces one of the nation's most significant talent shortages, with a gap of 6,513 unfilled positions.² As cyber threats continue to escalate, strengthening our cybersecurity workforce is critical to protecting personal information and ensuring digital security. Moreover, given the high demand for cybersecurity professionals, this sector presents a significant opportunity for economic growth and workforce development in Maryland.

This bill is similar to the Department of Labor's bill (SB241) heard on January 30th, which facilitates the transfer of the CyberMaryland program from TEDCO to the Maryland Department of Labor. However, it was drafted later, and thus has the benefit of being able to integrate the key findings from the Maryland Cybersecurity Talent Strategy³, and has additional details which expands the program's workforce development role and updates how its funding is utilized.

¹Cybersecurity Workforce Analysis & Strategy. (n.d.-b).
[https://www.tedcomd.com/sites/default/files/2024-05/TEDCO Cyber Maryland - Cybersecurity Workforce Strategy - Final Report.pdf](https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf). Page 13.

² Cybersecurity Workforce Analysis & Strategy. (n.d.-b).
[https://www.tedcomd.com/sites/default/files/2024-05/TEDCO Cyber Maryland - Cybersecurity Workforce Strategy - Final Report.pdf](https://www.tedcomd.com/sites/default/files/2024-05/TEDCO%20Cyber%20Maryland%20-%20Cybersecurity%20Workforce%20Strategy%20-%20Final%20Report.pdf). Page 17.

³ Maryland's Cybersecurity Talent Strategy 2025.

Maryland's Cybersecurity Talent Strategy was developed last year by the CyberMaryland Board and the Governor's Workforce Development Board. It has four fundamental goals aimed at closing the workforce gap for employers and expanding economic opportunity for Maryland in the process. These goals include:

1. Equipping every Marylander with foundational skills to grow the pipeline of potential cyber talent;
2. Transforming postsecondary cybersecurity education to align with industry needs;
3. Expanding new pathways into cybersecurity careers beyond traditional higher education; and
4. Strengthening the federal, state, and local Government cybersecurity workforce.

You will see these goals reflected in this draft of the bill. Specifically, SB 867 will:

- Transfer the CyberMaryland Program from TEDCO to the Department of Labor
- Expand the membership of the CyberMaryland Board, encourage diversity amongst board members, and set term restrictions for board members
- Require key performance metrics be included in the annual report on the Program to the Governor
- Allocate the funding in the Governor's budget to the CyberMaryland Fund to provide grants, while expanding and clarifying the eligibility criteria for recipient organizations to ensure activities in FY 2026 align with the most urgent priorities identified in the report.

The bill allocates:

- \$1,000,000 for the establishment of Cybersecurity Clinics to bridge the gap in education between theoretical and practical application, while simultaneously providing critical cybersecurity support to our water systems, hospitals and schools.
- \$500,000 to support the development of a service-based learning program for cybersecurity.
- \$500,000 to support transitioning veterans within the State who have cyber skills, adjacent skills, or relevant clearances acquired during their service.
- \$99,000 for talent pipeline management aligned with the framework from the U.S. Chamber of Commerce Foundation.
- \$250,000 to support existing or develop new programs and incentives for worker training.
- \$250,000 to support cybersecurity education at the kindergarten, elementary school, and secondary levels, including at summer camps.
- \$250,000 for a marketing campaign, in consultation with the Department of Commerce, to attract cyber talent and industry to the state
- \$250,000 for the Maryland Statewide Computing Alignment to Locate Education (SCALE) Portal. The Maryland Statewide Computing Alignment to Locate your

Education pathway (SCALE) project will enable youth and adults to follow a computing education training and/or industry certification pathway to enter Maryland's technologically advanced workforce.⁴

We have a consensus amendment from TEDCO and the Department of Labor for the committee which has a few technical changes and removes the re-appropriation of funds. We will share this amendment as soon as we receive it.

Moving the CyberMaryland Program will allow the Department of Labor to utilize existing resources and grants to better accomplish the goals of the Program. This version of the bill is strong because it clarifies and focuses how the state's resources will be spent. With this bill, we are taking a major step towards equipping Marylanders with the skills needed to enter the cybersecurity field and meet the growing workforce demand in our state.

For these reasons, I respectfully request a favorable report on SB867.

Sincerely,

A handwritten signature in dark ink, appearing to read "Katie Fry Hester". The signature is written in a cursive, flowing style.

Senator Katie Fry Hester
Howard and Montgomery Counties

⁴ *Statewide Computing Alignment to Locate your Education Pathway (SCALE)*. Retrieved from https://drive.google.com/file/d/1FqMG77ffxZ24S8RO5zx_qzDaawFtATvC/view

RJR-(NCF) SB867.HB1468 CyberMD Revisions (SUPPORT)

Uploaded by: Laura Nelson

Position: FAV



Senator Pamela Beidle, Chair
Senator Antonio Hayes, Vice-Chair
Senate Finance Committee
11 Bladen Street, Miller Senate Office Building, 3 East
Annapolis, Maryland 21401

Re: Senate Bill 867/ HB1468: Cyber Maryland Program – Revisions - SUPPORT

March 6, 2025

Dear Chairwoman Beidle and Committee Members:

As President & Chief Executive Officer of the National Cryptologic Foundation (NCF), I write this letter in support (with an amendment) of Senate Bill 867/ House Bill 1468, entitled: *Cyber Maryland Program – Revisions*.

Senate Bill 867/HB 1468 proposes transferring the Cyber Maryland Program from the Maryland Technology Development Corporation (TEDCO) to the Maryland Department of Labor. In addition, the legislation intends to expand the duties of the Program by supporting and investing in talent improvement strategies. The bill would also require the Cyber Maryland Board to award competitive grants (or contracts) to eligible groups that align with the strategy of the Board and Program – including financial support for cybersecurity education (for K-12) and summer camps.

The National Cryptologic Foundation (NCF) was incorporated in April 1996 as the National Cryptologic Museum Foundation. Over the years, NCF has broadened its purpose to include a robust Education Program and to deliver an innovative approach to solving cybersecurity challenges. NCF's Vision is advancing the nation's interest in cyber and cryptology, through leadership, education, and partnerships.

The mission of the NCF is to educate the public on the importance of cybersecurity in defending our nation with a focus on educating the public, especially the nation's brightest young minds. As a nationally reputed provider of assured quality cyber education resources focused on K-20 cohorts, NCF's efforts help reduce cyber workforce deficits and current skills shortfalls, thereby promoting cyber professions as a fulfilling career choice.

Over the last four years, NCF has proudly worked alongside the Maryland General Assembly, Senate Co-Chair, Joint Committee on Cybersecurity, IT and Biotech, and the Cybersecurity Association to support the successful enactment of cyber legislation three years ago.

The purpose of the Cyber Maryland program aligns with the NCF's educational and workforce goals in Maryland and across the country. It was why NCF proudly supported the legislative passage of

Senate Bill 801, which established the Cyber Maryland Program in 2023. Below are some examples of NCF's education initiatives in cybersecurity that are currently in use across the country:

- 1.) **#CYBERCHATSPodcast** - Expose youth to cybersecurity concepts, opportunities, and careers through conversations with industry professionals and youth in the cyber community.
- 2.) **Cybersecurity Computer Gaming** - In early 2021, NCF, with the help of Anne Arundel Community College student interns, developed two operational computer-based, cybersecurity-themed games with a focus on middle school students:
 - Amanita Whitehat and the Curious Case of the Compromised Computers; and
 - Amanita Whitehat and Mayhem at Mallory Middle

The target audience for the game is K-12 with a focus on middle school. This project had numerous benefits for the intern team, including project management experience and leveraging their cybersecurity, networking, digital forensics, and computer science knowledge.

- 3.) **OUTSMART CYBERTHREATS COLLECTION** - The NCF, in partnership with *Start Engineering*, developed, produced, and promulgated a customized focused booklet on data care and two digital companions, a Teacher's Guide and Student Workbook, aimed to engage data care novices and youth ages 10-18.

- Published and Distributed "*How to be Cyber Safe + Savy*" Booklet – Developed in partnership with Start Engineering and Gula Tech Adventures.

- 4.) **Cybersecurity Curriculum Guidelines (CCG)** - The NCF Cybersecurity Curriculum Guidelines (CCG) were created to encourage curriculum providers, teachers, and industry to create curriculum designed to inspire high school students to pursue a profession in cybersecurity, as well as develop thinkers with a cybersecurity mindset that will enhance any profession they pursue.

Seeing the need for a coherent set of guidelines, a team of K-12 educators, post-secondary educators, and cybersecurity experts, known as *Teach Cyber*, in partnership with the NCF, developed these Guidelines. *Teach Cyber* has also created teaching materials for educators ready to teach high school cybersecurity. The *Teach Cyber* courseware is creative commons licensed, giving educators the right to adopt, adapt, and disseminate the Teach Cyber course.

Curriculum Enhancements: The "Challenge of Cybersecurity" curriculum, consisting of 8 modules, has been updated to support both full-year and modular integration into existing computing courses. Recent updates include revised module overviews, new teaching guides with classroom support, improved lesson formats, updated videos/web links, and revised documents for US Cyber Range labs.

Curriculum Impact: To date, 2,607 educators have registered for the curriculum, leading to over 16,000 downloads. Five modules have been updated, and work is ongoing to revise the remaining three modules.

5.) NCF Ambassador Program - The goal of the NCF Ambassador Program is to educate students on principles of cybersecurity through live instruction by a trained educator/expert who focuses on lessons and exercises in the NCF's "Outsmart Cyberthreats" or OC booklet.

The program is carefully designed to teach students practical things they need to know to keep their personal and important information safe online. Upon successful completion of the (4-6 week) program, they are honored for their achievements and become "ambassadors" in their school and community to encourage fellow students to learn more about being cyber safe.

Through their partnerships, such as the NSA and the University of Maryland Global, NCF is providing national educational programming and resources that are positively addressing the cybersecurity workforce needs across the country and here in Maryland (where the Foundation is based). For those reasons, it's critical for the Cyber Maryland Program to invest in K-12 educational programs such as those developed by NCF and other nationally recognized organizations.

I strongly urge this committee to give SB867/HB1468 a FAVORABLE report. Thank you for your consideration.

Sincerely,



Laura Nelson
President & Chief Executive Officer
National Cryptologic Foundation

CA-2025-SB867-TESTIMONY-FWA.docx.pdf

Uploaded by: John Fiastro

Position: FWA



10440 Little Patuxent Pkwy
Floor 12
Columbia, MD 21044
+443-853-1970
info@cyber-association.com
www.cyber-association.com

SB867 – Cyber Maryland Program - Revisions
Senate Education Energy and Environment Committee
March 6, 2025
Favorable With Amendment

My name is Tasha Cornish, and I am writing on behalf of the Cybersecurity Association, Inc. (CA), a nonprofit 501(c)(6) organization dedicated to strengthening Maryland's cybersecurity industry. Our association represents over 600 businesses ranging from small enterprises to large corporations employing nearly 100,000 Marylanders. We appreciate the opportunity to offer testimony in favorable support of Senate Bill 867, which seeks to revise the Cyber Maryland Program to enhance cybersecurity workforce development and industry support across the state.

Support for the Transfer and Expansion of the Cyber Maryland Program

While we support these critical enhancements, we recognize that expanding the Cyber Maryland Program will require adequate funding and resources to be successful. The bill proposes using unused balances from existing programs to fund these initiatives, but additional state appropriations may be needed to fully implement the program's expanded scope.

To address this, we strongly support the inclusion of Section 3 in SB867, which ensures that any unencumbered funds can be redirected toward initiatives that strengthen Maryland's cybersecurity workforce and industry. This provision establishes a structured approach for reallocating funds that remain unspent by March 30, 2026, ensuring that these resources continue to serve the intended purpose of advancing cybersecurity education, training, and business development in the state. The amendment language in Section 3 provides the necessary framework for this reallocation, as follows:

Ensuring Feasible Implementation

While we support these critical enhancements, we recognize that expanding the Cyber Maryland Program will require adequate funding and resources to be successful. The bill proposes using unused balances from existing programs to fund these initiatives, but additional state appropriations may be needed to fully implement the program's expanded scope.

To address this, we strongly support the inclusion of Section 3 in SB867, which ensures that any unencumbered funds can be redirected toward initiatives that strengthen Maryland's cybersecurity workforce and industry. This provision establishes a structured approach for reallocating funds that remain unspent by March 30, 2026, ensuring that these resources continue to serve the intended purpose of advancing cybersecurity education, training, and business development in the state. The amendment language in Section 3 provides the necessary framework for this reallocation, as follows:

SECTION 3. AND BE IT FURTHER ENACTED, That:

Insert after (B)

(1) Beginning on March 31 of each fiscal year, any funds that have not been encumbered for the specified purposes may be reallocated by the Cyber Maryland Board to any of the following purposes:

(i) Competitive grants and contracts to support cybersecurity workforce initiatives, training programs, and education partnerships;

(ii) Research and development efforts to advance cybersecurity innovation and technology within Maryland;

(iii) Support for small and medium-sized cybersecurity businesses, including funding to enhance workforce recruitment and retention;

(iv) Outreach and engagement programs designed to expand cybersecurity workforce participation, particularly among underserved and underrepresented communities; AND

(v) Any other programmatic purpose within the scope of the Cyber Maryland Program that aligns with the workforce development and industry support goals set forth in this Act.

(2) The Maryland Department of Labor shall submit an annual report to the Governor and, in accordance with § 2-1257 of the State Government Article, the General Assembly detailing any reallocation of funds under this section. The report shall be submitted on or before December 1 of each year and shall include:

(i) The amount reallocated;

(ii) The purposes for which the funds were used; AND

(iii) The expected impact of such reallocation.

(C) This section shall take effect upon the enactment of this Act and shall remain in effect unless otherwise modified by the General Assembly.

Conclusion

SB867 is a strategic step toward strengthening Maryland's cybersecurity workforce and industry competitiveness. The Cybersecurity Association fully supports this legislation and encourages the General Assembly to provide the necessary funding and resources to ensure its success. The inclusion of Section 3 will provide much-needed flexibility to ensure the effective use of allocated funds to further Maryland's cybersecurity workforce and industry development.

We appreciate your leadership and commitment to advancing Maryland's cybersecurity landscape. Thank you for your time and consideration. I am happy to answer any questions the committee may have.

Support

Uploaded by: Mindy Lehman

Position: FWA



**TESTIMONY PRESENTED TO THE SENATE EDUCATION, ENERGY, AND THE
ENVIRONMENT COMMITTEE**

SENATE BILL 867 - CYBER MARYLAND PROGRAM - REVISIONS

**MARCH 6, 2025
SUPPORT WITH AMENDMENTS**

The Maryland Technology Development Corporation (TEDCO) is dedicated to economic growth through the fostering of an inclusive entrepreneurial and innovation ecosystem. TEDCO discovers, invests in, and helps build great Maryland-based technology companies.

As drafted, SB 867 - Cyber Maryland Program - Revisions transfers the Cyber Maryland Program from TEDCO to the Maryland Department of Labor (MD Labor), requires the Program to issue certain competitive grants and contracts beginning in fiscal year 2026; alters the purposes for which the Cyber Maryland Fund may be used; alters certain funding requirements related to the Program; requires that certain unused balances from certain programs and funds be transferred to the Program at the close of the fiscal year, and alters the membership of the Cyber Maryland Board.

SB 867 requires that unused balances from the Cybersecurity Investment Fund, among other programs and funds, be transferred to the Program at the close of the fiscal year. Established in 2014 by Maryland Chapter 534, the Cybersecurity Investment Fund (CIF) is a special, non-lapsing fund in TEDCO to invest in seed stage, Maryland-based cybersecurity startup companies. This investment fund was established by the Maryland General Assembly to function as an evergreen fund. By statute, any investment earnings the fund, are credited to fund, and used to make future investments.

The proposed sweeper provision to CIF, included in SB 867, would have the impact of eliminating the evergreen nature of the CIF fund, by redirecting carry-over balances, including CIF investment earnings that currently are credited to the fund and used to make additional investments.

Since FY2015, CIF has invested in over 50 Maryland cybersecurity companies. During that time, CIF investment earnings enabled TEDCO to fund nine of those companies, at about \$200,000 each.

The CIF consists of:

- (1) appropriations as provided in the State budget;
- (2) money made available to the Fund through federal programs or private contributions;
- (3) repayment of capital or principal or payment of interest on any debt or equity investments from the Fund;
- (4) investment earnings of the Fund; and
- (5) any other money accepted by TEDCO for the Fund.

The CIF fund is governed by Economic Development Section 10-464 (statute). The fund may be used to invest in cybersecurity technology product development companies and for the costs necessary to administer the fund. Currently, it is a non-lapsing fund, that is any remaining unspent money at the end of a fiscal year would remain in the fund and not revert to the State's general fund.

However, SB 867, as currently written, will change the current statute to require that any unspent balance in the CIF, including investment earnings, at the end of the fiscal year be transferred into Cyber Maryland fund.

The FY 2026 proposed budget includes a \$900,000 allocation for the fund, which is relatively small, given the high demand. Given Maryland's robust Cybersecurity ecosystem, there is high demand for funding under the Cybersecurity Investment Fund, and the balance of the fund is generally fully deployed each fiscal year. If funds are left at the end of the fiscal year, the funds will have already been dedicated to reserves for additional investments for qualified companies that are already in the CIF application pipeline.

To ensure the CIF is properly equipped to support and invest in the ecosystem as originally designed, TEDCO respectfully requests an amendment to remove the Cybersecurity Investment Fund in the list of funds that will be required to transfer unused funds to the Cyber Maryland Fund. TEDCO has shared its concerns with the bill sponsor and appreciates the sponsor's support of the amendment.

Chapter 578 of 2023 established the Cyber Maryland Program in TEDCO and tasked the program with creating a cybersecurity talent pipeline, serving as a hub for State workforce development programs in cybersecurity, and generally coordinating cybersecurity, research, and innovation in the State. The Act also created the Cyber Maryland Fund, a special, non-lapsing fund, and the Cyber Maryland Board.

TEDCO is appreciative of the opportunity to manage the program and is proud of the work it has achieved to date under the guidance of the Cyber Maryland Board. Last summer, 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, the Cyber Maryland Board partnered with the Governor's Workforce Development Board within the Maryland Department of Labor to engage over 65 industry leaders, educators, and other state and local stakeholders across the state to coordinate a unified ecosystem wide action plan.

Throughout this process, it became clear that Maryland is the national epicenter for cybersecurity; as a result, there is a global significance to developing Maryland's cybersecurity workforce. The development of a robust workforce pipeline that meets the demands of Maryland's cybersecurity ecosystem requires extensive resources and staff capacity, which can be achieved most efficiently and effectively through strong mission alignment.

Given the strong strategic alignment between the mission of the Cyber Maryland Program and the mission of the Maryland Department of Labor, TEDCO fully supports the transfer of the Cyber Maryland Program, Fund, and Board as proposed in SB 867, and is committed to working collaboratively and strategically with the Maryland Department of Labor to facilitate the proposed program transfer.

TEDCO appreciates the opportunity to provide testimony on SB 867 and urges a favorable with amendments committee report.

SB 0867 Cyber Maryland FWA.docx.pdf

Uploaded by: Secretary Portia Wu

Position: INFO

TO: Senate Education, Energy, and the Environment Committee Members
FROM: Maryland Department of Labor
DATE: March 6th, 2025
Committee: Education, Energy, and the Environment Committee

MD LABOR POSITION: FAVORABLE WITH AMENDMENTS

The Maryland Department of Labor (“MD Labor” or “the Department”) supports many of the provisions in SB 867 and believes that they will make a meaningful and necessary contribution to strengthening the Cyber Maryland Program (“the Program”). However, it is critical that any approach to the implementation of the Program is coordinated with our partners.

MD Labor appreciates Senator Hester’s continued leadership in shaping Maryland’s cybersecurity strategy and guiding the future of the Program, which was originally established through her legislation in 2023 (SB801). Thanks to that legislation, TEDCO/Cyber Maryland and the Governor’s Workforce Development Board collaborated on a [report](#) and are now advancing a statewide strategic plan for cybersecurity workforce development (“the Talent Strategy”).

The Program is now transitioning from an incubation phase to an execution phase, where it will move from strategy to action. Transferring the program to MD Labor at this critical juncture will harness the Department’s expertise and infrastructure to bring the strategy’s ambitious goals to life.

MD Labor has proposed its own legislation this session (SB 241 and HB82) that seeks to move the Program to the Department, and Governor Moore’s budget proposes key investments both via General Funds and the State Reserve Fund Dedicated Purpose Account (titled “Cyber Workforce Grants”) in order to jumpstart the work of the program.

SB 867 transfers the Program from TEDCO to MD Labor and clarifies the Program’s purposes, goals, and Cyber Maryland Fund (“the Fund”) usage. The bill expands eligibility for applicants, facilitates grant awards, ensures adequate staffing to manage the Fund, and establishes an annual reporting requirement to promote transparency and accountability.

MD Labor recognizes the need for a significant investment in the Program to build a cyber workforce that can meet growing demand. **However, in this uncertain**

budget climate, the Department recommends a more flexible approach to funding allocation.

As written, the bill designates specific dollar amounts to eight strategies. While MD Labor appreciates that many of these strategies align with the Talent Strategy recommendations, strict allocation at this level of detail may limit the Program's ability to adapt to industry needs, emerging opportunities, and budget realities. To ensure long-term success, MD Labor suggests enumerating these priorities within a broader, dedicated funding framework, allowing for strategic adjustments while still advancing the Program's core objectives.

Similarly, while MD Labor actively seeks funding to expand resources for businesses and jobseekers, the Department has concerns about a mandate requiring the securement of a specific level of non-state resources. Instead, MD Labor recommends revising the language to emphasize the directive rather than explicitly requiring a doubling of funds.

The bill proposes transferring unspent funds from certain programs and funds to the Program at the end of each fiscal year. This approach creates an inconsistent funding mechanism that may not provide predictable resources for the Program. It also diverts funds from other critical workforce development initiatives and includes programs that are not specific line items in the budget (e.g., Registered Apprenticeships in Cybersecurity). Moreover, since this provision impacts programs beyond MD Labor's scope, it would require input from additional agencies.

Finally, the bill contains language requiring grants and contracts for Information Technology or Operational Technology. MD Labor understands this as an effort to expand cybersecurity workforce development into other relevant technologies, rather than using state funds to procure the technology itself. This could be clarified with language indicating that grants and contracts are meant to support workforce development in cybersecurity-related technologies including informational technology, operational technology, and other emerging technologies.

MD Labor appreciates the opportunity to provide feedback on and amendments to Senate Bill 867 and looks forward to working with stakeholders to strengthen the Program.

For questions, please contact Caroline Bauk, at Caroline.Bauk@maryland.gov.