

Testimony for SB 801 (final)

Good afternoon, Madame Chair, Mr. Vice-Chairman, and members of the Senate Finance Committee.

My name is Bruce Spector and I am the Chairman of the Board of Baltimore Cyber LLC, a Baltimore based business that is dedicated to training cybersecurity professionals. I am also a current member of the board of directors and the legislative committee co - Chairman of the Cybersecurity Association of Maryland.

I would like to start by commending Sen. Hester for sponsoring SB 801. On behalf of CAMI and the cybersecurity industry, we sincerely appreciate your dedication and foresight in recognizing this very important issue.

It seems like every week, the newspaper headlines remind us of the very real threat from criminal enterprises and advanced state threat actors from

ransomware, denial of service attacks, data theft and other attacks against our critical infrastructure.

We are long past the point in time where we can speculate “if” there is a cyberattack impacting the citizens of Maryland, we must now accept this as more of a “when” we are attacked.

Its happened repeatedly in our own state- the Maryland Department of Health, Baltimore City, Baltimore County Schools, Washington County government.

As part of the EARN grant program ,which is a very successful, nationally recognized , State of Maryland workforce development program co-sponsored by Senator Klausmeier and administered by the Maryland Department of Labor , Baltimore Cyber has been doing our part to train cybersecurity professionals to join the front line ranks protecting our state and nation from these costly attacks.

We are also in the process of assisting the Maryland Department of Information Technology with training

and upskilling existing state employees to improve the state's cyber posture.

A number of workforce studies have indicated that there are 23,000 unfilled job openings in the cybersecurity field in Maryland right now.

I can personally attest to the number of open reqs with many of the U. S. defense and Intelligence companies that I personally work with. We are aggressively seeking employees right now. It is particularly important to note that these are not jobs that need to be created, they are in fact jobs that currently need to be filled. Maryland companies engaged in cybersecurity need to hire more people, do more work, and contribute more to the economy but the lack of manpower is holding us back.

Over the past 5 years, as a Maryland Department of Labor EARN Grantee we have trained 1000 unemployed or under employed Marylanders in entry level cyber security positions, and were able to place over 90 percent of these trainees in full time positions in the Maryland cybersecurity ecosystem. It should be noted that not only were these

Marylanders unemployed or underemployed, but they are now earning on average well over \$90,000 per year, plus benefits working in Cybersecurity.

I also want to point out some important statistics about diversity in my testimony. 70% of our trainees are people of color and 50% are women. This not only speaks to our focus, but illustrates demographic issues with diversity as it relates to unemployment in Maryland.

We are committed at Baltimore Cyber to doing our part to diversify this field.

SB 801 recognizes the need to develop an ecosystem in Maryland that will encourage training and coordinate with employers, higher ed, public and private entities like Baltimore Cyber who can get this done.

This legislation creates a very necessary public private partnership to help coordinate with employers and trainers to more efficiently align the training to the current up to the moment, real-time, needs of the employers.

I can assure you if we better align this training to the most current employer requirements, these unfilled jobs will be filled with your constituents. The need to vocationally prepare our workforce in cybersecurity skills is critically important to our economy and more importantly critical to our public safety and must be understood by our political leadership.

Recent policy initiatives from the White House and Department of Defense have recognized that vulnerable critical infrastructure like defense, government, health care, and manufacturing sectors must upgrade their defenses. Technology will be a part of this, but people are the key to a successful implementation.

The human factor is the most important factor in maintaining a strong defense. This will present an opportunity for jobs and for the economy if we meet the training challenge .

Due in large part to our strategic location, we are the home to a large number of national cyber

Security assets and its associated industry assets. This makes Maryland one of the largest cyber ecosystems in the world and by all reasonable accounts the most influential. With the National Security Agency, U.S. Cyber command headquarters and NIST/NICE within our borders most if not all cybersecurity policy is crafted and implemented right here in Maryland.

The state of Maryland benefits heavily from this concentration of jobs and companies, but we should not take our location for granted.

If we cannot provide the workforce to fuel these job needs, the jobs will gravitate to other parts of the country .

It is important to note that other states like Ohio, Florida, Massachusetts, and Georgia are ahead of this in developing and encouraging this talent base so we have some catching up to do.

With that I would respectfully request a favorable report on this legislation and thank you for your

attention today. I would be happy to answer any questions you might have.