TESTIMONY PRESENTED TO THE SENATE FINANCE COMMITTEE

SB 902 ECONOMIC DEVELOPMENT - CYBER WORKFORCE PROGRAM AND FUND - ESTABLISHED

POSITION: SUPPORT

MARCH 16, 2021

Chairwoman Kelley, Vice Chairman Feldman, and members of the Committee, thank you for the opportunity to provide testimony in support of SB 902 pertaining to establishing a Cyber Workforce Program and Fund.

My name is Laura Nelson and am the President and Chief Executive Officer of the National Cryptologic Museum Foundation (NCMF) and I serve as a member of the Maryland Cybersecurity Council on the Workforce Development Sub-committee. Also, I retired from the National Security Agency in 2018 after 37 years of service.

As the bill identifies, over 22 thousand cyber jobs in Maryland are wanting for qualified people to fill them with 500,000+ positions available nationwide. The workforce pool includes those already employed in other career fields, those ready for employment, and our future pool – students all the way down to those entering kindergarten. It is important to support career pathway development that encourages those who seek new employment opportunities the means to transition into cyber while also encouraging students to seek careers in cyber.

The mission of the NCMF is to educate the public on the importance of cryptology and 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, our efforts help reduce cyber workforce deficits and current skills shortfalls, thereby promoting cyber professions as a fulfilling career choice. Leveraging the National Initiative on Cybersecurity Education (NICE) Workforce Framework, Maryland's Department of Commerce teamed with the Cybersecurity Association of Maryland Incorporated (CAMI) and other organizations like the NCMF who are focused on cyber education, can provide the effective and efficient cyber education/training programs for individuals interested in cyber careers.

NCMF provides a head start on providing the cyber education programs at the middle and high school level. This summer a middle school targeted introduction to cybersecurity and "data care" is scheduled for release. For high school students, along with our strategic partner Teach Cyber, we developed a deeper understanding. This understanding can be broken down into eight "Big Ideas" to underpin the training. These include:

- Ethics – Understanding of the broad ethical implications within social, organization, and personal values. This includes a basic understanding of right and wrong in online behaviors.

- Establishing Trust – A key principle for cybersecurity is to establish and maintain trust in both users and computers or other devices.
- Ubiquitous Connectivity – The internet is a network of networks that work seamlessly together. Understanding the basics of networking will help ensure our own security.
- Data Security – Keeping data secure and private is essential for all individuals.
- System Security – An understanding of system security and how hardware and software work together. This includes a basic understanding of hardware or software vulnerabilities.
- Adversarial Thinking – Our adversaries are ever present and will exploit our weaknesses to take advantage of us for myriad reasons. Understanding what might possibly go wrong will help individuals better protect themselves from exploitation.
- Risk – An understanding of the complexity of systems of systems, the presence of adversaries, and the dynamic and distributed nature of computing.
- Implications – Advances and decisions at a local level in computing, connectivity, and big data are driving a global, interconnected phenomenon and have significant cybersecurity implications. Students need to understand important historical events and their cybersecurity implications.

Providing cybersecurity training at the high school level will provide a deeper understanding of the opportunities that an ever-increasing interconnected world provides, but also the accompanying inherent challenges and risk. This depth of training will serve Maryland Public School students well as they transition to college or enter the workforce. These “Big Ideas” can also be used as a baseline to develop a workforce transition plan for adults seeking new opportunities in cyber related fields. Maryland needs a qualified pool of cyber individuals to support a robust cyber economy that fills the over 22 thousand available jobs. A comprehensive Cyber Workforce Program provides the strategic pipeline to satisfy Maryland’s economic goals.

I am in full support of SB 902 as providing for a Cyber Workforce Program and Fund. Creating the educational/training programs to inspire and prepare individuals of all ages for cyber careers is critical to our national security.

To the members of this committee, thank you once again for the opportunity to give testimony here today. I urge a favorable report.