SUPPORT

Laura Nelson
President & Chief Executive Officer of the National Cryptologic Museum Foundation

Testimony in Support of

SB 162 Public Schools – Public Schools – Cyber Safety Guide and Training Course – Development, Implementation, and Reporting

Sponsor: Senator Hester

Education, Health, and Environmental Affairs, 1:00 p.m. January 19, 2022

Chairman Pinsky and Vice Chairman Kagan and members of the Education, Health, and Environmental Affairs Committee, thank you for the opportunity to support SB 162 pertaining to Development of a Cyber Safety Guide and Training Course for Maryland Public Schools.

My name is Laura Nelson and I am the President and Chief Executive Officer of the National Cryptologic Foundation (NCF) 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. 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.

Over the past two years our children have been online more than ever as they have adapted to remote learning. Our public-school systems and families were forced to quickly adapt to a new normal without having the luxury of time to fully plan and ensure that all were operating in a safe environment. Parents and children found themselves working, learning and socializing online. While the Internet can provide a wide range of fun and educational activities, there are also inherent risks that must be understood, especially as kids surpass their parents in tech savviness. Protecting our children's digital identity

Development of a Cyber Safety Guide and Training Course will equip today's students to better understand the interconnected world around us. This can include:

- **What is cybersecurity? We all hear this term used but what does it really mean?**

Taking good care of all online data makes the internet useful, important and necessary in our lives. This involves everyone each acting in various roles as individuals, schools, companies or the government. As we consider taking care of ourselves and our own "healthcare," we ensure that we eat healthy, get exercise and when necessary, seek help from healthcare professionals. In the same way we must take steps to ensure our cyber health through "data care" ensuring that our data is secure, appropriately accessible, and reliably accurate.

- **Why is cybersecurity or "data care" important to students?**

Every time you go online data is transmitted back and forth between an individual and many data gathering entities. Consider the mobile phone and the various uses (talking, texting, video chatting, playing games, streaming content, using apps, spending and accepting money, using online accounts) all the while providing background data such as geolocation or other identification information. These are all connected to us individually. What could possibly go wrong? You might click on a link in an email that you think is safe but turns out to be a phishing that opens a webpage that downloads a virus to your phone. Someone could hack into one of your accounts, running up charges or draining your funds Someone might use credentials of a teacher or principal to create chaos through a false bomb scare that is texted to all students. Children need to understand the benefits and pitfalls of operating in an interconnected environment.

- **Other considerations for a student's online presence?**

  Think before you post - Our online actions can have long lasting effects that need to be considered. In today's era of social media, adults and children post their activities with photos, memes, likes and dislikes. Our children need to understand that once something is posted online, it becomes somewhat permanent. A seemingly harmless post may be viewed by potential employers or college admissions boards unfavorably. Understanding the privacy settings of the applications must be a priority for adults and children.

  Stranger danger - We teach our children to be wary of strangers and the same applies to online behavior. Our children need to understand to spot red flags in any online communication with strangers. Of course, the best response is no response, but they need to understand the dangers and consequences.

  Cyberbullying – Bullying of any type can have severe consequences for our children. Cyberbullying (posting mean comments, spreading rumors, threatening or impersonating someone) can have broad psychological implications. Children need to understand that they can be comfortable talking with a parent or another trusted adult if they are being harassed. Likewise, those who bully must understand the consequences of their actions.

What is needed at the high school level?

A basic course providing an introduction to cybersecurity and "data care" is critical for elementary and middle school students. For high school students a deeper understanding may be required. This understanding can be broken down into eight "Big Ideas" to underpin the training. These include:

1. 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.
2. Establishing Trust – A key principle for cybersecurity is to establish and maintain trust in both users and computers or other devices.
3. Ubiquitous Connectivity – The internet is a network of networks that work seamlessly together. Understanding the basics of networking will help ensure our own security.
4. Data Security – Keeping data secure and private is essential for all individuals.
5. System Security – An understanding of system security and how hardware and software work together. This includes a basic understanding of hardware or software vulnerabilities.
6. 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.
7. Risk – An understanding of the complexity of systems of systems, the presence of adversaries, and the dynamic and distributed nature of computing.
8. 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.

I am in full support of SB162 as providing cybersecurity training from elementary through high school is critical for our children. Our children must be prepared to live in a world of interconnected phones, computers and “things” and have a basic understanding how they can best protect themselves and ensure their privacy and security.

To the members of this committee, thank you once again for the opportunity to give testimony here today.