SUPPORT

Mr. Robert Day
Councilman, City of College Park, Maryland
Member, Maryland Cybersecurity Council

Testimony in Support of

SB 1036
Maryland Emergency Management Agency – Cybersecurity Coordination and Operations Office – Establishment

Primary Sponsor: Senator Katie Fry Hester

Senate Education, Health, and Environmental Affairs Committee
12 March 2020

Chairman Pinsky, Vice Chairwoman Kagan, and Members of the Committee, thank you for the opportunity to testify in favor of SB 1036.

My name is Robert Day, and I am councilmember for the City of College Park, a member of the Maryland Cybersecurity Council, and a Senior Management Officer with a Technology Development Firm, White Rook Technologies. I have been in the Information Technology and Network Security field for over 30 years.

The threat of ransomware attacks has increased over the last few years, with no sign of it slowing down. Since 2016, 48 states and the District of Columbia have had ransomware attacks wreak havoc on Police and Fire departments, phone systems email and many other services. In 2019 the known financial impact on state and local governments, healthcare providers, universities, colleges, and school districts are in excess of $7.5 Billion. Last weekend, the City of Durham, North Carolina suffered a cyberattack which resulted in the City temporarily disabling all network access for Police, the 911 center, and the Fire Department phone services. This has hit close to home with the Baltimore attack costing the city at least $18 million.

Certainly, there are cities and counties across our state that are meeting the growing challenges of security, modernization, innovation, and leading-edge applications, however far too many are living with serious deficiencies; both known and unknown. As a city council member for College Park, I would like to think that we are on the cutting edge and ahead of the curve when it comes to technology and network security… But from working in the field with a diversity of clients both Commercial and Federal, I know how fast things change, and how quickly sophisticated hackers adapt.

As an elected city official we must do our best to make sure to protect all of the valuable citizen information within our networks. A successful attack on our city would erode the public trust, would slow growth in our city, and affect the willingness of many to take a risk and try new endeavors, businesses or investments.

A 2019 University of Maryland, Baltimore County nationwide survey of cybersecurity in U.S. local governments stated that “Serious barriers to their practice of cybersecurity include a lack of cybersecurity preparedness within these governments and funding for it,” and that “Local governments as a whole do a poor job of managing their cybersecurity.” The issues identified included:

- Just over one-third did not know how frequently security incidents occurred, and nearly two-thirds did not know how often their systems were breached.
- Only a minority of local governments reported having a very good or excellent ability to detect, prevent, and recover from events that could adversely affect their systems.
- Fewer than half of the respondents said that they catalogued or counted attacks.

In some cases, governments failed to implement even the most basic of IT best practices. A key statement from this report:

"Our research has shown that most American local governments do a poor job practicing cybersecurity. They must do better. And they can start by establishing a culture of cybersecurity throughout their organizations to best protect citizen information and maintain continuous service delivery."

— Donald F. Norris, PhD, Professor Emeritus, UMBC;
Laura Mateczun, JD, PhD student in Public Policy, UMBC.

The state of Maryland must continue to be proactive in addressing and developing ways to be proactive to combat Cyber-attacks throughout our state. The National Governors Association report," State Cyber Disruption Response Plans" brief warns:

"Significant cyber incidents could… stretch the federal government's ability to respond. In such a situation, states will need plans in place to ensure they are organized and prepared to respond without federal assistance."

Michael Garcia
Senior Policy Analyst Homeland Security and
Public Safety Division National Governors Association Center for Best Practices

Based on my experience working with IT infrastructure and Network and Cyber security, I strongly support SB 1036 because it will boost the help needed to address the growing complexities of applying best practice's, in planning and maintaining a strong Cybersecurity ecosystem throughout cities and local entities in our state. I agree that development of a Cybersecurity Coordination and Operations Office with reach throughout the state to help with assessments and implementation of best practices up and down the security stack will have immense impact.

I believe the objectives of this bill are necessary in developing a strong cybersecurity ecosystem within our state.

To the members of this committee, I thank you for your time and the opportunity to give testimony here today.

I encourage a favorable report of SB 1036. Thank you for your consideration.