Statement by Dr. Richard Forno, Senior Lecturer, UMBC, to the
Joint State Committee on Cybersecurity, Information Technology and Biotechnology
26 June 2019

Senator Hester, Delegate Jackson, members of the Joint Committee, I appreciate the opportunity to join you today on behalf of UMBC to offer some thoughts and recommendations on how to better protect state and local government infrastructures from cyber attacks. Incidents from ransomware and data theft to denial of service and more, remind us that cybersecurity is not just protecting digital bits and bytes in cyberspace. With the increasing use of e-government services across the state and cyber-physical "smart systems" such as smart traffic management, smart grids, and smart utilities, the effects of ransomware or other cyber attacks can be physical and practical as well as digital. With these attacks being employed by both nations and non-state actors with increasing frequency, I commend the members of this committee for your leadership in thinking broadly about cybersecurity issues in Maryland and convening this hearing today.

UMBC is well-known for innovation and inclusive excellence in cybersecurity education, research, entrepreneurship, and workforce development. For example: Together, UMBC and UMCP provide research leadership at the National Cybersecurity Center of Excellence's Federally Funded Research and Development Center under a $5-billion contract administered by MITRE. Our cybersecurity incubator at bwtech@UMBC Research and Technology Park hosts over 50 Maryland startup companies exploring all aspects of cybersecurity. Our International Cybersecurity Center of Excellence, just launched, brings together universities from around the world to examine and address cybersecurity challenges. And, of course, I would be remiss if I didn't mention that the UMBC CyberDawgs were the 2017 National Champions of the Collegiate Cyber-Defense Competition (CCDC) and the defending champions of the Maryland Cyber Challenge. Our graduates are amazing as well -- not only are we the #1 provider of technology talent to the NSA, but our alumni are IT leaders in organizations ranging from Apple and Amazon to Lockheed Martin, Northrop Grumman, T.Rowe Price, and the Johns Hopkins University Applied Physics Lab.

In keeping with the theme of today's hearing, I will offer some simple and cost-effective ideas for the state to consider to meet its current and emerging cybersecurity needs. Cybersecurity is an ongoing process, which means there are always lessons to be learned that allow us to improve ourselves.

Regardless of who the attacker is, where they come from, or where the tools used in the attack originate, the first step is effective preparation. In 2016, research conducted by senior UMBC faculty in collaboration with the International City/County Management Association examined cybersecurity preparedness for municipal, state, and local governments across the country. Their findings were published earlier this year in an article for *Public Administration Review*, a copy of which I am providing the Committee along with my statement today. This work was also referenced by the *New York Times* when discussing the recent cyberattacks on Atlanta.

Two findings from this research are especially relevant to today's hearing. First, nearly three in 10 governments surveyed did not know how frequently their systems were being attacked. Second, our researchers identified several barriers to effective state and local cybersecurity preparedness -- many of which can be summarized as a significant funding shortfall that prevents them from hiring and retaining qualified and knowledgeable cybersecurity staff at competitive salaries. These people, both technical and non-technical, are essential for necessary cybersecurity tasks ranging from policy development and cyber risk analysis to systems administration, deploying security monitoring tools, and conducting proactive patching and vulnerability management.

Clearly, cybersecurity measures - people and technology - require time and money. And since we are in short supply of both, we must be prudent in what, how, and where we assign our limited state resources. Unfortunately, history shows that most cybersecurity problems cannot be addressed through technology alone: it's often a people and staffing problem.

Having been a Chief Security Officer for a major internet infrastructure company, I know it's not practical for any organization to suddenly hire hundreds of new cybersecurity professionals - though we'd sure like to! But as a cost-effective first step, we should consider reinforcing Maryland's government cybersecurity workforce with some of the state's most valuable intellectual commodity – our very talented college and university students and faculty.

Thanks to forward-thinking legislation sponsored by Delegate Sandy Rosenberg and supported by Governor Larry Hogan, the Maryland Technology Internship Program (MTIP) helps Maryland retain top technical talent by increasing the number of paid technical internships offered in the state. MTIP is a neutral state resource administered by UMBC and funded by the State that offers matching funds to technology companies, state, and local agencies to hire technology interns. The program currently is supporting over 200 intern hires from various two- and four-year institutions. But these interns work mainly for commercial companies because many government agencies are not able to fund even *half* of their intern salaries or have the human resource mechanisms in place to manage them -- although the Maryland Department of Information Technology did hire four interns this summer through MTIP.

Because MTIP employer participants must pay half of the intern salary costs which typically range from $15 to $22 per hour, many Maryland government agencies are not well-positioned to compete for this student talent. Perhaps the legislature could work with Governor Hogan to increase funding for this program to make it cost-neutral for government agencies to take advantage of this resource and expand its visibility across the state. Or, perhaps legislation could be amended to provide immediate MTIP funding during a specific state-declared cybersecurity emergency to enable our governments to rapidly gain a 'surge' capability in staffing if desired.

But that's a longer-term process. We have immediate cybersecurity challenges today, and UMBC stands ready to do its part *right now*. As of yesterday, we have 74 students from our computing and cybersecurity programs answering our civic call expressing interest to serve as

paid cybersecurity interns right now to support Maryland government cybersecurity activities … all that's needed is appropriate intern-level funding for their time and the willingness of our state and local governments to reach out to our Career Center with a job description. MTIP, as an already established and neutral state resource for coordinating the recruiting, placement, and oversight of technology interns for Maryland entities, would be a logical coordinator for this initiative. There are talented and qualified students ready, willing, and able to help on cybersecurity matters -- let's put them to work!

Now consider the force-multiplier effect if a similar talent identification effort was implemented by other USM schools and community colleges around the state via an expanded MTIP: 50 students here, 10 there, 30 there, and pretty soon you've assembled some real IT/cybersecurity expertise! It's a win-win for everyone: Interns will gain first-hand operational cybersecurity experience during their educational years and our state/municipal governments will gain qualified, and more importantly, affordable, sustainable cybersecurity staffing support to help address today's needs. Better yet, many of those students may stick around after graduation to become cybersecurity professionals working in - or for - Maryland. Expanding MTIP would be an excellent addition to the work this body has already done by creating scholarships for Maryland students to study cybersecurity under the leadership of Senators Simonaire and Lee.

Last week, Governor Hogan created the position of state Chief Information Security Officer and the Office of Security Management. These are important actions that must lead to meaningful results. Working with the Maryland Cybersecurity Council and the newly-established Maryland Cybersecurity Coordinating Council, in addition to those specified in its executive mandate, some additional operational tasks these offices should consider taking include:

> First: Formally identifying a single point of contact in each agency and municipality responsible for cybersecurity,
>
> Second: Working with agencies and municipalities to ensure their cybersecurity plans, procedures, and technology comply with established industry best practices while respecting their unique contexts and realizing that while there is no one-size-fits-all approach to cybersecurity, oftentimes everyone is connected to everyone else,
>
> Third: Providing cybersecurity awareness training to elected public officials across the state so they understand the urgency of the situation and *why* their informed involvement and leadership on cybersecurity matters is crucial,
>
> Fourth: Encouraging the sharing of information about threats and attacks between Maryland government agencies and offering of mutual assistance during times of crisis,
>
> Fifth: Immediately verifying, validating, and/or developing where necessary appropriate incident handling, disaster recovery, and continuity of operations capabilities at all levels of government, and finally,

Sixth: Implementing measures to assess state and municipal cybersecurity preparedness on a regular basis to maintain an informed citizenry and ensure meaningful accountability on cybersecurity matters is achieved.

Actions like these will demonstrate real and tangible commitments to improving state and municipal cybersecurity and instill confidence in our citizens that Maryland is on-top of our many cybersecurity challenges - especially as we head into a national election year. The legislature should consider supporting such efforts where practicable, to include drawing upon the rich expertise of our various universities and workforce development organizations.

Maryland, UMBC, and the USM exist at the epicenter of global cybersecurity. Maryland has been a leader in cybersecurity. Maryland is a national, and indeed global, leader in cybersecurity. Maryland must continue to lead on cybersecurity through innovative, common-sense, and cost-effective thinking, planning, and action.

I look forward to our discussion today. Thank you.

Witness Bio:
Dr. Richard Forno is a Senior Lecturer in the UMBC Department of Computer Science and Electrical Engineering, where he directs the UMBC Graduate Cybersecurity Program and serves as the Assistant Director of UMBC's Center for Cybersecurity. His twenty-five year career includes helping build a formal cybersecurity program for the United States House of Representatives, serving as the first Chief Security Officer at Network Solutions (then, the global center of the internet Domain Name System), and consulting for the Department of Defense and Fortune 500 companies. He has worked with all levels of management on technical and non-technical projects pertaining to cybersecurity, incident response, information operations, and critical infrastructure protection. Richard is an affiliate of the Stanford Center for Internet and Society (CIS) and from 2005-12 was a Visiting Scientist at the Software Engineering Institute at Carnegie Mellon University, serving as an instructor for the CERT Coordination Center (CERT/CC).

Contact:
Phone: 410-455-3788
E-mail: rforno@umbc.edu

UMBC Center for Cybersecurity
http://cybersecurity.umbc.edu