May 7, 2014

United States Senate
Senate Appropriations Subcommittee on Homeland Security
Cybersecurity Hearing
Testimony: Dr. Jonathan Katz: Director, Maryland Cybersecurity Center
University of Maryland, College Park

Chairman Landrieu, Ranking Member Coats:

Thank you for the invitation, and the opportunity to speak to the subcommittee. It is an honor to be here.

As the committee has previously noted, we are continually faced with numerous cybersecurity threats. These threats are not static---in fact, the sophistication of attacks cybersecurity seems to change on a daily basis. New vulnerabilities are uncovered, different attack vectors are employed to exploit a system or a program, and patches for critical operating systems are deployed on a near-constant basis. As Director of the Maryland Cybersecurity Center (MC2), I am extremely familiar with the rapidity with which cybersecurity threats continue to evolve, and the challenges that these threats present to the federal government, the private sector, and our nation's academic institutions.

Developing an adequately prepared cybersecurity workforce is a daunting challenge. Put simply, demand for talented cybersecurity professionals is far outpacing the supply. A 2013 $(ISC)^2$ Global Information Security Workforce Study claims that 56 percent of companies nationwide report a workforce shortage. Maryland alone had more than 18,000 vacancies for cybersecurity jobs, according to a recent Abell Foundation report. And federal agencies are having difficulty filling cybersecurity roles as well, something highlighted in 2008 and 2010 by the CSIS Commission on Cybersecurity for the 44^{th} Presidency.

The University System of Maryland (USM), which includes 12 campuses, has a number of programs in place to augment the existing pipeline of future cybersecurity professionals. Maryland institutions are playing their part by not only training dedicated cybersecurity professionals, but also educating the general public on good cybersecurity practices and policies.

Below are some key ways in which USM institutions are helping to combat the shortage in our nation's cybersecurity workforce:

- USM institutions offer a broad range of degrees in cybersecurity-related fields, and approximately 4,400 cybersecurity-related degrees (BS, MS, and PhD combined) were awarded in the 2012-2013 academic year.
- Four USM institutions (UMD, UMUC, UMBC, and Bowie State) are NSA and DHS Centers of Academic Excellence in Information Assurance Education.

- UMD College Park, with support from Northrop Grumman, launched the Advanced Cybersecurity Experience for Students (ACES) in 2013. This is the nation's first undergraduate honors program in cybersecurity.
- UMBC's Center for Cybersecurity Training offers numerous courses for skill enhancement and certification opportunities.
- Multiple USM campuses offer MS programs in cybersecurity, cyber policy, and/or digital forensics.

In addition to our current educational offerings, USM institutions also perform outreach to the general public to spark interest in the field and communicate cybersecurity best practices. Examples include:

- Cybersecurity camps for middle-school girls and high-school students at UMCP.
- Summer camps for high-school STEM teachers held at UB as part of the DHS-funded Cybersecurity Education and Training Program.
- "Tech talks" given by undergraduate cybersecurity-club members to the broader undergraduate student body

Educational opportunities cannot be created or refined in isolation. USM has numerous cybersecurity programs that are developed with input from industry and government sources. Sharing information about current workforce knowledge gaps, and how to best address them, is one of the many ways that USM institutions benefit from our sustained and regular interactions with private industry and the federal government. However, as educators, we must not only train students in the problems of today, but must also ensure that they master key fundamentals that will provide the foundation for understanding and remediating cybersecurity threats of tomorrow.

Federal and private support to continue to grow the future cybersecurity workforce is essential to closing the "demand gap" for those professionals. Continued—and perhaps expanded—investment from federal agencies, like the Department of Homeland Security, the National Science Foundation, and the National Security Agency, for example, is critical to sustaining the progress that has already been made.

Again, thank you for the opportunity to appear before the subcommittee. I look forward to answering your questions.