**PRESS RELEASE**

# CyberWatch Launches Phase II of Comprehensive K-12 *SECURE IT* Program to Fill the Cybersecurity Workforce Pipeline

*June 8, 2010 Largo, MD.*---The CyberWatch Center announced today at the 2010 CISSE Conference that it has partnered with the Baltimore County and Howard County School Systems in Maryland to launch Phase II of its K-12 *SECURE IT* Program (Strategies to Encourage Careers in Cybersecurity and Information Technology) to help fill the Cybersecurity workforce pipeline. Educators and security experts alike have identified the growing gap in cyber security workers as a major weakness for the nation. *SECURE IT* is a unique effort that will establish the viability of a comprehensive program covering all K-12 grade bands and multiple stakeholders by pioneering a response for the nation in the state of Maryland.

Additionally, CyberWatch will pilot the nation's first high school Information Assurance (IA) Career track in partnership with Baltimore County and the Maryland State Department of Education.

The K-12 CyberWatch Program is the natural outgrowth of 10 years of work within the STEM community, building collaborative programs between business and education, and creating and piloting a robust curriculum for schools. During Phase I of a National Science Foundation grant, CyberWatch's K-12 division under the direction of **Dr. Davina Pruitt-Mentle** piloted courses targeted to elementary, middle, and high schools, and developed summer programs to immerse students in the IA career field. In this second phase, the various levels will be united, and students will be tracked longitudinally, particularly to identify program success in maintaining interest in STEM disciplines in general, and Cybersecurity fields specifically.

The program is unique in several ways. "First, it includes multiple stakeholders. Students, parents, educators, industry speakers, and faculty, staff and students from our higher education community are all involved. We've also been doing it for some time now and have worked out what kids enjoy and what teachers can do in the informal setting that ties to their content classes and vice versa," said Dr. Pruitt-Mentle. "Content topics were co- developed with CyberWatch IA faculty. It also connects the career awareness with the general cybersecurity awareness effort. Even if some kids choose not to go into the IA field, if they gain a stronger understanding about how to behave ethically, safely and securely online, we still feel we have made a difference."

The educators who are involved with SECURE IT are very involved and supportive of this initiative. Here is what Baltimore County Public School system Superintendent **Dr. Joe A. Hairston** said regarding this new opportunity: "Other nations clamor to emulate

our nation's treasure: our creativity and innovation. This has been our global legacy and strength, and it will continue to move us forward. To succeed in this environment, our students will need a 21st century education. We have sought long-term and powerful collaborations designed to create pathways to careers for students; and explore the ways we can support and advance instructional environments with virtual and real-world learning opportunities." Added **Dr. John Quinn**, Executive Director, STEM for BCPS: "We are delighted by the prospects of preparing more students for the field of Information Assurance and look forward to participating in the SECURE IT program."

Similarly in Howard County, **Dr. Sydney Cousin** Superintendent of Schools had an equally supportive statement to make: "Howard County was extremely fortunate to be involved in the first phase of this project, and we are thrilled to continue our participation. The *SECURE IT* Program offers an excellent STEM opportunity for our students while helping to fulfill a need for our future workforce."

The *SECURE IT* effort will be presenting an in-depth status report at the 9th Annual C3 Conference in October 2010. For more information, see http://www.edtechpolicy.org/C32010/

For more information on the *SECURE IT* program or the K12 Division of CyberWatch, contact Dr. Davina Pruitt-Mentle at dpruitt@edtechpolicy.org To learn more about CyberWatch and to receive multi-media files and reports regarding its accomplishments, visit www.cyberwatchcenter.org or contact Dr. Costis Toregas, CyberWatch Marketing Director at toregas1@gwu.edu .

Details of the Program

CyberWatch's K-12 Division uses a comprehensive model to promote awareness about both proper use of technology and careers in Information Assurance. *SECURE IT* (Strategies to Encourage Careers in Cybersecurity and Information Technology) is considered the earliest and the most complete K-12 Information Assurance (IA) program which includes after school and summer programs, student competitions, lesson plans and training for educators, and resources and materials for parents and guidance counselors.

CyberWatch http://cyberwatchcenter.org. is a National Science Foundation-funded Advanced Technological Education (ATE) Center, whose mission is to improve the quality and the quantity of the Information Assurance workforce. CyberWatch is a consortium of 32 community colleges and 14 universities in 17 states and growing, plus numerous government and industry partners, headquartered at Prince George's Community College in Maryland. "We accomplish our mission through extensive curriculum development and sharing, faculty professional development, student competitions and internships, K-12 programs, and dissemination and outreach to the community" states Dr. Bob Spear, Director of CyberWatch Center.

Much of the Center's efforts over the past years have been in developing a model two year IA curriculum, training faculty, forming articulation agreements between 2 and 4 year institutions, expanding the Mid-Atlantic Cyber Defense Competition and most recently assuming leadership in working with DHS and NSA to establish the CAE2Y award program, Centers of Academic Excellence in IA Education (CAE/IAE) for 2 year institutions and developing the CAE2Y Mentor Program. However, quietly the K12 Division led by Dr. Davina Pruitt-Mentle has developed and tested a robust model that includes elements for multiple stakeholders. *SECURE IT* provides a comprehensive approach to address three overarching goals: 1) increasing general awareness and education about Cybersecurity; 2) addressing the critical shortage of the Cybersecurity workforce pipeline by increasing the number and diversity of students pursuing careers in Cybersecurity; and 3) increasing the research knowledge base about STEM career preparation, specifically careers in Cybersecurity.

Activities include: an Annual C3 Conference (Cyberethics, Cybersafety and Cybersecurity), Careers in IA workshops for career counselors and STEM coordinators, Cool Careers in Cybersecurity Workshop for Girls and the *SECURE IT* curriculum. The curriculum currently includes five modules: Cryptography; Programming; Digital Ethics, Safety and Security; System Vulnerabilities; and Digital Forensics. The five modules include activities that have been developed for grade bands 4-5 (Mindtools), 6-8 (Jr. Cyberwarrior) and 9-12 (Cyberwarrior).

Tied to national math, science and technology standards, students engage in hands-on STEM activities and improve digital literacy skills while learning and applying concepts through gaming, modeling and simulation development. Speakers and field trips are integrated in the curriculum. The central focus is the field of Cybersecurity, but it is supported by the too often neglected topics of citizen awareness of ethics, safety and security.

The *SECURE IT* model design is comprised of seven essential components: after-school and Saturday programs for elementary and middle school students; summer programs for high school students; teacher professional development; training and materials for counselors and STEM coordinators; integrated core curricular modules; resources and activities for parents/guardians, and a new Cybersecurity Olympiad competition.

"Components of the program have been on-going since 2001, well before cybersecurity was in vogue. Last year the first comprehensive program, covering elementary through high school, was piloted in Maryland. Phase II will allow us to test the community saturation model in two counties, both of whom will be impacted

directly for the need for a trained IA workforce due to the BRAC initiative along with the relocation of US Cyber Command at Ft. Meade," said Davina Pruitt-Mentle. "We also have program components running currently in Anne Arundel, Harford, Howard and Prince George's counties in Maryland and have been contacted by other states to partner and get materials out."

The program is unique in several ways. "First, it includes multiple stakeholders. Students, parents, educators, industry speakers, and faculty, staff and students from our higher education community are all involved. We've also been doing it for some time now and have worked out what kids enjoy and what teachers can do in the informal setting that ties to their content classes and vice versa," said Dr. Pruitt-Mentle. "Content topics were co- developed with CyberWatch IA faculty. It also connects the career awareness with the general cybersecurity awareness effort. Even if some kids choose not to go into the IA field, if they gain a stronger understanding about how to behave ethically, safely and securely online, we still feel we have made a difference."

"But most importantly, we are targeting kids not in the pipeline yet. Defense competitions are great but they tap kids who are already starting down that career path. The field of IA is very broad and kids, educators and parents need to know the plethora of choices in this field. Some of the girls might not be thrilled about programming but really enjoy cryptography. Digital Investigation has also peaked interest for students and the instructors."

Other funding is being sought to formalize the tested curriculum and lesson plans for national distribution. Efforts including the Cybersecurity Olympiad Competition will begin in the Fall 2010, while a conference dedicated to C3: Cyberethics, Cybersafety, and CyberSecurity will take place on October 7-8, 2010 on the University of Maryland campus (see http://www.edtechpolicy.org/C32010/ ).