CyberWATCH Interim Report
June 1, 2006

CyberWATCH became a virtual regional center on October 1, 2005 with the grant from the National Science Foundation (NSF). The CyberWATCH Regional Center was established to address:

- The lack of cybersecurity/information assurance (IA) curriculum at many higher education institutions
- The alignment of security curricula from high school through graduate school
- The need for faculty development and expertise in IA
- The shortage of a highly skilled security workforce in the fields of information assurance and digital forensic

In its short, eight month existence, CyberWATCH has made significant inroads in all its goals. CyberWATCH's beginning in the middle of the fall semester has prevented PI's from being sufficiently active due to their established and full teaching schedules. Nonetheless, the accomplishments and achievements in this short time are significant.

CyberWATCH Partners:

Higher Education Institutions:

The initial number of higher education institutional partners in CyberWATCH has expanded from the original 10 to15 institutions to date. Two additional community colleges and three additional universities joined CyberWATCH. These higher education partners are making significant contributions to CyberWATCH and benefiting from its activities and programs. The newly added partners are identified with an asterisk.

COMMUNITY COLLEGES:

Anne Arundel Community College (AACC)
Community College Baltimore County (CCBC)
*****College of Southern Maryland (CSM)
*****Howard Community College (HCC)
Montgomery College (MC)
Northern Virginia Community College (NVCC)
Prince George's Community College (PGCC)

COLLEGES/UNIVERSITIES

*****Bowie State University (BSU)
*****Capitol College (CC)
George Mason University (GMU)
George Washington University (GWU)
Johns Hopkins University (JHU)
Towson University (TU)
University of Maryland College Park (UMCP)
*University of Maryland University College (UMUC)

Of the eight university partners, six are Centers for Academic Excellence in Information Assurance Education (CAEIAE). They are: Capitol College, George Mason University, George Washington University, Johns Hopkins University, Towson University, and University of Maryland University College.

Government Partners and Supporting Agencies/Businesses:

PARTNER:

Metropolitan Washington Council of Governments (MWCOG)

PUBLIC/PRIVATE SUPPORTERS:

APPTIS
Assured Decisions, LLC
Cisco Systems
CompTIA
Computer Sciences Corporation
Defense Intelligence Agency
Department of Homeland Security
GSX
Investment Management Enterprise
Lockheed Martin Corporation
Maryland Association of Community Colleges
Maryland State Department of Education
Nashville State Community College
Prince George's Workforce Services Corporation
Solvern Innovations

CyberWATCH Staff:

Director: Vera Zdravkovich, PGCC
Project Manager: Cynthia Mason Posey, PGCC
Project Coordinator: Diane Webb, PGCC
Co-Directors:

David Hall, MC
Fred Klappenberger, AACC
Margaret Leary, NVCC (replaced Dennis Stewart, NVCC)
Casey O'Brien, CCBC

CyberWATCH Advisory Board:

The 18 member CyberWATCH Advisory Board has been established and held the first meeting on February 23, 2006. The Board is diverse and represents academe, public and private sector. The complete list is attached in the Addendum.

CyberWATCH Goals:

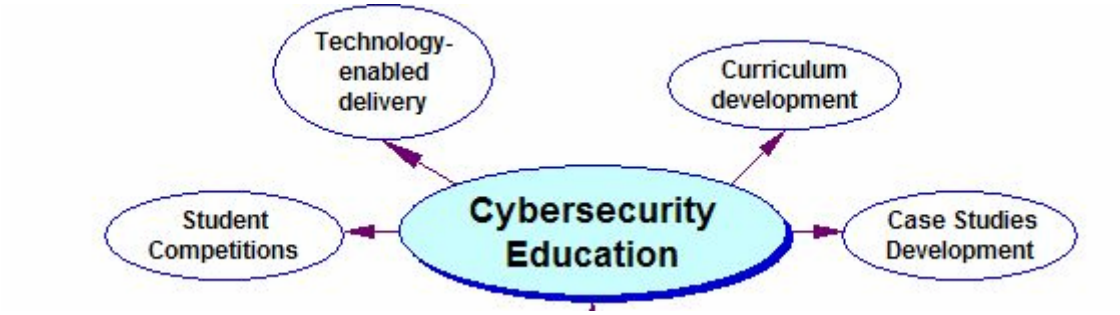
The overarching goal of CyberWATCH is to improve the quantity and quality of the security workforce on all levels, associate degree level, baccalaureate level, and advance degree levels. This is to be accomplished through the following five goals:

I. Cybersecurity Education
II. Professional Development
III. Career Pathways
IV. Dissemination and Sustainability
V. Security Awareness

I. CYBERSECURITY EDUCATION:

This is a multi-faceted goal that includes:

1. Curriculum Development
2. Student Competitions
3. Problem-Based Case Studies
4. Technology-enabled Delivery



1. Curriculum Development

COMMUNITY COLLEGES:

On December 2, 2005, Anne Arundel Community College (AACC) hosted a Curriculum Kick-Off to introduce the partner community colleges to the National Security Agency's (NSA) 4011 Information Assurance (IA) Training Standards. Six community colleges attended this curriculum workshop. An NSA representative, Ms. Lynn Hathaway, reviewed established IA Training Standards with emphasis on NTISSI 4011 and the IA Course Evaluation program that provides for electronically submitted courseware. Ms.Hathaway also helped participants understand the issues involved in aligning the curriculum with the 4011 standards.

AACC shared with the group its approach to performing its own mapping: A nine person AACC team of experts mapped over 50 credit and non-credit courses.
The team held a progress and work meeting every week over a three month period. They produced an information security degree program that received approval from the Maryland Higher Education Commission (MHEC).

Curriculum Kick-Off attendees were given several handouts including the NSA and AACC presentations, a spreadsheet template to assist in mapping their courses to 4011, and links to important NIAET Internet sites. Attendees were asked to look over the materials and their institutions' course offerings to get a sense about what they would have to do to implement an academic program in IA and initiate a mapping to 4011.

During the first two weeks of February, 2006, AACC met with each of the community colleges that attended the December, 2005 meeting. In January, AACC had completed its submission to NSA to renew its 4011 certification and had published on the college's

website detailed course descriptions and outlines and a spreadsheet showing the course mappings to the level of detail in the course outlines. In the February meetings, AACC provided the visited community colleges with hardcopies of the mapping, program layout, and course outlines. During the meetings each community college reviewed its curriculum and facility status and identified its needs as it saw them at that time for support to pursue its own IA program. The meetings dealt with practical aspects of doing the course mappings, entering the data into the database, and manpower estimates.

Another series of meetings was held between AACC and each of the community colleges during April and May. Each of the colleges was at a different stage in the process, and each of them has its own unique administrative, management, and organizational structures that need to be finessed to create an IA program. Several of them lack faculty and/or physical resources to build an IA program quickly. At these meetings the discussions focused on how to accelerate developing their IA programs.

Creating a common CyberWATCH degree program among the community colleges will make it easier to negotiate articulation agreements with four year institutions. Also, a general model will expedite mapping program courses to NTISSI 4011 for everyone.

CyberWATCH community college partners are at different stages in mapping their curricula to NTISSI standards. By 2007 all partners expect to have their courses mapped.

UNIVERSITIES:

The mapping of the curricula at the baccalaureate level is also at different stages. GMU has completed the mapping of the course content to the ACM SIGITE Model Curriculum. GMU also intends to map to the NSA's security-specific in the next academic year. GWU and JHU have completed the mapping of all courses in their programs; UMUC has an undergraduate program offered as either a freestanding certificate or as part of the information systems management baccalaureate degree. UMUC is certified for CNSS 4011, 4012, and 4013 and is currently preparing the documentation for the 4014, 4015, and 4016 certification.

The University of Maryland University College (UMUC), developed a new online Post-doctoral Fellowship in Information Assurance (IA). Faculty members at institutions throughout the world are invited to apply for program. In this program, faculty members will remain on their own campuses while taking the five graduate courses necessary to obtain an IA certificate online. Tuition, books, fees, and a stipend will be paid to program participants. These courses may be taken at the rate of one or two per semester and completion is expected within three to six semesters.

Fellows will have access to courseware using UMUC's proprietary WebTycho online platform and will interface with the Network & Security Laboratory online asynchronously. Successful graduates will be prepared to teach IA in an information technology-oriented program. Upon completion of the program, they will teach a course online for UMUC. The University of Maryland University College is designated a National Center of Academic Excellence in Information Assurance Education by the Departments of Defense (National Security Agency) and Homeland Security.

2. Student Competitions

Mid-Atlantic Regional Collegiate Cyber Defense Competition

The Community College of Baltimore County (CCBC), in conjunction with White Wolf Security and the CyberWATCH Center, hosted the 1st Annual Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC) at the Burle Business Park in Lancaster, PA on March 24-26, 2006.

While similar to other cyber defense competitions in many aspects, the Mid-Atlantic Regional CCDC, as part of the National CCDC (http://utsa.edu/cias/CCDC/), is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. CCDC exercises generally examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester. In contrast, the Mid-Atlantic CCDC focused on the more operational task of assuming administrative and protective duties for an existing "commercial" network.

The competition involved five teams of between four and eight students each, representing four year universities and community colleges from Maryland, Pennsylvania, and Virginia. The participating teams represented:

Anne Arundel Community College (Maryland)
Community College of Baltimore County (Maryland)
George Mason University (Virginia)
Millersville University (Pennsylvania)
Towson University (Maryland)

The teams were co-located in Lancaster, PA. Each team was given physically identical computer configurations at the start of the competition. Their task was to ensure that the systems provided the specified services while under attack from a volunteer Red Team – which continued throughout the competition. In addition, the teams had to deal with and satisfy periodic "injects" that simulate business activities, such as requests for services, IT staff face in the real world.

Scoring was based on the team's ability to detect and respond to outside threats, maintain availability of existing services, such as mail servers and web servers, respond to business requests such as the addition or removal of additional services, and balance security needs against business needs. The final standings were:

1. Millersville University
2. Anne Arundel Community College
3. Community College of Baltimore County
4. George Mason University
5. Towson University

Millersville University represented the Mid-Atlantic Regional in the first-ever national CCDC hosted by the University of Texas at San Antonio on April 21-23, 2006 and sponsored by the Department of Homeland Security (DHS). Millersville took second place at the National CCDC.

3. Problem-Based Case Studies (PBCS)

This goal will be accomplished with the assistance of Nashville State Community College. Multiple workshops are planned around the theme of the development and use of problem-based case studies (PBCS) in security courses, starting with a four hour awareness workshop on September 27, 2006 (location to be determined). The awareness workshop will teach faculty how to use PBCS modules in their courses with a discussion on how to actually create one.

A three-day design and implementation institute will be held in January 2007 (dates and location to be determined) offering faculty teams from CyberWATCH institutions an opportunity to create actual PBCS' for their courses.

4. Technology-enabled Delivery

One of the greatest impediments to high tech training at the college level is the high cost of purchasing and maintaining state-of-the-art equipment. This is especially true in IT security and data forensics as these topics require specialized devices – hardware firewalls, VPN collectors, specialized servers, etc.— which cannot be used effectively in other IT curricula. It just isn't cost effective for an institution to purchase high-end equipment which will sit idle 90% of the time.

To address this issue, CyberWATCH is developing a state-of-the-art IT security lab physically located on the Germantown Campus of Montgomery College and available to all CyberWATCH institutions via the Internet – a Virtual Lab.

Up to this point most institutions have invested in local labs — rooms filled with high tech equipment and computers – in order for students to gain hands-on experience during class hours. High-tech equipment in this type of lab may be mounted on mobile equipment racks or on permanent, immobile racks located in wiring closets adjacent to the actual classrooms. The down side of this is that these rooms must often remain idle due to scheduling considerations. It is also impossible for other institutions to use these lab rooms or share the equipment.
In designing the Virtual Lab, three requirements needed to be addressed:

1. accommodate several types of currently available security curricula
2. adapt to a variety of security classes now and in the future
3. render the lab available for scheduling at any time to all CyberWATCH institutions via Internet access

The structure of the Virtual Lab is a design based on Cisco Networking Academy Fundamentals of Network Security Courseware. This design was chosen because many CyberWATCH participating institutions already have Cisco Networking Academy programs in place. Additionally, the requirements of Cisco's security certification are a recognized standard in the industry. We also have the advantage of working with Erich Spengler of Moraine Valley Community College in the Chicago area where a similar lab has been pioneered.

The CyberWATCH Virtual Lab modifies the standard Cisco security lab by enabling Internet access from remote classrooms. The CyberWATCH Virtual Lab will initially be able to accommodate 12 remote students simultaneously (224 remote students in a typical four-hour class period) and can be available at any time of day.

The lab is designed to handle two routers and firewall-device security. We expect to expand the lab's capability to accommodate a variety of classes. The lab will initially be populated with the equipment needed for router security, switch security, VPN security, and workstation and server security courses. We hope to expand the equipment in the lab to continue to support the security curricula of all CyberWATCH institutions. The newest CyberWATCH partner, Bowie State University, plans to establish a second Virtual Lab working closely with Montgomery College.

II. PROFESSIONAL DEVELOPMENT

1. College Faculty Development

Improving faculty expertise in information assurance and digital forensics through faculty training and professional development is an important CyberWATCH goal, and is directly linked to the quality of the curricula and graduates. A number of training opportunities are available during the late spring and summer 2006.

Information Assurance
May 15 – 19, 2006
Location: Radford University
This class is being offered in a modular format to allow attendees to take certain portions of the class and also to attend other Single-Day tracks being offered at this year's Working Connections. The topics of the course include a detailed look at developing Security Policy, Network Scanning, Intrusion Detection, Computer Forensics, and establishing an Incident Response Team. Each day will feature lecture, hands-on components, and a day-long project exercise that will force attendees to immerse themselves in the topic.

Computer and Network Forensics
May 30 – June 3, 2006
Location: Towson University
The Maryland Alliance for Information Security Assurance (MAISA) is conducting this training with support from NSF and NSA grants. This course is a core component of an Information Assurance curriculum and covers a forensic analysis methodology. The participants will work on a case study in which they will apply sound data collection techniques and perform reliable, repeatable analysis of incidents. The course quite deliberately makes use of free open source tools, though it is tool-independent. It is about understanding of methodology, one in which the chosen tools can and will vary.

Colloquium for Information Systems Security Education Conference
June 5-June 8, 2006
Location: The University of Maryland, University College (UMUC)
The Colloquium provides a forum for academia, government, and industry INFOSEC experts to discuss:

- INFOSEC undergraduate and graduate curricula
- Common requirements
- Specific knowledge, skills, and abilities
- Certification requirements

IT Security Training
August 14 – 19, 2006
Location: Arlington Center of Northern Virginia Community College
CyberWATCH partner Northern Virginia Community College will offer faculty training in August. This training will be offered at beginning, advanced, and expert levels based on a recently completed survey of faculty needs. The survey results indicate that there is a wide range of faculty involvement in the cyber security discipline in terms of area of concentration and level of expertise. Once a base level of knowledge has been established within the consortium, the survey can be utilized as one of the tools for determining future training needs, and possible source of trainers. The complete results of the survey are available as a handout.

2. High School Teachers and Counselors Development

CyberWATCH aims to improve the expertise of high school teachers and general understanding of IT security/IA/digital forensics among the high school teachers and staff. To this end CyberWATCH supports conferences, workshops, and training opportunities for high school teachers and staff.

Cyberethics, Cybersafety & Cybersecurity, (C3) Conference

CyberWATCH provided for the expansion of the Cyberethics, Cybersafety & Cybersecurity, (C3) Conference held October 6-8, 2005, at the Riggs Alumni Center at the University of Maryland College Park (UMCP). The conference served as one of the kick-off events for the yearly "October is Cyber Security Awareness Month national initiative, spearheaded by the National Cyber Security Alliance (NCSA).

CyberWATCH supported the addition of several critically needed workshops focusing on the IT administrator's needs at both the local school system and school building level. While the conference focuses on Cyberethics, Cybersafety and Cybersecurity as related to the educational setting (K-20), NSF funding allowed an additional day and a half to be devoted specifically to Cybersecurity issues for the user services and IT support staff. As security has become a front-and-center concern of IT departments and a common frustration for end-users, the support requirements for help desks and IT support staff have emerged as a critical competency for the central and departmental IT organization. This portion

of the conference provided IT support personnel with an introduction to the common cybersecurity issues that their organizational users face. It also explored strategies and solutions for addressing user concerns and organizational requirements for improving the security of information systems.

Specific 2005 CyberWATCH initiatives included:

Workshop
Microsoft Security Tools and Tips: Running Windows XP Safely workshop
David Norris, Productivity Advisor, Microsoft Public Sector

First Full Day of Cybersecurity related content
Key Note 1: Understanding and Addressing the Current Threats from Internet Access
JEFF GREENSPAN, President of Database & LAN Solutions

Key Note 2: The 5-Step Security Checkup
SPEAKER : BARBARA CHUNG
Senior Technology Specialist, Education Security Advisor
Microsoft Corporation
Protecting Sensitive Information and Keeping Your Identity Your Own

AMY GINTHER
Director, Project NEThics - University of Maryland
Security Practices Educator/Administrator Perspective

Moderator: ROBERT MAXWELL
Lead Incident Response Handler, OIT Security, University of Maryland

KEYNOTE LUNCHEON
Introduction: RON TEIXEIRA, Executive Director, National Cyber Security Alliance

ORSON SWINDLE III
Senior Policy Advisor Center for Information Policy Leadership at Hunton & Williams

Second Day: Selected/Added Cybersecurity breakout sessions
Interactive discussion on Computer Security on Educational Networks
AJAY GUPTA
CISSP, Faculty Computer Science, Director of Security Services
Prince George's Community College

Implementing Effective Cybersecurity
JOHN PORTER and JOSEPH RENARD
Consortium for School Networking (CoSN)

NSF funding paid for registration for 32 attendees (recruited from local school system, private/charter school and area 2-4 year college IT departments). This registration included access to all 3 days of the conference, speakers, a breakout session and workshops on Cybersecurity, a CD of course material, and numerous handouts. With additional monetary support from the National Cyber Security Alliance, and workshop sponsorships from Microsoft, iSAFE, and the Socrates Institute, we were able to deliver a high quality, well received conference that addressed the needs of the educational community. The first day workshops were attended by over 50 people, and the conference as a whole was attended by 147 participants. The conference website can be found at: http://www.edtechoutreach.umd.edu/C32005/index.html

The C3 conference has become one of the annual activities associated with National Cyber Security Awareness month--a congressional initiative led by the National Cyber Security Alliance. Each year the C3 conference will be held the first week in October to help kickoff the monthly awareness campaign. The 2006 conference will be held October 5, 6 & 7.

Summer 2006 High School Teacher Training
During the summer of 2006, high school teachers will receive train-the-trainer training in several Cisco courses. Teachers will represent high schools from Maryland and Washington, DC. Training will be provided by Baltimore County Public schools and Prince George's Community College. As class sizes are limited, two locations will be used to maximize the number of available training seats.

Cisco Instructor Orientation Training
This course offers introductory content to the Cisco Network Academy Program with special emphasis on using The Academy Connection course management application. Teaching methodologies are also covered. Participants must prepare a lesson plan and submit a video taped 30-minute presentation.

June 8th & 9th
Provided by Prince George's Community College

July 17th & 18th
Provided by Baltimore County Public Schools

Cisco CCNA 1: Networking Basics
Network Basics is the first of the four instructor courses. CCNA 1 introduces Cisco instructors to the Cisco Networking Academy Program and to the networking field. The course focuses on network terminology and protocols, local-area networks (LANS), wide-area networks (WANS), Open System Interconnection (OSI) models, cabling, cabling tools, routers, router programming, Ethernet, Internet Protocol (IP) addressing, and network standards.

CCNA 1
June 12th - 20th
Provided by Prince George's Community College

CCNA 1
July 19th – 25th
Provided by Baltimore County Public Schools

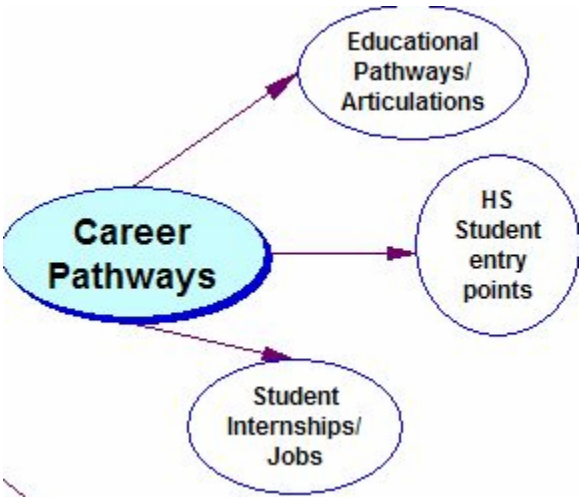
Cisco CCNA 2: Routers and Routing Basics
Routers and Routing Basics is the second of the four instructor courses. CCNA 2 focuses on initial router configuration. Cisco IOS Software management, routing protocol configuration, TCP/IP, and access control lists (ACLs). Instructors will develop skills on how to configure a router, manage Cisco IOS Software, configure routing protocols, and create access lists controlling access to the router.

CCNA 2
July 28th – August 4th
Provided by Baltimore County Public Schools

Cisco CCNA 3: Switching Basics and Intermediate Routing
Switching Basics and Intermediate Routing is the third of the four instructor courses. CCNA 3 focuses on advanced IP addressing techniques Variable Length Subnet Masking (VLSM), intermediate routing protocols (RIP v2, single-area OSPF, EIGRP), command-line interface configuration of switches, Ethernet switching, Virtual LANs (VLANS), Spanning Tree protocol (STP), and VLAN Trunking Protocol (VTP).

CCNA 3
July 19th – 23rd
Provided by Prince George's Community College

III. CAREER PATHWAYS



1. Educational Pathways/Articulations

An essential part of this goal is to establish articulations among the member higher education institutions and build a seamless CyberWATCH pipeline for students. This also implies articulating with high schools to expand the pipeline from high school to graduate school. At this time most community colleges are in the process of curriculum development and mapping of courses. Baccalaureate granting institutions are in a very similar situation. Mapping of courses will assist with curriculum alignment, formal articulations, and seamless pipeline. The completion of this goal will take longer. It is expected that it will be partly accomplished by the end of 2007.
Several articulations have already been completed:

> The articulation agreement between the Virginia Community College System (VCCS) and GMU for the IT major reflects the restructuring of the security content of the degree and takes effect in August for the 2006-7 academic year.
>
> An articulation agreement has been formed between Howard Community College and Johns Hopkins University for a 2-2-2 curriculum in Network Security.

2. High School Entry Points

George Mason University, GMU, became officially a Cisco Regional Academy. GMU will be working with Local Academies over the next few months thus impacting the high school-college pipeline.

The teacher training programs at Prince George's Community College utilize the Cisco CCNA Academy Program, which is an alliance among Cisco, education, business, government, and communities. This program trains high school teachers to prepare their students for higher education in computer science and engineering as well as for networking and IT-related jobs in the public and private sectors.

University of Maryland hosted the first in a series of ***Cool Careers in Cybersecurity Workshops*** which provided information and skills necessary to navigate the professional pipeline in the vast fields of Cybersecurity and Information Assurance as well as other science, technology, engineering, and mathematics (STEM) fields. The first workshop was held Friday April 21, 2006 focusing on ***Cool Careers in Cybersecurity for Girls***. The workshop provided participants with a full day of speakers, hands-on activities and campus site visits. 30 middle school girls had the opportunity to learn from women from companies and agencies throughout the state about what it takes to be a true success in the field. Attention was given to issues for women from underrepresented groups.

Cool Careers in Cybersecurity Workshops sponsored by Educational Technology Outreach within the College of Education draws on research that that indicates recruiting and retaining girls to the science and technology fields should include targeted programs to educate women and minorities about STEM career choices. Many women and minorities have had limited exposure to computing in grade school and high school, especially if they come from lower-income households and communities. A new National Research Council report indicates that general Information and Technology Fluency skills and concepts will also be needed by all citizens if they are to be competitive in the modern world. Curricula should provide early exposure to real-world examples of the content of interest connected to careers. Enrichment programs should emphasize team projects and diverse real-world examples of technology applied in content areas. Curricular material that addresses major societal and/or environmental problems has been shown to attract women to the discipline. Mentoring and role models in the career choices has also shown success in recruitment and retention.

The opening speaker for the ***Cool Careers in Cybersecurity for Girls*** Workshop was Vonda Williams, CISM, CABM, Director, Information Assurance, Solvern Innovations, who applies cutting edge technology solutions and simulations providing objective solutions to critical problems of importance to national security. Her presentations were ***Cool Careers! Information Assurance*** [PPT ... PDF] and ***All Aboard the Cool Security Express*** [PPT ... PDF]. Joan Upole, Executive Officer for a subcommitte of the SIGINT Committee at NSA, then discussed ***Ethics and Computing*** [PPT ... PDF] which showed a variety of both legal and ethical issues one must consider when participating online. Ms. Upole then discussed these issues in the context of what participants want to do, what they think they should do, and what they can be prosecuted for doing. She also discussed some of the ways a person's persona is identified online and how that information can be exploited. After lunch students visited Trufina, a small start up company located in the Technology Advancement Incubator Program on campus that provides a web based application to assure a safer, secure and trustworthy way to identify yourself to others and for others to truthfully identify themselves to you. The girls then toured the GIS lab in the Department of Geography to visit a number of researchers and current research projects.

Girls were recruited through the campus Talent Search Program. Funded by the U.S. Department of Education, Talent Search is designed to provide students with early college awareness and post secondary opportunities. The program targets youth in families in which neither parent graduated from college. Female middle school members of the Educational Talent Search who participated in the Cool Careers for Girls in Cybersecurity Workshop were individuals who have maintained a 3.3 or above, have held

a consistent "B" average in math and science, and have good citizenship as described by their teachers and counselors. Students stay with their middle school "UMCP counselor" for 2 years and then move to a "UMCP high school counselor" for their high school career—many of these students will have the opportunity to participate in additional workshops over the next four years. Rising juniors and seniors may also participate in the Young Scholars Program - Students, Learning, and Technology.

Specific 2006 CyberWATCH initiatives included:

Workshop

- Recruiting 30 middle school girls from Prince George's County school system
- As a result of University of Maryland campus PR (press release and FYI listserve) an additional 8 middle school girls and 2 university students (one undergraduate and 1 graduate student) contacted the PI for approval to attend the workshop.

Detailed Agenda

9:00 AM	COE Computer Lab Benjamin Bldg	Welcome and Logistics Pre-Profile
9:30-10:30 AM	COE Computer Lab Benjamin Bldg	Opening Speaker Vonda Williams, CISM, CABM Director, Information Assurance Solvern Innovations
10:30-Noon	COE Computer Lab Benjamin Bldg	Joan Upole SIGCOM National Security Agency ***Ethics and Computing*** There are a variety of both legal and ethical issues one must consider when participating online. Ms. Upole will discuss these issues in the context of what you want to do, what you think you should do, and what you can be prosecuted for doing. She will also discuss some of the ways your *persona* is identified online and how that information can be exploited.
Noon - 12:45 PM	Stamp Union Food Court	Lunch
1:00 - 1:45 PM	Trufina in the on campus TAP Technology Advancement program Directions	TAP is leading incubator and accelerator which assists early-stage technology companies in achieving their goals. We all know the web is a great place to meet people, job hunt and do business. The only thing we never really know is who's on the other end … until now. Trufina provides a safer, secure and trustworthy way to identify yourself to others and for others to truthfully identify themselves to you.
2:00 – 3:00PM	GEOG and GIS programs Directions to LeFrak Hall	GEOG and GIS programs
3:00 PM	Closure—Bus Back Home	

It is imperative that students are trained in key 21st century skills, including cyberethics, cybersecurity and cybersafety, which will help them play a part in these fields and others, and prepare themselves with the skills necessary to meet the shifting and constantly changing demands of the future workplace. Modeled after the successful UMCP Young Scholars Program, *Students, Learning, and Technology*, UMCP is preparing for the 2006 IA/IT Young Scholars Program. The 3 week program runs from July 10 through July 28. The program will allow seven students explore and expand their knowledge of essential 21st century skills (technology fluency and applications, team building, collaboration tools, problem based critical thinking), while also exposing them to real-life instances of professionals using these skills in exciting IA careers. This program will provide a means to explore current and future IT and IA career opportunities, the variety of choices within these categories, as well as, the multiple pathways to enter the workforce in these areas. Field trips and guest speakers will show how cybersecurity plays out in the modern work environment. Students were recruited through the local school systems guidance and ESOL departments.

The teacher training programs planned for summer 2006 will expand the understanding of teachers of the career opportunities, expectations and appropriate student preparation for the IA field.

3. Student Internships/Jobs

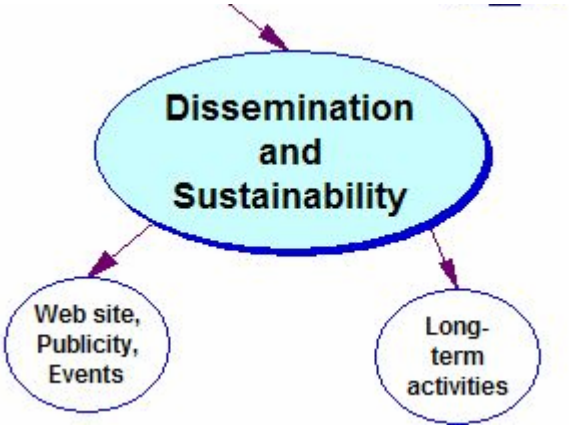
In preparation for student internships, MWCOG organized a business-higher education Forum titled "Building a Cybersecurity and Information Assurance Workforce" held on April 25, 2006 at their premises in Washington, DC. The Forum aimed to improve the understanding of faculty as to the expectations businesses have for the graduates and interns. Questions were raised regarding certain courses such as ethics in the undergraduate curriculum. Businesses present at the Forum offered assistance with internships for students and externships for faculty.

Building a Cybersecurity and Information Assurance Workforce

AGENDA
8:30 – 9:00 Registration & Continental Breakfast
9:00 – 9:10 Welcome
David Robertson, Executive Director, MWCOG
9:10 – 9:30 Overview of CyberWATCH
Vera Zdravkovich, Ph.D., Director, CyberWATCH Center
9:30 – 10:00 The State of Cybersecurity and Information Assurance
A federal intelligence agency expert will provide an overview on current and future cybersecurity threats and trends in information assurance solutions.
John B. Chesson, Special Agent, Cyber Division, FBI
10:00 – 11:00 Panel Presentation: Government and Corporate Cybersecurity Needs and Trends
A panel of government and industry representatives will discuss current and future cybersecurity job trends and qualifications.
Twyla N. Garrett, Ph.D., President and CEO, Investment Management Enterprise

Vonda Williams, Director of Information Assurance, Solvern Innovations
Wanda Gibson, Chief Technology Officer, Fairfax County, Virginia
11:00 –11:10 Break
11:10 –11:50 Roundtable Discussion
Panelists and forum participants will be given an opportunity to begin a dialogue that will assist educators in creating higher education curriculums tailored to meet industry needs and help match qualified graduates to current and future job openings.
Facilitator: Vera Zdravkovich, Ph.D.
11:50 Closing Remarks, Calvin L. Smith, Director, Human Services, Planning and Public Safety, MWCOG

IV. DISSEMINATION AND SUSTAINABILITY



1. Website, Publicity, Events

WEBSITE:

The CyberWATCH website is alive and operational. It is not yet fully populated, but will be completed by the end of June 2006. Homer Sharafi, an IT faculty member from PGCC, is serving as the "CyberWATCH webmaster" and will be responsible for maintenance and upkeep of the website. CyberWATCH members are responsible for providing information to Homer who will be placing it on the website. This website will be publicized on all CyberWATCH publications such as newsletters, brochures, business cards, etc. Partner colleges will have links to the CyberWATCH websites and vice-versa.

PUBLICITY:

CyberWATCH received excellent publicity and coverage in local papers resulting from the January Kick OFF event and other local events. Every event that is planned also has an associated publicity feature. Media is invited to these events to provide coverage.

Two volumes of the CyberWATCH Newsletters have a been published and distributed widely to education, and private and public sector. The Newsletters provide information about CyberWATCH activities, and serve to increase the publicity for the Center. They are routinely given to participants at various events and conferences. CyberWATCH partners are encouraged to "spread the word" by disseminating brochures and newsletters.

EVENTS:

The major event to date has been the January 25 CyberWATCH Kickoff, an event attended by well over 100 guests from education, and public and private sector. Agenda for this event is attached in the Addendum. Additional events planned for

the fall 2006 are: the opening of the Virtual Lab at Montgomery College on September 28, and the opening of the computer classroom at Northern Virginia Community College in November.

2. Long Term Activities:

PARTNERSHIPS AND RELATIONSHIPS

CyberWATCH gained five additional higher education partners, two community colleges and three universities. The synergy built among the partners, and the relationships through curriculum development, faculty development, and articulations will result in long term activities and relationships.

Additional relationships with public and private sector, with agencies such as Department of Homeland Security, National Security Agency, American Association of Community Colleges, Lockheed Martin, Solvern Innovations, and Investment Management Enterprise, will have a long-lasting impact.

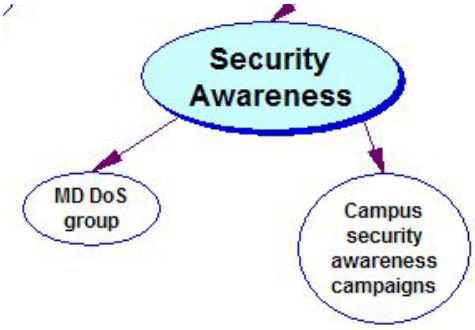
ADVISORY BOARD

The CyberWATCH Advisory Board includes representatives from academe, public, and private sector. The board members will gain knowledge and understanding of CyberWATCH goals and activities and will be advocates for the field and activities after the project completion. The Advisory Board membership list is attached in the Addendum.

CURRICULUM and FACULTY

Curricula and faculty expertise developed under the CyberWATCH auspices represents the intellectual capacity that academic partners will retain long after the completion of the program. Improving the quality of graduates through stronger curricula and better qualified faculty will have a long-lasting impact on the security community.

V. SECURITY AWARENESS



MIDDLE SCHOOLS

The **University of Maryland at College Park** conducted the first of a series of workshops on April 21, 2006aimed at providing middle school girls the information and skills necessary to navigate the fields of Cybersecurity and Information Assurance as well as other science, technology, and mathematics (STEM) fields. The Cool Careers in Cybersecurity Workshop offered 30 participants the opportunity to hear and learn from women in companies and agencies throughout the state about what it takes to be a true success in the field. Attention was given to issues for women from under-represented groups.

In order to increase the security awareness at the middle school level, **George Mason University** exhibited at the Sally Ride Science Fair on May 7, 2006. The exhibit included a live but isolated chat room with custom functionality designed to elicit private information from visitors. A printed copy of the chat room transcript was provided along with a letter to parents explaining the purpose of the exercise and the need for awareness by parents and children. (The chat content was contained within the system and deleted as soon as it was printed.) In the near future, the system will be enhanced and packaged for use by other institutions.