# Interim Report

## April 15, 2007

Submitted by CyberWATCH Staff

# CyberWATCH  Interim Report II
# April 15, 2007

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 one and a half year existence, CyberWATCH has made significant inroads in all its goals. CyberWATCH's initiation in the middle of the fall 06 semester has prevented PI's from initially being sufficiently active due to their established and full teaching schedules. Nonetheless, the accomplishments and achievements in this relatively 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 to17 institutions to date. Four 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)
*Chesapeake Community College (CCC)
Community College Baltimore County (CCBC)
*College of Southern Maryland (CSM)
*Howard Community College (HCC)
*Hagerstown 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 highlighted above). 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
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: Sally Sullivan, 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:

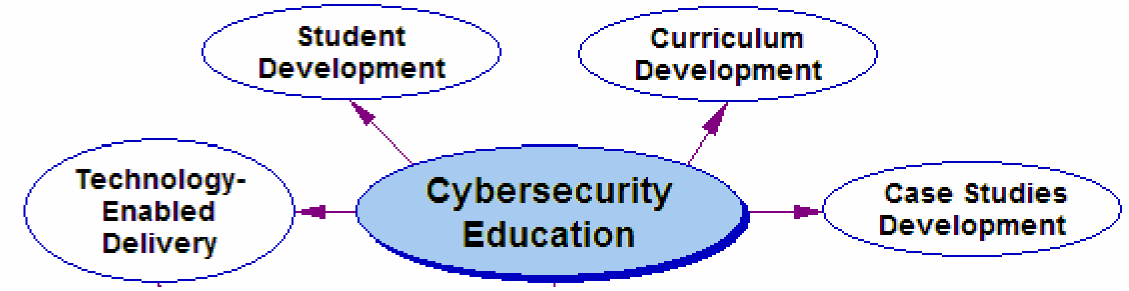
I. Cybersecurity Education
II. Professional Development
III. Career Pathways
IV. Dissemination and Sustainability
V. Security Awareness

Cybersecurity Education
Professional Development
Career Pathways
CyberWATCH Project Goals
Security Awareness
Dissemination and Sustainability

# I. CYBERSECURITY EDUCATION

This is a multi-faceted goal that includes:

1. Curriculum Development
2. Case Studies Development
3. Student Development and Support
4. Technology-enabled Delivery



## 1. Curriculum Development

**COMMUNITY COLLEGES:**

The major curriculum development accomplishment is the establishment of the common CyberWATCH model degree program, CyberWATCH **A.A.S.** Information Security/Information Assurance degree program. All eight participating community colleges have adopted/adapted this curriculum initially developed by Anne Arundel Community College (AACC). The new CyberWATCH **A.S.** degree program is being developed, so that the community colleges will have a choice of two model programs, A.A.S. and/or A.S. degree program.

Howard Community College is currently developing a full set of modularized classroom materials for Anne Arundel Community College's detailed class outlines that are mapped to the NSA 4011 standard. At this time the 165 class materials are complete, and were delivered in January 2007. Classroom materials for the 219 outline are approximately 75% complete, and should be finalized/submitted by end of April. Classroom materials for the 217 outline have been slowed, due to Thomson's delayed release of their new Hardening the Infrastructure textbook. This textbook is now slated for release in June. Delivery of the modularized 217 classroom materials should follow within two months.

Efforts are under way to establish an articulation of these programs with CyberWATCH senior institutions. While there are articulation agreements between individual community colleges and universities, there is currently no agreement that recognizes the CyberWATCH model program.

CyberWATCH community colleges have been working with the CyberWATCH consultant, Liz Harrison, on mapping of their courses.  Considerable progress has been made in this direction.

Specific Curriculum Development and Mapping Status

Anne Arundel Community College (AACC)

- AACC received approval for its Information Systems Security (ISS) degree program from the Maryland Higher Education Commission in the spring of 2005 and offered the program for the first time in fall 2005.
- AACC remapped its courses to 4011 in the fall of 2005 and submitted the mapping NSA on Jan 13, 2006 (AACC had been previously certified three years earlier).
- AACC received recertification of its course mappings to 4011 in the spring of 2006.
- As of spring 2007, approximately 70 students have declared majors in ISS.
- AACC is working on mapping courses to 4013; development of some new courses and modification of some existing courses are anticipated.
- AACC has established curriculum and textbook committee composed of partner institutions.
- AACC is modifying curriculum template for broadening articulation appeal to four year institutions.
- AACC continues to work with other institutions to provide guidance to mapping courses to 4011

Chesapeake College (CC)

- Chesapeake College offers no certificate and/or degree currently, only several IA related courses.

Community College of Baltimore County (CCBC)

- In addition to its current certificate in Information Security, CCBC is working on finalizing a degree in Information Security. Classes for the degree will be offered in the spring of 2008.
- CCBC has received NSA approval for mapping its courseware to the 4011 standard in March, 2007.

College of Southern Maryland (CSM)

- CSM will be submitting its degree program to the Maryland Higher Education Commission for approval.
- CSM is planning to begin offering the program in Fall 07.
- D.J. Singh from CSM will be attending sessions on 4011 mapping in April.

Hagerstown Community College

- Hagerstown  offers no certificate and/or degree currently, only several IA related courses.

Howard Community College (HCC)

- HCC has evaluated their existing curriculum, as well as AACC's 4011 certified curriculum, for their NSA certified degree and certificate programs.
- HCC has decided to map their existing curriculum to the 4011 standard, and supplement it where needed to achieve NSA certification.
- HCC is in the process of mapping their courses to the NSTISSI 4011 requirements, and is approximately 70 percent complete.
- Initial data entry into the NSA database has also been started.
- AACC continues to work with HCC, with NSA application planned for January 2008

Montgomery College (MC)

- MC has laid out a preliminary program template of its proposed courses for its information assurance degree and is preparing to submit the program and new courses to the MC curriculum committee.
- The proposed program will add five new courses to its existing offerings. Two of these courses are based on AACC courses, two are Cisco Academy Security courses, and one has been developed for CyberWATCH in a cooperative effort between MC and PGCC.
- AACC is sharing course details (descriptions and outlines) with MC.
- MC will begin mapping to 4011 after the new courses are developed and accepted by the college's curriculum approval committee.

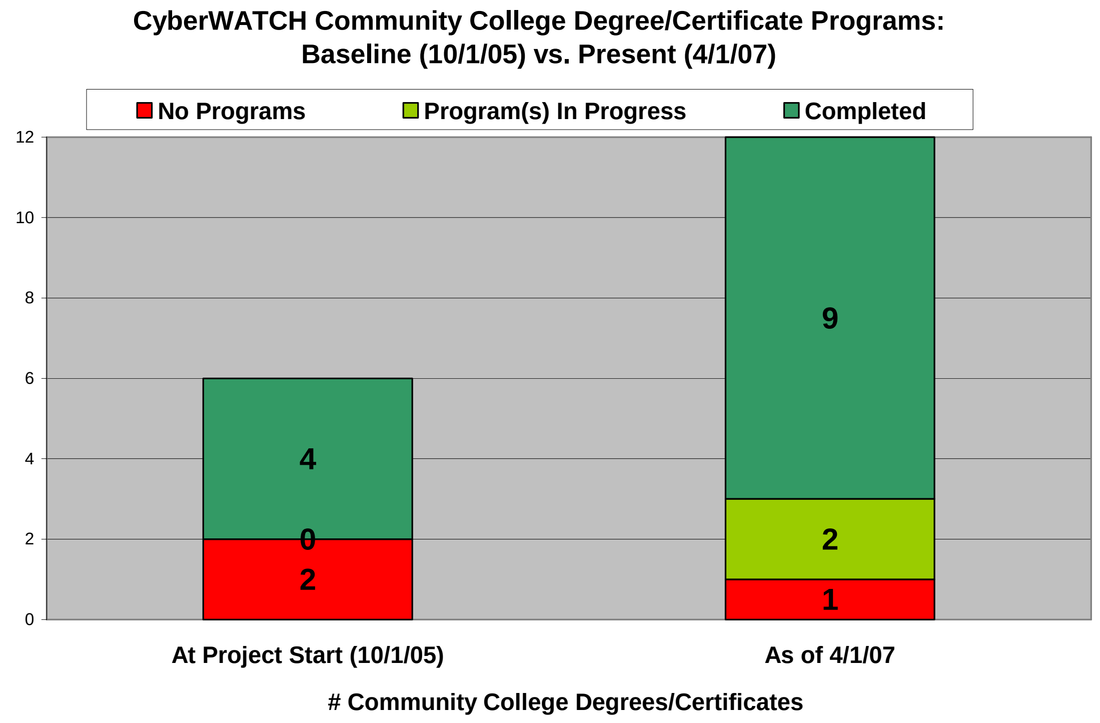
Northern Virginia Community College (NVCC)

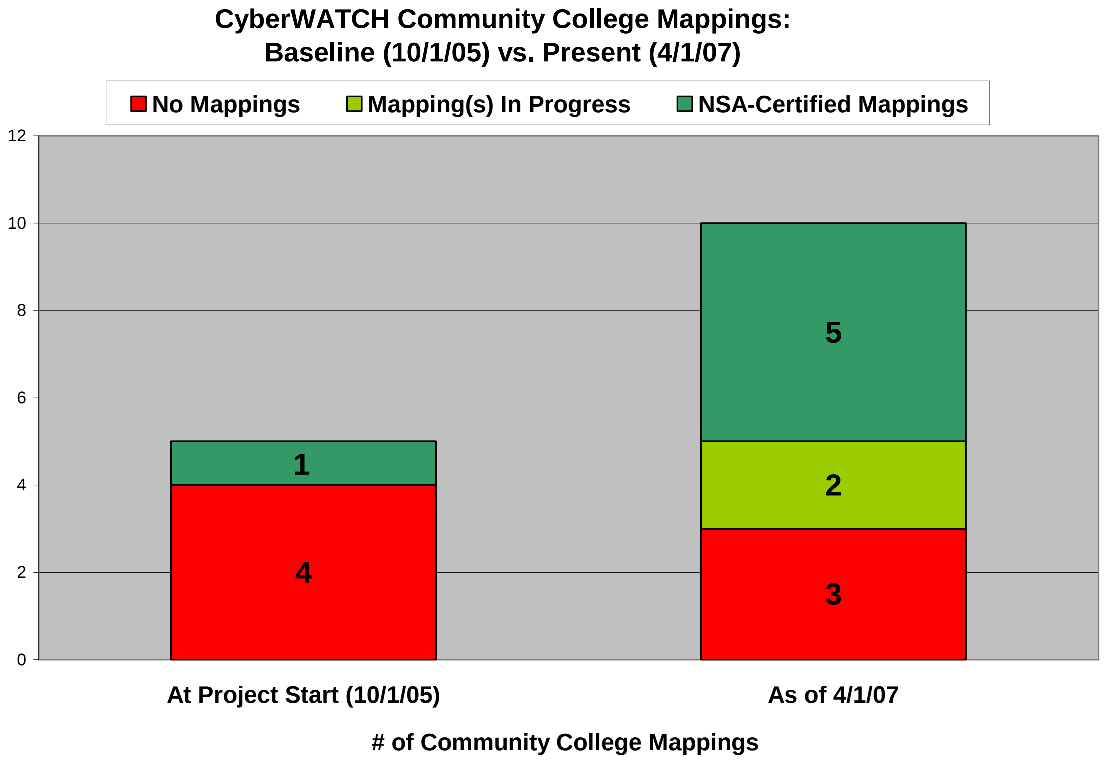
- NVCC successfully mapped to NSA's 4011 standards in March 2007.
- NVCC has updated their web presence to publicize the availability of its program – see www.nvcc.edu/cyberwatch/
- NVCC will be offering a new Network Security Specialization in their IST A.A.S. degree beginning in the Fall 2007 semester.

Prince George's Community College (PGCC)

- PGCC has received approval of its Information Security degree and certificate program from MHEC.
- PGCC completed mapping courses to the 4011 NSA standard in January, 2007. Application has been made to NSA, with approval pending.

The following graphs show the progress of community colleges in the curriculum development and mapping/certification process:





**Note: PGCC's 4011 mapping is pending certification as of 4/1/07.**

**UNIVERSITIES:**

The curriculum development and mapping at the baccalaureate level is also at different stages.

George Mason University (GMU)

A review of the Information Security content of the IT major was completed in 2006. As a result, a number of changes were made to the IT major:

- The required introductory course was modified to focus more on policy and business aspects than technologies.
- The previous course in network security was expanded to a two semester sequence.
- An alternative capstone sequence was developed that focuses specifically on cybersecurity.
- One course was deleted, its content absorbed into revised existing courses.
- A new course in Computer Crime, Forensics, and Auditing was added.
- The content of all security courses was revised to offer an orderly progression from theory (e.g. policy, management principles) to practice (e.g. technologies).
- An initial mapping of the IT curriculum to the ACM sigITe Model Curriculum for IT was completed, which included mapping of the content of the revised security courses.

Over the summer, the articulation agreement with Virginia Community College System institutions (principally NVCC) was updated to reflect changes at GMU and VCCS schools and ensure smooth transition from VCCS schools to the GMU program.

Due to the significant changes in the security curriculum, mapping to NSTISSI 4011 did not begin until 2007. This effort is expected to be completed this summer. Note: Mapping of graduate courses to NSTISSI 4011 was completed in 2005.

As part of the curriculum review, the requirements for an Accelerated BS/MS transition process (which allows students to count 6 credits toward both programs) were streamlined to make the process easier for students.

University of Maryland University College (UMUC)

A new online Post-doctoral Fellowship in Information Assurance (IA) has been created. 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.

UMUC was designated a National Center of Excellence in Information Assurance Education in 2002 and renewed in 2005. Its graduate curriculum is mapped to NSTISSI 4011, 4012, and 4013. The undergraduate curriculum is mapped to NSTISSI 4011. Beginning in Fall, 20007, UMUC will offer an undergraduate degree in Information Assurance, upgraded from a track.

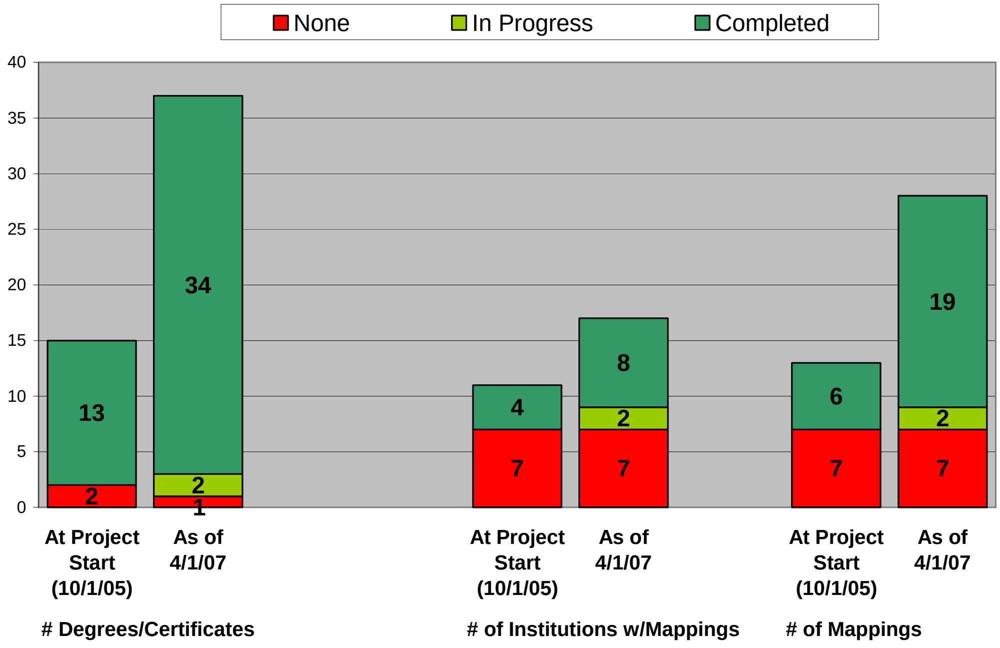
UMUC's IA program currently has a total of 3600 enrollments and has totaled over 12,000 since 2001. The majority of these study online. Online programs are enhanced with remote access laboratories, a gift of the Cisco Corporation.

UMUC offers undergraduate an IA major, minor and certificate, a masters level degree and certificate, and a security track in the doctor of management degree.

Capitol College

The Capitol College (CC) Information Assurance (IA) curriculum maps to the professional competencies found in the six CNSSI/NSTISSI federal standards (4011, 4012, 4013, 4014, 4015, and 4016). Three are mapped at the advanced level (4013A, 4014A and 4016A) as evaluated by the National Security Agency and the CNSS. The CC IA graduate program is delivered online, worldwide, using Centra as the delivery platform. The graph below shows progress in curriculum development and mapping by all CyberWATCH members.

**CyberWATCH Project-Wide Degree/Certificate Programs and Curriculum Mappings: Baseline (10/1/05) vs. Present (4/1/07)**



## 2. Module Development

In addition to the degree and certificate development efforts accomplished by CyberWATCH institutions, a number of course modules were developed and are made available to faculty in higher education.

A total of **14** modules have been developed by Casey O'Brien (CCBC) and Ajay Gupta (PGCC) for use by all participating CyberWATCH faculty. Current modules include:

1. Password Assurance (Windows Operating Systems)
2. Password Assurance (Linux/UNIX Operating Systems)
3. Analyzing Packets
4. Setting Up Access to a Wireless Access Point
5. Successful CISSP Preparation
6. Introduction to Encryption and VPN Technologies
7. Securing and Auditing Network Systems
8. Firewalls and Internet Security
9. Introduction to Intrusion Detection Systems
10. Scanning: A View from a Distance
11. Security Awareness
12. Policies and Procedures
13. Social Engineering
14. Change Management

Other modules the Center plans to develop are:

15. Developing Security Policies
16. Cyberethics
17. E-mail security
18. Web security
19. Operating Systems Security
20. Computer Forensics
21. Other topics not listed here

## 3. Student Development

### Mid-Atlantic Regional Collegiate Cyber Defense Competition, CCDC

CyberWATCH established the new Mid-Atlantic Regional Collegiate Cyber Defense Competition, CCDC.

- 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. The five participating teams were: Anne Arundel Community College (Maryland), Community College of Baltimore County (Maryland), George Mason University (Virginia), Millersville University (Pennsylvania), Towson University (Maryland).

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.

- The **2nd Annual** Mid-Atlantic Regional Collegiate Cyber Defense Competition was held in Hunt Valley, MD on March 9-11, 2007. It was hosted by the CyberWATCH Center, in conjunction with the Community College of Baltimore County (CCBC) and White Wolf Security. The number of participating teams increased from five in 2006 to eight in 2007. The eight participating teams were: Anne Arundel Community College (Maryland), Bowie State University (Maryland), Community College of Baltimore County (Maryland), George Mason University (Virginia), Howard Community College (Maryland), James Madison University (Virginia), Millersville University (Pennsylvania), Towson University (Maryland).

Millersville University won the 2nd Annual CCDC and will again represent the Mid-Atlantic Regional in the second national CCDC to be hosted by the University of Texas at San Antonio on April 13-15, 2007. The Community College of Baltimore County finished second, bettering its third place finish in 2006.

While similar to other cyber defense competitions in many aspects, the Mid-Atlantic Regional CCDC, as part of the National CCDC, is unique in that it focuses on the operational aspect of managing and protecting an existing network infrastructure. While other exercises examine the abilities of a group of students to design, configure, and protect a network over the course of an entire semester, this competition is focused on the more operational task of assuming administrative and protective duties for an existing "commercial" network. Teams are scored based on their 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.

## 4. Technology - Enabled Delivery

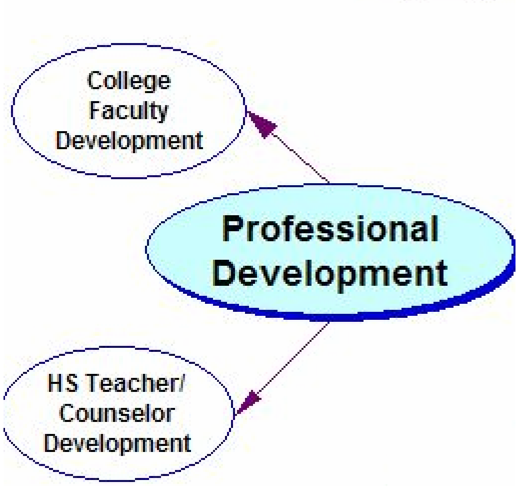
One of the greatest impediments to high tech training at the college level is the high cost of purchasing and maintaining state-of-the-art equipment. This is especially true in IT security and data forensics as these topics require specialized devices – hardware firewalls, VPN collectors, specialized 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 has developed 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. The Lab was launched on September 28, 2006 at Montgomery College in Maryland. Dr. David Hall and his staff have been working closely with Moraine Valley Community College (MVCC) to have the lab ready for use by participating institutions in Spring of 2007. After wading through several layers of configurations, the lab is now being configured for classroom use. The Lab is on schedule to start presenting the "how to" steps for member colleges and institutions. The first introductory session was held on 23 March at MC's Germantown Campus and was aimed at instructing member intuitions on how to configure Virtual Lab access for their faculty and students.

As not all institutions were represented on 23 March, MC will hold these sessions periodically for the next few months. Once representatives from member institutions learn how to access the lab, they will be able to request blocks of time for classroom use. We at MC expect to work closely with member institutions for the next few months (possibly the end of June?) to fully familiarize instructors with the Virtual Lab.

- Supported in part by CyberWATCH funds a new computer lab has been established at NVCC. NVCC will officially launch their **CyberWATCH lab** and program located at its new Arlington Center in Arlington, VA in April, 2007.

# II.  PROFESSIONAL DEVELOPMENT


College Faculty Development
Professional Development
HS Teacher/ Counselor 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 were available during the past year.

**Information Assurance**
The Information Assurance class was offered On May 15–19, 2006 at Radford University 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 included a detailed look at developing Security Policy, Network Scanning, Intrusion Detection, Computer Forensics, and establishing an Incident Response Team.  Each day featured lecture, hands-on components, and a day-long project exercise that forced attendees to immerse themselves in the topic.

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

**Colloquium for Information Systems Security Education Conference**
The Colloquium for Information Systems Security Education Conference held on June 5-June 8, 2006 at the University of Maryland, University College (UMUC), provided 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

**Security + Workshop**
Held on August 14 – 18, 2006 at the Arlington Center of Northern Virginia Community College, the Security + Workshop was attended by 16 CyberWATCH faculty representing 2 and 4-year schools. The CyberWATCH survey results indicated that there is a wide range of faculty involvement in the cyber security discipline in terms of area of concentration and level of expertise. The Security+ workshop participants will sit for the CompTIA Security+ certification exam as well as use materials provided during the workshop in their own courses.

**Problem-based Case Studies (PBCS)**
Orientation Workshop was held at Montgomery College on September 27, 2006. Participants from CyberWATCH member institutions learned how Problem-based Case Studies (PBCS) are structured and how they are currently used in technical education. This was the first of a four-part program. Part two, a 2-day Design and Development Workshop was held February 15-16, 2007 at Anne Arundel Community College. The Design and Development Workshop discussed the critical steps involved in the development of problem-based case studies. Part three, the implementation of the case studies takes place during the Spring 2007 semester. Part four, a Review and Edit Workshop, will be held in May 2007.

**Certified Information System Security Professional (CISSP)**
Twenty one faculty members from CyberWATCH two- and four-year member institutions received $1400 scholarships from CyberWATCH to attend the online CISSP Certification Preparation Program conducted in fall 2006 by Capitol College, a CyberWATCH partner. All CyberWATCH partners will continually receive the reduced rate for this program as well as all other information assurance online programs that are developed by Capitol College.

Two CISSP domains are covered in five contiguous Saturdays. The online program enables faculty to understand current security issues and concepts, practices and trends, and prepares them for the CISSP exam. Almost all of the CISSP instructors are CISSP certified; all are highly specialized IT and IA professionals. The third online CISSP program runs March 17 through April 14, 2007 on the five contiguous Saturdays.

Attendees who successfully complete our CISSP review program and have difficulty with the CISSP examination can do a one-time retake of the five week program free other than the textbook should it change. In addition to the live recording of every class, another unique feature in the program is having students take practice micro examinations to reinforce the learning process on each of the domains as they move through the training program.

Two CISSP domains are covered in five contiguous Saturdays. The online program will enable faculty to understand current security issues and concepts, practices and trends, and prepare them for the CISSP exam. All the CISSP instructors are CISSP qualified and are IT and IA professionals. The third online CISSP program starts March 31 through April 28 on five contiguous Saturdays. Additional certification preparation programs under development which will be available to faculty are: Security +, SSCP, CISA, and CISM. All certification preparation programs are developed and taught in the same manner as the CISSP program.

Attendees who successfully complete the certification preparation programs and have difficulty with the examinations can do a one-time retake of the programs free. Attendees are responsible for the purchase of textbook. In addition to the live recording of every class, another unique feature in the program is having students take practice micro examinations to reinforce the learning process on each of the domains as they move through the training program.

**"Train the Trainer" Program Workshops:**
NVCC offered several one-day workshops:
December 1, 2006 - CyberWATCH Security Foundations Workshop - TCP/IP Foundations, attended by 17 faculty members;
December 8, and 28, 2006 - Introduction to Wireless Administration, attended by 28 faculty members;
December 15th - Introduction to Wireless Security, attended by over 20 faculty members.

**Computer Forensics Workshop**
NVCC is offering the Computer Forensics Workshop to CyberWATCH members on April 20, 2007. This one-day workshop is designed to provide IT faculty interested in instructing Computer Forensic courses with an overview of computer forensics and will include hands-on labs using tools such as Encase to retrieve evidence data off of a hard disk. The workshop will be taught by an active law enforcement professional in the computer forensics field.

**Computer Network Defense**
A week-long workshop was held January 15-19, 2007, at White Wolf Security with 15 faculty members participating. This was a follow-up workshop to the August Introduction to Information Security (Security+) course. This workshop was a series of modules that walk the participants through various computer and network attack tools and their countermeasures. Materials/labs will be provided to the participating faculty to use in their own programs.

**CyberWATCH Faculty Graduate Program –** This program initiated in December 2006 and January 2007 offers an opportunity to CyberWATCH faculty to take IA graduate courses toward a graduate certificate and/or advanced degree with financial support from their home institution and CyberWATCH Center. This program is designed to build a cadre of highly trained professionals in the region. Thirteen faculty members from six different community colleges have been accepted into this program, and most are already taking courses.

## 2. K-12 Program

CyberWATCH Center is committed to generating motivation among the K-12 students, and improving the expertise of K-12 teachers, in addition to improving the general understanding of IT security/IA/digital forensics among the school teachers and staff. To this end CyberWATCH supports conferences, workshops, and training opportunities for high school teachers and staff.

This year's **6th Annual Cyberethics, Cybersafety, & Cybersecurity (C3) Conference: Implications for the Educational Community** will be held October 4 & 5, 2007 at the University of Maryland College Park. Last year's conference was held on October 5-7, 2006. 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.

While the conference focuses on Cyberethics, Cybersafety and Cybersecurity as related to the educational setting (K-20), NSF funding continues to allow additional workshop content and conference sessions 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 continues to provide IT support personnel with an introduction to the common cybersecurity issues that their organization and its users face. It also explored strategies and solutions for addressing user concerns and organizational requirements for improving the security of information systems. CyberWATCH provided participant support in the form of handouts (both printed and CDROMs), and subsistence during the conference. With additional monetary support from the National Cyber Security Alliance, Symantec and CyberSmart, as well as workshop sponsorships from iSAFE, iKeepSAFE 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 60 people, and the conference as a whole was attended by 149 participants. The conference website can be found at: http://www.edtechoutreach.umd.edu/C32006/index.html

Specific **2006 CyberWATCH initiatives** included:

- iSafe and NetSmartZ included section on ethical issues (hacking) and security—virus protection etc.
- iSafe is designed to bring an Internet Safety Program to schools and communities in all 50 states and Department of Defense schools.

- NetSmartz instructs how Internet safety resources can help prevent online victimization and keep your information secure.
- Dr. Radnofsky's workshop spoke to participants about her 2006 article "Corporate and Government Computers Hacked by Juveniles." The Public Manager 35(3), pp. 50-55. (http://www.socratesinstitute.org/research/Hackers.html) and then demonstrated NetEdGE (Internet Educational Game of Ethics) This interactive session gives participants a chance to experience NetEdGE (Internet Educational Game of Ethics), a cyberethics game for tweens and teens to teach middle and high school students the legal, ethical, safe, and secure online practices. This unique game of cyberethics has both online and group interactions, featuring three characters – a juvenile cybercriminal, a victim, and an undercover FBI agent – each of whom must make decisions regarding their cyber activity that could have real-life consequences. Participants play the game from the perspectives of each character, working through different decision points and consequences. The online component was demonstrated following the live action simulations and discussions.
- Don McCabe, Founding Past President of the Center for Academic Integrity and Professor of Organization Management Strategy & Policy at Rutgers University spoke about Cyberethics and its role in today's academic and work environment and the role of ethical courses and content.
- Naomi Lefkovitz of the Division of Privacy and Identity Protection at the Federal Trade Commission spoke about identity theft and how to keep yourself secure.
- Casey O'Brien, Associate Professor and Network Technology Program Coordinator at the Community College of Baltimore County (CCBC) spoke about CyberWatch and an overview of: what information security is; the challenges to information security; the latest trends; best practices to help protect your digital assets; and the need for Information Security professionals.
- Craig Holcomb from the National Security Agency discussed security issues such as Computers and Privacy, and Crime, Abuse, and Hacker ethics.
- Jim Teicher of CybeSmart! spoke about how good safety, security and ethics practices impact every academic subject as teachers embrace the new literacy skills associated with information and communication technology (ICT) – striving to meet standards and raise student achievement.

The second in a series of **Cool Careers in Cybersecurity Workshops** was hosted by the University of Maryland hosted and 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 second workshop was held Friday October 6, 2006.The workshop was run in conjunction with the 5th annual Cyberethics, Cybersafety and Cybersecurity (C3) conference. 30 middle school girls and 20 high school students (N: F=11; M=9) participated in a full day session which included hands-on activities, speakers, and an opportunity to talk with professionals in the field. Students had the opportunity to learn more about Cyberethics, security and safety, as well as, learning first hand from IT/IA experts about career opportunities and pathways in Cybersecurity. Attention was given to issues for women from underrepresented groups.

Two other workshops are being scheduled to take place in Arlington VA in partnership with the Girl Scouts Council of the Nation's Capital (GSCNC). GSCNC serves the entire Greater Washington metropolitan area, including Washington, DC; the Virginia counties of Arlington, Fairfax, Fauquier, Loudoun and Prince William; and the cities of Alexandria, Fairfax and Falls Church. The original date scheduled conflicted with Rosh Hashanah. A second date was chosen but had to be canceled due to inclement weather.

**The Young Scholars Program: Students, Learning and Technology (SLT)** was held at the University of Maryland College Park, July 10-28, 2006.

**The Young Scholars Program Computer Security/Digital Forensics: Students, Learning and Technology (SLT)** will be held at the University of Maryland College Park, July 8-27, 2007. The CyberWATCH grant supports seven students in the course. The course focuses its material around activities that would highlight topics in cybersecurity to illustrate the need to operate in a secure manner and to emphasize the exciting opportunities in this field. Imbedded within the CS/DF SLT course, participants will engage in hands-on activities and learn about installing, configuring, and protecting operating systems; setting up basic and advanced networks; defending against viruses, Trojan Horses, and worms; avoiding SPAM and removing spyware; and applying basic security concepts. Students will also learn about using and configuring firewalls and will discuss such topics as cryptography, system vulnerabilities, and careers in computer security. Tours of the computer security department at UMCP will be conducted, and students will have the opportunity to hear from a variety of speakers from NSA and NIST and visit on campus and local security companies. The highlights include modeling/simulation of virus attacks on computers, construction of an interactive cybersecurity story for youth, and a cybersecurity "game" built in Excel. Recruitment this year is through the Maryland State Department of Education Careers and Technology Division.

**Summer 2006 -2007 High School Teacher Training**

The Cisco Networking Academy Program uses Regional Academies to train and monitor Local Academies. Prince George's Community College and Baltimore County Public Schools performed "train-the-trainer" courses for high school teachers during the summer of 2006 and during the 2006-2007 academic year. Some school systems have their Cisco students complete courses in Information Technology Essentials I and II before they take actual Cisco courses. Depending upon the school system's program, the students may then take the CCNA 1 and 2 courses only, or CCNA 1,2, 3, and 4. Security is an important component of each course in the Cisco program.

**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. Completion of this course is required before an instructor can teach any course through the Cisco Networking Academy Program.

During the summer of 2006, two teachers from PGCPS and one from DCPS successfully completed this course through the Regional Academy at Prince George's Community College.

**Cisco CCNA 1: Networking Basics**
CCNA 1 introduces Cisco instructors to the networking field. The course focuses on network terminology and protocols, local-area networks (LANs), wide-area networks (WANs), the Open System Interconnection (OSI) model, cabling, cabling tools, Ethernet, Internet Protocol (IP) addressing and subnet design, and network standards.
During the summer of 2006, 1 teacher from PGCPS and one teacher from DCPS successfully completed this course through the Regional Academy at Prince George's Community College. An additional twelve teachers from PCCPS are currently taking this course at Prince George's Community College and should complete it by April 2007.

**Cisco CCNA 2: Routers and Routing Basics**
CCNA 2 focuses on initial router configuration. Cisco IOS software management, routing protocol configuration, TCP/IP, and access control lists (ACLs). During the summer and fall of 2006, one teacher from PGCPS and one from DCPS successfully completed this course through the Regional Academy at Prince George's Community College.

**CCNA1 and CCNA 2**
On July 17th and 18th, July 19th – 25th, and July 28th – August 4th the Baltimore County Public Schools provided training to teachers in the following areas: Baltimore County, Washington County, Baltimore City and the Public School System of New Jersey.

**Cisco CCNA 3: Switching Basics and Intermediate Routing**
CCNA 3 focuses on advanced IP addressing techniques such as 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). During spring 2007, one teacher from PGCPS took this course and should finish by April 2007.

**IT Essentials I**
This course maps to CompTIA's A+ certification. During the summer of 2006, five teachers from Prince George's County Public Schools (PGCPS) and one from the District of Columbia Public Schools (DCPS) successfully completed this course through the Regional Academy at Prince George's Community College.

**IT Essentials II**

This course maps to CompTIA's Security+ certification. During the winter of 2006-2007, two teachers from PGCPS successfully completed this course through the Regional Academy at Prince George's Community College.

**WLAN Security**

It has been decided that the CyberWatch WLAN "In-a-Box" project will not be implemented. No WLAN equipment will be purchased. Justification for this decision is based upon the following considerations:

- The CyberWatch WLAN "In-a-Box" project was proposed at a time when wireless LANs were relatively rare and expensive to construct (over three years ago). Since WLAN standards are continually changing (802.11b, 802.11a, 802.11g, and soon 802.11n), the WLAN hardware is constantly transitioning. New WLAN equipment is required to implement each new standard and to implement supported security improvements.
- The participating MD community colleges were surveyed regarding their proposed WLAN programs. It was determined that those colleges that intended to offer a WLAN course had already purchased the equipment needed (both for WLAN and WSEC).
- The problematic logistics of keeping track of who has what which hardware, how does it get from school to school, and who is responsible for: shipping, inventory, performing repairs, and upgrading, etc

**Wireless LAN Security (WSEC) Supplemental Instructional Modules**

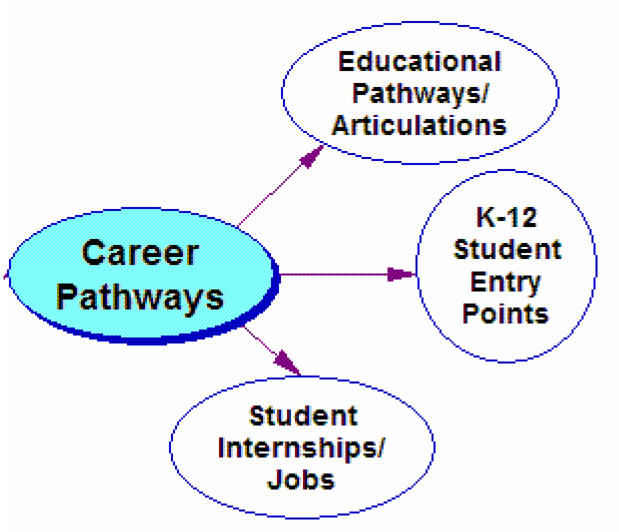
Seven WSEC instructional modules were developed by Engineering Technology faculty at Prince George's Community College to supplement an existing wireless LAN course (WLAN) ENT 219. Full utilization of the WSEC modules assumes knowledge of Ethernet LANs and WLANs. Due to copyright considerations, use of the modules in the classroom requires adoption of the listed textbook. The modules have been additionally integrated into other security courses in the Information Security curriculum at Prince George's Community College: ENT 189, CIS 140, CIS 162, CIS 163, and CIS 166.

The modules are listed below and are available for CyberWATCH consortium members online at:

http://academic.pgcc.edu/ent/WLAN_Sec_Modules/WLAN%20Security%20Modules.html

- **Wireless Security Basics**-- Concise overview of crucial OSI Layer 1 WSEC concerns
- **WSEC Use of Routers**-- Basic router configurations
- **WSEC Module 1** -- WLAN security principles
- WS**EC Module 2** -- WLAN vulnerabilities
- **WSEC Module 3 –** WLAN security (WSEC) basic concepts
- **WSEC Module 4 –** Wireless authentication and encryption
- **WSEC Module** 5 **–** WIDS attack detection, WIPS attack prevention

# III. CAREER PATHWAYS


Career Pathways
Educational Pathways/ Articulations
K-12 Student Entry Points
Student Internships/ Jobs

## 1. Educational Pathways/Articulations

Most CyberWATCH community colleges have individual articulations with different colleges and universities. However, the goal is to establish articulation of the CyberWATCH model A.A.S. Degree Program in Information Security/Information Assurance with the comparable program at partner universities. Mapping of courses will assist with curriculum alignment, formal articulations, and seamless pipeline. As the new A.S. Model is developed, this too will be articulated in the same manner. This broad articulation will eliminate the need for individual institution-to-institution articulations. The model already exists in Maryland in teacher education.

The inter-institutional dialogue to accomplish this goal has been initiated with Capitol College and the University of Maryland University College.

In Virginia, the Virginia Community College System provides a central framework for member institutions to standardize course offerings. This also facilitates articulation with other systems and institutions. The community colleges are a part of the Virginia Higher Education System.

## 2. High School Student Entry Points

George Mason University became a Cisco Regional Academy in Spring 2006 and is actively working with Cisco Local Academies thus impacting the high school-to-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.

## 3. Student Internships/Jobs

The CyberWATCH internship program provides CyberWATCH students with training opportunities and real-world experience in the areas of cybersecurity and information assurance. A variety of summer internship opportunities will be offered beginning in 2007 along with job-readiness skills training. CyberWATCH is partnering with local businesses and IT professionals to give CyberWATCH students a unique opportunity to learn valuable skills and job experience to help explore an industry they hope to move into. Internships may also lead to future employment. CyberWATCH students are matched with local businesses based on their interests, academic experience and skill levels. The Metropolitan Washington Council of Governments (COG) is facilitating the internship program for CyberWATCH. COG is a voluntary association of the area's 21 local governments, working cooperatively to solve mutual problems that are regional in scope and not confined by political or geographic boundaries.

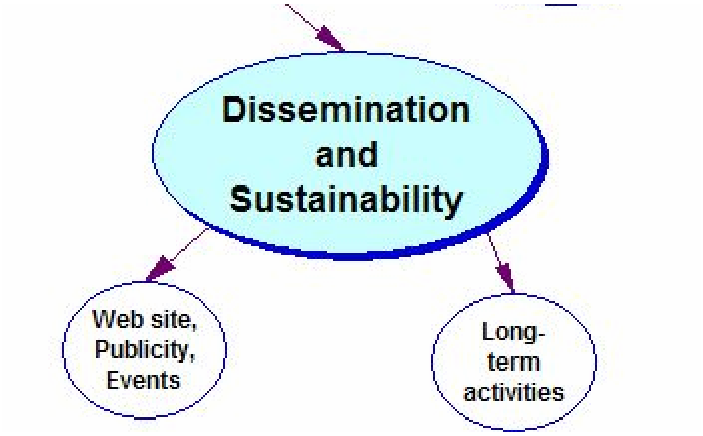
In preparation for the student internship program, COG organized a business and higher education Forum titled “Building a Cybersecurity and Information Assurance Workforce” which was held on April 25, 2006 at their premises in Washington, DC. The Forum aimed to improve the understanding of faculty as 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. Information gleaned from the Forum assisted in developing the CyberWATCH internship model.

The formal launch of the internship program began in Fall, 2006. COG has developed a website (seen at: www.mwcog.org/cyberwatch) which offers information on the program and an online application form to allow students to easily register if they are interested in the program. Internships will typically occur during the summer months of June – August. They will generally run 6 – 10 weeks but could be shorter or longer depending on offerings from CyberWATCH Internship Business Partners. Once a student completes the application process, they are formally approved by CyberWATCH partnership school faculty advisors to verify the student’s participation in the CyberWATCH program. COG then matches student interests and skill levels with the types of internships being offered. Final selection of interns will be based upon interviews with the prospective internship sites.  Business partners will select interviewees based on the strength of the students' qualifications as presented in their application materials.  COG has focused on recruiting business partners from small to medium sized IT consulting firms or other larger firms with small or no internship programs.  Many of the large corporations have internship partnerships already in place with specific institutes of higher learning and larger universities.  Business partner recruitment will continue to allow CyberWATCH to offer the widest range of internship opportunities.

The application period for the Summer 2007 Session began on November 15, 2006 and will run through April 15, 2007.  Interviews by CyberWATCH Internship Business Partners for specific internship placements will take place April – May, 2007.  Final notifications of internship placements will be made by May 30, 2007.  COG expects to place between 10 and 15 students in internships during the first year of the program.

COG has advertised the internship program though flyers distributed to students which advertise the internship website.  COG staff have also made on--site presentations to CyberWATCH students at four partner schools including Northern Virginia Community College - Arlington, Alexandria and Woodbridge campuses; and Ann Arundel Community College.

# IV. DISSEMINATION and SUSTAINABILITY



## 1. Website, Publicity, Events

**WEBSITE:**

A new CyberWATCH Web site is in the process of being designed, and is expected to be operational in April 2007. The CyberWATCH site will:

- provide tools, and present resources for Cybersecurity education (e.g. modules).
- provide information about: student competitions, resources on Problem- Based Case Studies, professional development opportunities, and career pathways and internships/externships.
- facilitate partnership building with other academic institutions, government agencies and the business community.
- provide information on K-12 initiatives.
- provide links to the CyberWATCH virtual labs.
- provide links to quarterly newsletter and press releases.
- Provide evaluation and benchmarking data for the CyberWATCH grant

**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.

- Five of the CyberWATCH Newsletters have 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.

- CyberWATCH Center and its goals were described in the article titled "Securing Cyberspace" in *Corridor Inc.* in its August 2006 issue. *Corridor Inc.* is a political and business newsmagazine that has a broad circulation of 55,000 leaders in Anne Arundel, Howard, Montgomery, and Prince George's Counties in Maryland.

**EVENTS:**

- The first major event CyberWATCH Kickoff took place on January 25, at Prince George's Community College. This event was attended by well over 100 guests from education, and public and private sector.

- Opening of the CyberWATCH Virtual Lab at Montgomery College took place on September 28, 2006.

- Opening of the CyberWATCH computer classroom at Northern Virginia Community College, Arlington Center will take place on April 19, 2007. It is anticipated that 80 – 100 invited guests will be in attendance. On April 20th, the NVC will have an opportunity to interface with faculty trainees while they participate in a Computer Forensics workshop in the newly opened lab.

- CyberWATCH was part of the panel presentation at the invitational Maryland Cyber Security Consensus Symposium held in Baltimore on September 16, 2006. The Symposium was organized by the Maryland Governor's Office of Homeland Security to produce a White Paper "Importance of Partnering for Cyber Preparedness" with input from all stakeholders.

- CyberWATCH Center was a part of the Showcase Session with a poster, handouts, and "give-aways" at the NSF ATE Principal Investigators Conference, October 18-20, 2006. Two CyberWATCH Co-PI's, Dr. Fred Klappenberger and Casey O'Brien moderated a roundtable session titled "Making Articulation Work." Jean Golub, a student from GMU participated in the Student Showcase Session and interacted with conference participants.

- Presentation on CyberWATCH was given to the Maryland Council of Community College Chief Academic Officers on November 10, 2006. The interest was great prompting several CAO's to pursue affiliation with CyberWATCH.

- NVCC Workforce Development and Continuing Education will showcase and promote the CyberWATCH program and its network security courses at a regional workforce training conference in April 2007.

- NVCC provided information on their network security program and CyberWATCH partnership to other community college security educators from around the nation at the Homeland Defense and Security Education Summit, held at George Mason University, Feb 27-28, 2007. The educational summit is sponsored annually by the Naval Postgraduate School, in partnership with academic and a variety of Homeland Security related organizations, attracting military personnel, researchers and faculty from institutions around the county. It is designed to provide academic institutions the opportunity to share highlights of their programs, issues, and challenges. This year was the first time that that the conference was extended to include presentations by two-year colleges.

## 2. Long-term Activities

### PARTNERSHIPS AND RELATIONSHIPS

CyberWATCH gained seven additional higher education partners, four 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

Security Awareness
MD DoS group
Campus security awareness campaigns

MIDDLE SCHOOLS

The **University of Maryland at College Park** conducted the first of a series of workshops on April 21, 2006 aimed 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 security awareness at the middle school level, George Mason University (GMU) developed a **prototype system for high school students,** designed to teach them about the security risks inherent in use of the Web and other Internet applications.  The system presents a typical “chat room”, but with the additional ability of administrators to inject messages from apparently legitimate users to attempt to solicit private information from users.  To protect the privacy of users’ data, the system is isolated from the Internet at all times. The system was demonstrated to the GMU IT faculty and exhibited at the Sally Ride Science Festival in May, 2006.  Approximately 40 girls in the Year 5-8 range actively used the system, showing a wide range of levels of awareness of the security issues.  A summary of chat room content was provided to parents of approximately 20 of the students to encourage dialogue with their daughters about the dangers of online activities and ways to protect young users.  (The chat content was contained within the system and deleted as soon as it was printed.) The prototype system is being revised to make it more robust and easier to operate.  The final version will be shared with CyberWATCH members to promote community awareness of this important issue.