This Interim Report presents CyberWATCH accomplishments and addresses the concerns raised in the National Visiting Committee (NVC) report in April 2007. Italicized blue paragraphs are direct quotes from the NVC Report from April 2007.

CyberWATCH Highlights:

- Eight partner community colleges offer 10 degree programs in information security (a 333% increase from three in 2005)
- Student enrollments in information security in community colleges have grown over 50% since January 2006.
- Five community colleges have been certified as meeting Standard 4011 by the Committee on National Security Standards (CNSS); four more are expected to be certified in Spring 2008/09 (a 500% increase from one in 2005).
- One community college has been certified as meeting Standard 4013 by the CNSS; three more are expected to be certified in 2008/09.
- Nine student teams (Anne Arundel Community College, Community College of Baltimore County, George Mason University, George Washington University, James Madison University, Millersville University, Northern Virginia Community College, Towson University, and the University of Pittsburgh) competed in January in the 3rd Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC) qualifying rounds, the top four teams competed in the 3rd Mid-Atlantic Regional CCDC (Community College of Baltimore County, George Washington University, James Madison University, and Towson University). A total of 55 students and 11 faculty advisors participated in the 3rd Mid-Atlantic Regional CCDC.
- Community College Baltimore County (CCBC) won the 3rd Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC). It is the **first community college** in the country to qualify for the National CCDC.
- A total of 139 students, 20 faculty members, and agency representatives have participated in the Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC) since its inception in 2006.
- Two community colleges and two universities used the CyberWATCH Virtual Lab established at Montgomery College.
- Twenty three faculty members from CyberWATCH institutions received CISSP exam preparation training.
- The CyberWATCH faculty graduate program has resulted in two completed graduate certificates in IA and three others in progress. Three additional faculty are working toward Master's and/or doctoral degrees in IA under this program.
- 265 CyberWATCH faculty members have participated in professional development workshops/institutes/conferences since 2005. The majority of these were sponsored by CyberWATCH.
- CyberWATCH is developing the process for a robust student internship/job placement program.
- Over 200 K-12 students participated since 2005 in CyberWATCH supported activities such as the Young Scholars Program and Cool Careers in Cybersecurity conferences.

CyberWATCH Partners:

The number of higher education institutional partners in CyberWATCH keeps expanding. It increased from the original **10 to19 institutions** in April 2008. The newest additions to CyberWATCH since April 2007 are Harford Community College and Chesapeake College in Maryland and Erie Community College in New York.

Community Colleges
Anne Arundel Community College
Chesapeake College
College of Southern Maryland
Community College of Baltimore County
Erie Community College, NY
Hagerstown Community College
Harford Community College
Howard Community College
Montgomery College
Northern Virginia Community College
Prince George's Community College

Prospective New Partners:
Germanna Community College, VA
Holyoke Community College, MA
Carroll Community College, MD
Warwick Community College, MD

Universities
Bowie State University
Capitol College
George Mason University
George Washington University
Johns Hopkins University
Towson University
University of Maryland College Park
University of Maryland University College

Prospective New Partners:
Louisiana State University, LA
Wilmington University, DE

Public/Private Supporters
Assured Decisions, LLC
Cisco Systems
CompTIA
Computer Associates, Inc.
Computer Sciences Corporation
Cyber Innovation Center
Department of Homeland Security
GSX
Information Assurance Technology Analysis Center
Lockheed Martin Corporation
Maryland Association of Community Colleges
Maryland State Department of Education
Metropolitan Washington Council of Governments
Michael Mumford of the Defense Intelligence Agency
Nashville State Community College
Northrop Grumman
Prince George’s Workforce Services Corporation

CyberWATCH Advisory Board

NVC Concern

The NVC was troubled that only three Advisory Board members were in attendance at the Thursday night dinner meeting. When speaking with this small sample of the committee, they clearly were not able to define their mission, and they did not seem engaged in the Center, except to attend a couple of meetings, annually, and be fed information on the status of the Center. It may be time to re-populate the Advisory Board, and supply them with an explicit charter. (NVC Report, April 2007)

The Advisory Board MOU was crafted, shared with all Advisory Board members and sent to the NVC in September 2007. The Advisory Board was expanded with addition of several new members:

- Linda Miller, Manager, Business Development, Northrop Grumman Information Technology
- Lisa McKelvie, Internal IT Auditor, Prince George's County Public Schools
- David Buie, National Intelligence Officer for Information Operations, NSA
- Rodney Petersen, Government Relations Officer & Security Task Force Coordinator, EDUCAUSE
- Thomas Goodman, Senior Solution Engineer, Computer Associates, Inc.
- Paul Joyal, Vice President, National Strategies, Inc.
- Dr. Alan Harbitter, Chief Technology Officer, NORTEL Government Solutions, VA
- Ido Dubrawksy, Security Advisor, Microsoft Communications Sector North America

CyberWATCH continues to work on strengthening and expanding the current Advisory Board.

- Curt Aubley, Chief Technology Officer, Lockheed Martin Information Technology
- William Gary, Vice President, Workforce Development, Northern Virginia Community College
- Kathleen Happ, Dean School of Business, Computing and Technical Studies, Anne Arundel Community College
- G. Mark Hardy, President, National Security Corporation
- Matt Heller, Vice President, Technology, TIG Global
- Ron Knode, Computer Sciences Corporation
- Carroll McGillin, Cisco Networking Academy
- Timothy Mullen, Executive Officer, 129th Signal Battalion
- Michael Netzer, Academic Dean, Community College of Baltimore County
- Mary Kay Shartle-Galotto, Executive Vice President for Academic and Student Services, Montgomery College
- Greg von Lehmen, Interim Vice Provost and Dean, School of Undergraduate Studies, University of Maryland University College

CyberWATCH Strategic Plan

NVC Concern

One of the Center's main deliverables is to increase the IA workforce in the Washington Metro area. To achieve this goal, the NVC recommends that CyberWATCH now develop a very explicit strategic plan. During the first 18 months of existence CyberWATCH has enhanced the skill/knowledge set of their faculty, built courses/degree programs/certificates that map to government standards, and expanded the supporting infrastructure. It is now time to attend to recruitment, internships, business relationships, and community involvement to build the pipeline of students and to attack the ever-problematic issue of sustainability of this worthy project. The NVC has confidence in the CyberWATCH leadership to devise the strategic plan, supported by your accomplishments from the first 18 months, that will get you to your goal of increasing the IA-trained workforce. (NVC Report, April 2007)

The new CyberWATCH Strategic Plan 2007 – 2009 developed in Summer 2007 has been shared with the NVC members in the Fall 2007. The Strategic Plan addresses the original CyberWATCH goals and is accompanied by a detailed CyberWATCH Year 3 Action Plan. Additionally, the CyberWATCH members spent extensive time discussing the CyberWATCH Year 3 Action Plan. The completion of these plans will address and accomplish the NVC's concern about the impact on the security workforce in the region.

Many of the elements of the Year 3 Action Plan and Strategic Plan have been addressed or are in progress. The Evaluation Report demonstrates the degree to which the activities in the Year 3 Action Plan and Strategic Plan have been completed.

Sustainability has been discussed at Strategic Planning and Consortium Meetings. Consideration is given to incorporating CyberWATCH as a not-for-profit organization.

Curriculum Development

NVC Recommendations

Curriculum: *CyberWATCH, within the next academic year, will have both an A.A.S. degree in IA and an articulation-grounded A.S. degree that can serve as curricular models for schools wanting to invest in IA education. It is recommended that thought and planning be given to these valuable curricular assets and a mechanism developed for making all US schools aware of their existence, for more widespread dissemination.* (NVC Report, April 2007)

Courses: *A recommendation was made to have the PIs discuss the feasibility of adding a measurement of course/module quality/effectiveness (not just quantity) to the evaluation measurements. For example, performance might indicate that CyberWATCH has 14 IA modules in the curriculum, but an effectiveness measure might show that the14 modules have increased enrollment, increased the number of IA/IT major, etc.* (NVC Report, April 2007)

NVC Concern

A concern of the NVC was the approach used when gaps were identified during the mapping process. Specifically, it was reported that gaps were filled through the creation of new courses. While this may be appropriate some of the time, an equally relevant course of action would be to judiciously integrate the missing concepts/content into existing courses. Or, said another way, the gap analysis resulting from certifications or mappings shouldn't drive curriculum. (NVC Report, April 2007)

All components of 4011, except two, are completely mapped to six courses in the CyberWATCH Information Systems Security AAS degree. Those courses are: Introduction to Computers CW 120, Microcomputer Operating Systems CW 130, Network Security Fundamentals CW 160, Information Systems Security CW 215, Networking 4 CW 251, and Windows 2003 Server CW 230. The two components not satisfied by an ISS program course are *E. SYSTEM OPERATING ENVIRONMENT (Awareness Level), (b) Telecommunications systems, Hardware and Software.* (For 4011 mapping certification purposes, these topics are covered in the Data Communications course which is not part of the ISS program). These two topics were integrated into the existing Information Security Capstone course.

The common CyberWATCH model degree program, **A.A.S.** Information Security/Information Assurance degree program established during the first year and half of CyberWATCH, is being adopted and adapted by a number of CyberWATCH community colleges. The three tables below demonstrate the status of curriculum development and mapping to NSA standards by the CyberWATCH member community colleges.

4011 Standings

College	Mapped	Note	Curriculum
Anne Arundel	100%	Accepted 2006	Model
Baltimore County	100%	Accepted 2007	Modified
Chesapeake CC	0%	Pending Curriculum Development	Model
Erie CC	0%	Curriculum Review 2008	Undefined
Hagerstown CC	0%	Summer 2008 Completion	Undefined
Harford CC	0%	Target – Summer 2009	Model
Howard CC	100%	Accepted 02/08	Modified
Montgomery CC	0%	Summer 2008 Completion	Modified
NVCC	100%	Accepted - 2007	Modified
Prince Georges	100%	Accepted 2007	Model
Southern MD	100%	Submission Pending Course Offerings	Model

4013 Standings

College	Mapped	Note	Curriculum
Anne Arundel	100%	Approval April 2008	Model
Baltimore County	0%	2008 Completion	Modified
Chesapeake CC	0%	Pending Curriculum Review	Model
Erie CC	0%	Curriculum Review 2008	Undefined
Hagerstown CC	0%	2009	Undefined
Harford CC	0%	2009	Model
Howard CC	0%	2008 Completion	Modified
Montgomery CC	0%	2009	Modified
NVCC	0%	2008 Completion	Modified
Prince Georges	0%	2008 Completion	Model
Southern MD	0%	2008 Completion	Model

Mapping Schedule

College	2006	2007	2008	2009	2010	2011	2012
Anne Arundel CC	4011 R		4013 C	4011 R			
CCBC		4011 C		4013 C			4011 R
Chesapeake College					4011 C		
Southern MD				4011 C 4013 C			
Eric CC				4011 C			
Hagerstown CC				4011 C 4013 C			
Howard CC			4011 C	4013 C			
Harford CC				4011 C			
Montgomery College				4011 C 4013 C			
Northern VA		4011 C		4013 C			4011 R
Prince Georges CC		4011 C		4013 C			4011 R

Anne Arundel Community College (AACC), a CyberWATCH institution, received national recognition for its Information Assurance A.A.S. program and was awarded the 2007 Innovation of the Year award by the League for Innovation. The award cited the program pathway that begins in high school, segues into the community college and is fully articulated with several 4-year colleges and universities. The award also noted that the program addresses the workforce needs to prepare qualified persons to work in information security within the homeland security industry and that it prepares students to sit for industry certifications including the Computing Technology Industry Association's A+, Network+ and Security+ certifications; Cisco's Certified Network Associate certification; the Security Certified Network Professional certification, the Certified Wireless Network Administrator, and the Certified Computer Examiner credentials.

Anne Arundel has also prepared an A.S. version of the Information Assurance degree. The primary difference between the two programs is that the A.S. version replaces the two technical elective courses in the A.A.S. with general education courses that are required to satisfy the A.S. designation.

During the summer and fall of 2007, the CNSS 4013 Standard (Network Administrator) was mapped to courses offered by the college. AACC received confirmation of the CNSS 4013 Standard certification.

Community College Baltimore County (CCBC) - the A.A.S. degree and updated certificate programs were officially approved in June 2007 by the CCBC curriculum committee. CCBC will be offering the second course in the program, Introduction to Firewalls, in the Spring of 2008. The first class, Introduction to Information Security, remains a requirement in all the IT-related certificate and degree programs throughout CCBC.

College of Southern Maryland (CSM) has developed an A.A.S program in Information Systems Security, which is modeled after the Anne Arundel Community College program. It has received approval from the board and has been sent to MHEC for approval. CSM is starting to offer courses from the program in Fall 2007. CSM has already started mapping efforts to map the A.A.S curriculum in Information Systems Security to the CNSS 4011 Standard with the help of Elizabeth Harrison, CyberWATCH consultant. This process is expected to be completed by Spring 2008.

Erie Community College (ECC) located in Buffalo, NY will be graduating its first five graduates of the Information Systems Security Certificate Program this May. ECC also developed a new course in Digital Forensics, which is offered as an elective in the ISS Certificate. Also, ECC has been in contact with Elizabeth Harrison, CyberWATCH consultant, regarding the mapping to the CNSS 4011 Standard for the ISS Certificate.

Harford Community College developed the Information Systems Security A.A.S. degree during the 2007 academic year. Harford adopted the CyberWATCH A.A.S. model degree program. Additional curriculum development for the program was completed during the fall 2007 semester. The first two (2) Cisco courses were offered in fall 2007 with a combination of credit and non-credit students. For the spring 2008 semester, all four (4) Cisco courses were offered and an enrollment of nine (9) credit and non-credit students. Initial discussions have been held with Towson University regarding an articulation agreement with Harford and Towson. Harford has also identified faculty to work on the curriculum mapping with NSA standards in conjunction with other CyberWATCH partners.

Hagerstown Community College has revamped the Information Systems Technology Networking Degree to reflect the CyberWATCH initiatives. This new curriculum has been approved by the Colleges' Curriculum Committee and will appear in the 2008-09 Catalog. This new curriculum will offer the students two options in networking education: Option 1-Network Administrator, Option 2-Network Security. Option 2 will carry a message reading: Option 2, Network Security, mapping is pending to NSTISSI-4011, National Training Standard for Information Systems Security (INFOSEC) Professionals. The new Networking Degree option will offer students education that encompasses information assurance principles. On November 29, 2007 Steve Shank and Margaret Spivey met with Elizabeth Harrison to begin the process of mapping its curriculum to the CNSS 4011 Standard. This mapping process will continue during the summer 2008 semester.

Howard Community College (HCC) updated its1st year lecture and lab materials in Spring and Summer 2006 and the 2nd year lecture and lab materials in Summer 2007. HCC shared Anne Arundel Community College's lessons learned from their first curriculum mapping to the CNSS 4011 Standard. As a result, the five core Information Assurance courses in the AAS and Certificate programs were mapped to the CNSS 4011 Standard. In order to contextually tie each class lecture to a real world Information Assurance example, HCC developed and deployed a comprehensive hands-on lab with targeted lab exercises. HCC has officially been NSTISSI 4011 Certified February 2008 for the five core classes.

Montgomery College (MC) - The new A.A.S. in Information Systems Security and a Certificate in Information Systems Security was approved by the MC Curriculum Committee in Fall 2007. It has now been approved by the MC Board of Trustees and is currently awaiting MHEC approval. It will officially begin in Summer 2008. Due to changes in the requirements for the CNSS 4011 Standard, MC was advised to postpone the mapping of its curriculum to those standards until summer 2008. The Cisco courses in the curriculum have been available at MC since 1999. However, MC has begun offering its new CyberWATCH curriculum courses.

Northern Virginia Community College (NVCC) is the only two-year college in Virginia and one of only 5 institutions of higher education in Virginia to have mapped to the CNSS 4011 Standard. NVCC has developed an A.A.S. degree program in Network Security that was first offered Fall 07. The degree recently articulated with Capella University's (an NSA CAE) 4-year Network Security degree program. Working with Tidewater CC and Germanna CC, NVCC developed two Computer Forensics courses that have been sent to the Virginia Community College System (VCCS) for approval and inclusion in the Master Course File, making them available to all Virginia community colleges. Once added, the courses will form the basis of a Career Studies Certificate in Computer Forensics that fits into the modular IST degree. All three of these Virginia community colleges are presently offering computer forensics courses in their curriculum.

Prince George's Community College (PGCC) – In addition to the A.A.S. degree that was approved in 2006, two certificate programs were established in 2007. They are awaiting MHEC approval. The certificates are non-overlapping certificates in Information Security and Cisco CCNA Preparation. All courses in the certificates count toward the A.A.S. degree. In June, 2007, PGCC received approval for its course mapping to 4011. Preparations are underway for mapping to the 4013 in the fall of 2008. Revisions to our capstone course in Information Security, along with a CISSP prep course are planned; one of the effects of this is that groundwork will be laid for 4013 mapping. Since our A.A.S. degree is based on the CyberWATCH model curriculum developed by AACC, we will be able to quickly adopt their A.S. degree, which is currently under development.

The model A.A.S. IA program has been articulated with University of Maryland University College, (UMUC), Capitol College, Towson University (TSU), and University of Baltimore (UB). While there are articulation agreements between individual community colleges and universities, they follow the same matrix and MOU established by Anne Arundel Community College and partner universities. The matrix below demonstrates how the CyberWATCH courses (those with **CW** designation) relate to the courses offered by individual institutions.

Cross Reference of courses offered at each institution mapped to CyberWATCH course identifications:

CyberWATCH ID	Course Title	AACC	CCBC	MC	NVCC	PGCC
CW 110	CyberEthics	CSI 194	PHIL 250	NA	ITE105	NA
CW 120	Intro to Computers	CSI 113	CINS 101	CS 110	ITE100	CIS 101
CW 130	Microcomputer Operating Systems	CSI 130	NA	NW 127	ITN 106	CIS 170
CW 140	Unix/Linux	CSI 135	CINS 142	NA	ITN 171	CIS 272
CW 150	Networking 1	CSI 157	DCOM 217	NW 151	ITN 154	ENT 194
CW 151	Networking 2	CSI 158	DCOM 218	NW 252	ITN 155	ENT 195
CW 160	Security +	CSI 165	DCOM 258	NW 173	ITN 260	CIS 162
CW 170	Digital Forensics	CSI 208	DCOM 213	NA	ITN 295 (2)	FOS 260
CW 215	Information Systems Security	CSI 214	NA	NA	ITN 262	NA
CW 225	Hardening the Infrastructure	CSI 217	NA	NW 245	NA	CIS 163
CW 230	Microsoft Windows Server	CSI 265	DCOM 202	NW 203	ITN 200	CIS 231
CW 232	Microsoft Windows Networking	CSI 266	NA	NA	ITN 117	CIS 230
CW 235	Network Defense and Countermeasures	CSI 219	NA	NW 246	ITN 261	CIS 166
CW 240	Advanced Unix/Linux	CSI 235	DCOM 259	NA	ITN 270	NA
CW 241	Unix/Linux Sys Admin	CSI 236	CINS 244	NA	ITN 170	CIS 276
CW 245	Wireless LANs	CSI 269	NA	NW 229	ITN 120	ENT 219
CW 250	Networking 3	CSI 257	DCOM 219	NW 253	ITN 156	ENT 196
CW 251	Networking 4	CSI 258	DCOM 220	NW 254	ITN 157	ENT 197
CW 260	Firewalls	NA	DCOM 211	See NW 261	NA	NA
CW 261	Intrusion Detection Systems	NA	DCOM 212	See NW 262	ITN 263	NA
CW 270	Capstone	CSI 270	NA	NW 270	ITN 293	CIS 269

The CyberWATCH identifier for each course will be useful in cross-referencing courses among institutions for transfer purposes by students, registrars, and articulation specialists. Each institution has its own prefix, numbering system, and course title identifying catalog courses. A computer introductory course, for example, might be designated as “Introduction to Computers – CSI 113” at one institution and “Computer Literacy - CIS 101” at another. And both courses could contain essentially the same content and mapping to a CNSS standard. However, this similarity or equivalence might not be obvious from the catalog description alone.

The CW designations are supplemental, not replacements, to each institution’s designators. It is recommended that each institution add the CW designators to the course descriptions in their catalogs and schedules of classes.

Capitol College (CC) offers a broad suite of degree programs and certification preparation courses in the field of information assurance. These include:

- Bachelor of Science in Information Assurance
- Master of Science in Information Assurance
- Master of Science in Information and Telecommunications Systems Management with an emphasis in Information Assurance
- Master of Business Administration with an emphasis in Information Assurance
- Certification review courses to include CISSP, SSCP, and Security+

All master’s degree courses are offered online in real-time. The same holds true for the certification review courses. Beginning fall 2008, Capitol College will begin delivering the 3rd and 4th year courses that lead to the B.S. in Information Assurance in the online format, thereby providing access to associate-level students at-a-distance. Capitol College is the only institution in the nation to offer an online curriculum in information assurance that is fully mapped, at the advanced level where appropriate, to all six CNSS (Committee on National Security Systems) standards. Graduates of this curriculum receive documentation (listing all six standards) that indicates they have studied and been determined to meet the curriculum requirements as approved by the CNSS. In addition, degree-seeking students can select classes that lead to a post-graduate certificate in network protection and/or security management. Likewise, participants in the certification preparation course(s) also receive a document of completion that reflects that they are prepared to sit for the respective industry certification(s), thereby preparing themselves to meet the federal requirements as set forth by DoD 8570.1.

George Mason University (GMU) added several new courses and revised the curriculum for 2006-7. The enrollments in the GMU program increased about 20% over the prior year. Estimated number of students in the current year is 400 as compared to the 2006-7 total which was about 350. While the total enrollment in the GMU program is steady extra sections of the required security course were added in Fall 2007 and Spring 2008 semesters accounting for the +50 bump.

George Washington University (GWU) has two primary responsibilities to CyberWATCH. The first is to support a graduate student whose efforts are directed toward the Collegiate Cyber Defense Competition. Our GTA (Kerry McKay) worked on the local and regional contests, supporting Casey O'Brien.

Dr. Costis Toregas from the Computer Science Department at George Washington University was engaged to conduct research designed to improve the communications and placement capacity of the CyberWATCH program. In Phase I, a small number of Community Colleges were interviewed to determine the needs and resources available within the system. Phase II will work to publicize the capacity of the community colleges and to brand the CyberWATCH students as an outstanding resource in computer security. Phase II will also establish an internet-based fair and work to create a central, go-to place within CyberWATCH for internships and jobs for our students.

University of Maryland University College (UMUC) offers Bachelor's in Information System Management with IA major and minor, Undergraduate Certificate, Master's of Science in Information Technology with IA specialization, Graduate certificate, and Doctoral core course in Information Assurance and opportunity to write a dissertation in IA. UMUC has a Network and Security Lab, Database lab, and offers instruction face to face and provides online remote access. UMUC has been a National Center of Academic Excellence in Information Assurance Education since 2002 and has its curriculum mapped to CNSS 4011, 4012, and 4013.

Course Development

Faculty at Prince George's Community College developed two new non-technical courses, Cyber Law and Disaster Recovery and Risk Management. Disaster Recovery and Risk Management is being offered for the first time this fall. Both courses will be offered in an online format and shared with all partner institutions.

The **Cyber Law course** is offered at NVCC and is included as a core in their Network Security A.A.S. degree. It examines current and emerging cyber law issues that are critical to business, government, and individuals. Students examine jurisdiction; protection of intellectual property; contracts and licensing agreements; sales tax; raising equity capital online; privacy; obscenity in cyberspace; defamation; internet and information security; computer crime; and ethics. The course is being modified so that it can be offered in an online format to partner institutions and a training workshop was performed March 14, 2008.

Disaster Recovery and Risk Management, developed by PGCC, provides individuals and organizations with tools to prepare for and recover from both natural and man-made disasters. Students will gain an understanding of risk and crisis management, the need for business continuity and information assurance planning, as well as addressing the leadership, human, organizational and public policy components of disasters. In addition to offering this course, PGCC has developed a Letter of Recognition and a Certificate for Disaster Recovery and Risk Management.

To facilitate dissemination of this information, Drs. Boyce and Breen are planning to participate in the 2008 Colloquium for Information Systems Security Education. Dr. Breen is also exploring the possibility of organizing a Millennium Management Lecture on Disaster Recovery and Risk Management for Fall 2008

NVCC also offered a BUS 212/ITN 295 – Disaster Recovery Planning for Managers in the Fall 2007. While only a few students enrolled, it managed to attract students from outside of IT courses as it was offered as either IT or Business credit. NVCC has also developed the following courses this year:

- Topics in: Intro to Homeland Security (1 cr.)
- Topics in: Cyberterrorism (1 cr.)
- Topics in: Cyberfraud (1 cr.)
- Topics in: Intro to Computer Forensics (1 cr.)
- Computer Forensics I – Physical Layer (3 cr)
- Computer Forensics II – Logical Layer (3 cr)
- Topics in: Gray Hat Hacking (3 cr)
- Wireless Security (3 cr)
- Topics in: CISSP Prep (3 cr)
- Topics in: Network Visualization (3 cr) (under development)

NVCC will also be expanding the Cisco Academy program to its Alexandria campus. It is presently at Annandale and Woodbridge campuses, where it is integrated with Forest Park High School's program. The courses will be offered in an online format and shared with all partner institutions.

Materials Development

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

These modules include a combination of PowerPoint slides, hands-on lab exercises, case studies, and exams and are available for **FREE** to participating CyberWATCH faculty for use in their programs.

Modularized materials - In 2006-2007, Howard Community College developed and delivered modularized classroom materials to supplement the three detailed class outlines developed and mapped to the 4011 standard by AACC. AACC class designators were CSI 165 - Network Security Fundamentals, CSI 217 - Hardening the Infrastructure, and CSI 219 - Network Defense and Countermeasures. Over a seven month period, the CSI 165 and CSI 219 modularized materials were completed and delivered on schedule.

Additional CyberWATCH courses with modules available include:

-CW 225- Hardening the Infrastructure
-CW 235 - Network Defense and Countermeasures
-CW 160 - Security+

To see a complete list of modules, by CyberWATCH course, see http://www.cyberwatchcenter.org/educators/modules.htm.

CyberWATCH Textbook and Curriculum Committee met on July 17, 2007 at Anne Arundel Community College. Representatives from Anne Arundel Community College, Chesapeake Community College, College of Southern Maryland, Community College of Baltimore County, Hagerstown Community College, Howard Community College, Montgomery Community College, Prince George's Community College, and University of Maryland University College attended. All representatives agreed that it is desirable for all core and elective technical courses related to the institutions' ISS programs be freely shared with CyberWATCH partners through the CyberWATCH Web site. In the future institutions offering courses in addition to those making up the core and elective CyberWATCH model, will make the course descriptions, detailed outlines, and textbook recommendations available through the website. Attendees agreed that each institution would provide templates to guide students through a four semester completion path. In order to facilitate articulation agreements for CyberWATCH community college partners with four year institutions, it was proposed that a standard CyberWATCH designator be embedded in the partners' course descriptions.

The CyberWATCH Textbook and Curriculum Committee met again at Anne Arundel Community College on November 15, 2007. In attendance were representatives from Anne Arundel Community College, Chesapeake Community College, College of Southern Maryland College, and Hagerstown Community College.

The committee addressed the development of a matrix (spreadsheet) depicting the offering of CyberWATCH core technical courses at each participating community college (on page 10 of this report).

Student Development

Mid-Atlantic Regional Collegiate Cyber Defense Competition, CCDC

> **NVC Recommendation**
>
> **CCDC:** *The NVC recommends that a formal way to collect feedback from competition participants be devised. As an example, Howard Community College solicited post-event feedback from their participants as to how to modify their curriculum.* (NVC Report, April 2007)

The CyberWATCH evaluator worked in conjunction with Casey O' Brien, CyberWATCH Co-PI and the lead person for CCDC worked to develop surveys to assess the impact on current competition participants (both students and faculty), and past student participants. These surveys were implemented for the 2008 competitions The student survey asked CCDC participants to assess the impact of CCDC participation relative to a variety of factors, including:

- Increased ability to apply technical skills and knowledge to real-world situations.
- Increased ability to handle the pressure of real-world situations.
- Increased ability to work on a team to handle real-world problems.
- Increased knowledge of cybersecurity and information assurance.
- Better preparedness to work in the IA/Cybersecurity field
- Increased inclination to pursue a career in the IA/Cybersecurity field.

Students were also asked to assess their overall satisfaction with CCDC participation, its effectiveness as a learning experience, its impact on their future career and educational goals, and how the experience changed them. Students were also asked to report on any interactions they had with recruiters or potential reporters.

Faculty participants were asked to assess their overall satisfaction with CCDC participation and its effectiveness as a learning experience.

Detailed results of these surveys can be found in the CyberWATCH Evaluation Report.

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.

In its third year, the Mid-Atlantic Regional CCDC has grown from 5 teams to 9, representing two- and four-year schools from Maryland, Pennsylvania, Virginia, and the District of Columbia. The number of students that have participated in the past three Mid-Atlantic Regional CCDCs is 138, comprising both undergraduate and graduate students.

The Mid-Atlantic Regional CCDC continues to innovate and in terms of the growth and scalability:

1. U.S. secret Service play an active role as law enforcement (requiring teams to conduct a live investigation with federal law enforcement);
2. Entire segments of the of the real Internet have been replicated (thus, simulating assets that are not controlled by the defending teams, but are required to maintain functionality and connectivity to the outside world); and
3. Scoring engine supports mapping visualization, basic Red Team tracking, and three-dimensional modeling of the teams' assets.

Digital Forensic Cup

The Digital Forensics Community College competition was kicked off on Feb. 11, with an announcement to the CyberWATCH community college members. This first trail of the competition was kept to the CyberWATCH membership so we could more effectively evaluate the competition, its operation and effectiveness. To date two teams from local community colleges have entered the competition. Their results are due by April 18, with an announcement of the winner in early May.

The competition consisted of 8 challenges, ranging from 'straight-forward' to 'difficult'. The teams were instructed to submit their solutions by April 18. It is not expected that a team will have solutions for all the challenges. They were instructed to submit whatever they have by the deadline. We are using students from the Johns Hopkins Digital Forensics program to evaluate the submissions.

The challenges were developed in partnership with the DoD Cyber Crimes Center (DC3). They were instrumental in providing guidance and challenge data for the competition.

CyberWATCH Virtual Lab

NVC Recommendation

***Virtual Lab:** It is suggested that CyberWATCH personnel, and Montgomery College in particular, plan for how the lab's utilization and effectiveness will be evaluated.*

The state-of-the-art IT Security Virtual Lab is physically located on the Germantown Campus of Montgomery College and is available to all CyberWATCH institutions via the Internet. The Virtual Lab was launched in Fall 2006. During spring 2007 the lab was refined and improved. Lab Access training for instructors was made available on most Fridays during the period March-July 2007 and on an on-demand basis in Fall 2007 and Spring 2008. Representative instructors from Northern Virginia Community College, Hagerstown Community College, Prince George's Community College, Capitol College, University of Maryland University College, and the College of Southern Maryland attended these orientation sessions. In addition, a Faculty User Guide was provided on CD to all attendees of Lab Access training. The Lab is currently available to all member institutions and access can be scheduled 24/7. Since orientation began several institutions have scheduled blocks of time to begin working with the Virtual Lab in order to familiarize their faculty with the facilities. These institutions are Capitol College, Montgomery College, Prince George's Community College, and University of Maryland University College. An Advanced Instructor Training workshop is planned for summer 2008.

The plan for determining the Virtual Lab's utilization and effectiveness was first suggested in 2007. It was determined that such information could be gathered in two ways: 1) Modify the software (RASSLe) to keep detailed records on which institutions were actually using the lab, the times students were logged in, the particular devices they were using, and a required, on-line evaluation from users at the end of each semester. 2) Have each institution individually provide data on their student and faculty use of the lab.

The preferred option was the use of the RASSLe software originally obtained from Moraine Valley Community College (MVCC). MVCC is the technical support for this software program. However, as the company that created RASSLe went out of business in summer 2007 and the programmer who designed the software was very hard to reach and unresponsive, MC has not been able to obtain the modifications of RASSLe software needed to closely monitor institutional and student use. Consequently, at present institutional use and effectiveness can only be gauged by the number of hours requested by each institution.

The alternative is called Netlab. However, the Netlab alternative is very expensive, so it was decided to go with Moraine Valley's contracted software (RASSLe was provided to MC free of charge.) The Netlab option was reconsidered but, as mentioned above, is prohibitively expensive. The initial installation of Netlab hardware and software in the Virtual Lab would cost an estimated $40~$50,000 and the yearly required maintenance for Netlab is estimated in excess of $20,000. MC does not see any way at this point for the Virtual Lab to generate that kind of additional revenue. Consequently, that option is not viable.

Concerning the second option, surveys can be designed for classes which are using the Virtual Lab. However, most member institutions have not yet made full use of the lab and so student evaluations are not yet available.

A survey (see below) was conducted of a pilot class which was held in early summer 2007. That survey indicated a very positive response to the Virtual Lab. The instructor and the students found the Virtual Lab to be much more convenient than a classroom lab due to its availability anywhere and anytime. (One of the disadvantages of a classroom lab is that they are only available when an instructor or proctor is available on-site and the facilities are open during normal working hours.)

Pilot Class held May~July 2007 – Montgomery College ran a pilot course which took full advantage of the remote lab resources. (Note: This course is now part of the security degree program adopted by Montgomery College as part of CyberWATCH.)

- All installed equipment currently available in the remote lab was tested under normal lab-use conditions.
- Any problems were corrected.
- Additional software was added to server systems.
- Configuration modifications were made to network gear.
- This course was very successful. Student responses to use of the remote lab were as follows:

Question	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree
The hands-on lab activities helped me to achieve the stated course objectives.				40%	60%
The e-Lab activities (Interactive Lab Activities) helped me to achieve the stated course objectives.				50%	50%
Having access to equipment in the classroom helped me learn. (Virtual Lab, on-line.)				10%	90%
Having access to equipment outside the classroom helped me learn. (Virtual Lab, on-line.)			20%*	20%	60%

*Note: These students did not make use of the lab outside normal classroom hours.

Montgomery College will continue to improve the lab and assist other member schools in adapting labs and curriculum to the equipment available in the lab.

College Faculty Development

Since April 2007 a number of training opportunities were offered to CyberWATCH faculty.

Computer Forensics Workshop
The Computer Forensics Workshop offered by the Northern Virginia Community College in April 2007 was attended by 24 CyberWATCH faculty. This one-day workshop was designed to provide IT faculty interested in instructing Computer Forensic courses with an overview of computer forensics and included hands-on labs using tools such as Encase to retrieve evidence data off of a hard disk. The workshop was taught by Det. Ken Haynes, an active law enforcement professional in the computer forensics field.

Digital Forensics Working Group (DFWG)
The four-day Digital Forensics Working Group 2007 at the University of Louisville in June 2007 was attended by 6 CyberWATCH faculty. The conference was an opportunity for educators who are interested in implementing, or who already have implemented, programs in Computer Forensics at their institutions to share current research and address forensic education issues.

Colloquium for Information Systems Security Education Conference
The Colloquium for Information Systems Security Education Conference held on June 4-June 7, 2007 in Boston was attended by seven CyberWATCH faculty members. The conference provided a forum for academia, government, and industry INFOSEC experts to discuss:

- Assessment of need for IS workers/researchers/faculty (numbers)
- Integration of IA topics in existing graduate or undergraduate curricula
- Alignment of curriculum with existing IA standards
- Emerging programs or centers in IA
- Best practices
- Vision for the future
- Tools to help educate the public in computer security

Certified Wireless Network Administration (CWNA)+ Security
Two Certified Wireless Network Administration + Security Workshops were hosted by Howard Community College over the past year. Both were designed for individuals with advanced knowledge of, and experience with, troubleshooting, maintaining, and hardening wireless networks. The workshop from July 23-27, 2007 was attended by thirteen CyberWATCH faculty, while the workshop in January 2008 was attended by three CyberWATCH faculty.

GMU 2007 International Training Symposium in Computer Forensics
The George Mason University 2007 International Training Symposium in Computer Forensics, sponsored by the Regional Computer Forensics Group, was held August 6-10, 2007. Seven CyberWATCH faculty attended. The conference provided an opportunity for faculty to train on forensic tools in hands-on labs and provided information and presentations on forensic issues and tools.

All About Labs Workshop

The Community College of Baltimore County organized and presented a four-day workshop, “All About Labs,” from August 20-23, 2007. Nine faculty from eight CyberWATCH institutions participated in this workshop. Workshop participants learned how to setup different face-to-face lab environments, as well as how to access and use the CyberWATCH Virtual Lab and CyberWATCH Virtual Private Network. Participants left the workshop with a variety of virtualization options and images, security tools, and completed labs that could be immediately implemented in their programs.

Certified Information System Security Professional (CISSP)

Twenty three faculty members from CyberWATCH two- and four-year member institutions supported by CyberWATCH completed the online CISSP Certification Preparation Program conducted by Capitol College, a CyberWATCH partner. Capitol College continues to provide the discount rate to CyberWATCH faculty in 2007.

Cyberlaw Workshop

Twelve faculty members attended a workshop at NVCC designed to provide information to CyberWATCH faculty members interested in teaching a cyberlaw course. Topics addressed during the workshop included suggested course content, requisite faculty qualifications, course focus and locating partnership opportunities with other academic departments. Faculty attending received a USB thumb drive containing information that can be used in their own course, including sample course content and syllabus, example case studies, and content and textbook resources.

Future workshops scheduled for 2008 include:

- **Intrusion Detection Systems (IDS) – Fall 2008 at Arlington.** A hands-on one day workshop intended to train faculty on the basics of installing and managing IDS. The workshop will provide labs and resources that can immediately be used in their classes.
- **Cybercrime Workshop –** TBD Fall 2008. Online workshop**.**
- **Network Visualization Workshop – Sept. 2008.** One day hands-on workshop.
- **Certified Ethical Hacker (CEH) Prep - August 2008.** A week-long hands-on workshop to prepare interested faculty for the CEH examination.

Additionally, NVCC is purchasing an island in Second Life that can be used to establish a virtual training center for CyberWATCH faculty. As CyberWATCH expands, this will allow training to be delivered online to faculty located anywhere over the Internet in a dynamic, virtual reality classroom.

CyberWATCH Faculty Graduate Program

The program initiated in December 2006 and implemented in January 2007 continues to grow and fulfill its goal of building a cadre of highly trained professionals in the region. Nine graduate courses have been completed by participants in the Faculty Graduate Program since April, 2007. Two faculty members have already completed graduate certificates in Information Assurance at Capitol College. Participants from College of Southern Maryland and Hagerstown Community College are currently working on graduate certificates; one of these participants is planning to pursue a Master’s degree in the field and the other plans to pursue a doctorate in IA. Another faculty member from UMUC plans to pursue a Master’s degree in an IA program at James Madison University that is housed in computer science, giving it a more technical focus. He begins course work in May.

Two CyberWATCH faculty from Anne Arundel Community College and Northern Virginia Community College are also currently in doctoral or post-doc programs. Although these are not being financially supported by the CyberWATCH graduate program, they certainly help the mission of developing the professional cadre. The breath of the program, both in terms of the institutions of those participating and the institutions being attended, is impressive. The depth, going beyond the certificates and into master’s, doctoral, and post-doc programs, is impressive as well.

K-12 Programs

The *Young Scholars Program: Students, Learning and Technology* (SLT)

This program for high school students was delivered by the Educational Technology Policy, Research, and Outreach Inc. at two locations in the summer of 2007. The Harford County Program took place at Joppatowne High School in Joppatowne, MD (Harford County) from July 9 through July 20th . The Prince George's County Program took place at Walker Mill Middle School from July 9th through 27th.

Both programs focused on activities that highlighted topics in cybersecurity to illustrate the need to operate in a secure manner and to emphasize the exciting opportunities in this field. Students engaged in hands-on computer activities and learned about digital literacy (technology fluency and applications, team building, collaboration tools, problem based critical thinking), defending against viruses, Trojan Horses, and worms; and applying basic security concepts through gaming, modeling and simulation development, while investigating exciting careers that interconnect the fields of science, math, technology, and computer security. Students also discussed such topics as cryptography, system vulnerabilities, and careers in computer security and digital forensics. Tours of local labs, NIH, NSA, and Carderock Observatory were also conducted, and students had the opportunity to hear from a variety of speakers from state and federal agencies and local security companies.

The CyberWATCH grant supported a total of 56 students. Thirteen high school students attended Program I at Joppatowne High School and 43 middle and high school students attended Program II at Walker Mill Middle School.

Douglas Handy, Career and Technology Program coordinator for MSDE Program suggested the program be held at Program I at Joppatowne High School as a component of recruitment for a newly proposed MSDE CTE track. Students were recruited for the Joppatowne High School Program through Leah Beaulieu who is the program coordinator for a new Homeland Security and Emergency Preparedness Program being piloted in the Fall 2007-08 school year. The program will be added to the Maryland State Department of Education (MSDE) Career and Technology Education programs. This activity was the subject of a July 22 article in the Baltimore Sun, Harford County Edition.

Recruitment for Program II was done through Prince George's County Schools and The Patriots Technology Training Center (PTTC), a non-profit foundation committed to promoting technology-related careers.

Middle Schools Program

This program for middle school girls was third in a series of ***Cool Careers in Cybersecurity Workshops*** was held Thursday October 4, 2007**.** It provided information and skills necessary to navigate the professional pipeline in the vast fields of Cybersecurity and Information Assurance as well as other Sciences, Technology, Engineering, and Mathematics (STEM) fields. The workshop was run in conjunction with the 6th annual Cyberethics, Cybersafety and Cybersecurity (C3) conference. 33 middle school girls and 25 high school students (N: F=14; M=11) from Fairfax County schools attended. Sessions included hands-on activities, speakers, and an opportunity to talk with professionals in the field. Participants learned more about Cybersecurity, as well as ethics and safety. Participants also learned first hand from IT/IA experts about career opportunities and pathways in Cybersecurity by visiting two UMD Technology Incubator companies: **Trufina** and **TRX Systems**. A fourth workshop was held in McLean, VA January 2008 in partnership with Safe Community Coalition and Girl Scouts of the USA. 21 Elementary Girl Scouts participated. Activities included hands-on activities, speakers, and an opportunity to talk with professionals in the field. An evening session for parents/community members-*Cybersecurity: the Forgotten Element* was also included. A fifth workshop will be held with Girls Scouts of Central Maryland on March 26th.

High School Teacher Training

George Mason University (GMU)

GMU became a Cisco Regional Academy in Spring 2006 and is actively working with Cisco Local Academies, thus impacting the high school-to-college pipeline. It serves 15 Local Academies with approximately 300 students. GMU also operates a Local Academy with approximately 20 students per semester taking courses on a voluntary basis.

One instructor has completed the CCNA & CCAI Instructor Certificates and has taught his first course at NVCC Annandale. Six more instructors are in the process of completing those certificates. At the annual meeting in January, 15 instructors completed CCNA Certificates in Continuing Education – coursework included design and implementation of a 4-router network at Mason's Manassas campus.

Prince George's Community College (PGCC)

The teacher training programs at PGCC 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.

The Cisco Networking Academy Program at PGCC uses Regional Academies to train and monitor Local Academies. The Regional Academy at Prince George’s Community College provided multiple “train-the-trainer” courses for high school teachers during 2007-08. These courses included: 1) Cisco’s Information Technology Essentials, which many school systems use as a lead-in to the actual CCNA courses; 2) the actual CCNA curriculum in both the 3.1 version and the new CCNA 4.0 Discovery and Exploration versions; and 3) an Orientation course for instructors who are new to the Cisco Networking Academy program.

Cisco Curriculum Updates

In the fall of 2008 academic year, many schools adopted Cisco’s new CCNA Discovery and Exploration curricula, which feature security components that are greatly enhanced over those in the previous Cisco curriculum. To help schools prepare to teach the updated curriculum, the Cisco Regional Academy at Prince George’s Community College and the Cisco Advanced Technology Center (CATC) at West Virginia University provided update training in the new curricula. The training for the CCNA Discovery curriculum took place on August 7 and 8 and the update for the Exploration curriculum took place August 9. The instructors who received the update training were from Prince George's County Public Schools (7), Anne Arundel County Public Schools (2), Frederick County Public Schools (3), Baltimore County Public Schools (1), and the District of Columbia Public Schools (3). Instructors from community colleges received the update training as well – Anne Arundel Community College (1), Prince George's Community College (2), and Hagerstown Community College (1).

IT Essentials I
This course maps to CompTIA's A+ certification. During the summer of 2007, six teachers from Prince George's County Public Schools (PGCPS) successfully completed this course through the Regional Academy at Prince George's Community College. During December 2007, two instructors from the District of Columbia Public Schools completed this course through the PGCC Regional Academy.

Cisco CCNA 2: Routers and Routing Basics
CCNA 2 focuses on initial router configuration, Cisco operating system software management, routing protocol configuration, TCP/IP, and access control lists (ACLs). During the spring and summer of 2007, eight teachers from PGCPS successfully completed this course through the Regional Academy at Prince George's Community College.

Cisco CCNA Discovery 1: Networking for Homes and Small Businesses
This is the first course in the new curriculum, aimed at high school students. The Regional Academy at Prince George's Community College provided this course for two instructors from PGCPS and one from Montgomery County Public Schools during August 2007 so that they would be qualified to teach it at the start of the 2007-08 academic year.

Cisco CCNA Discovery 2: Working at a Small-to-Medium Business or ISP
This is the second course in the new Discovery curriculum, and involves IP addressing and router configuration. During February 2008, two instructors from PGCPS completed this course through the regional academy at PGCC.

Cisco CCNA Discovery 3: Introducing Routing and Switching in the Enterprise
Cisco CCNA Discovery 4: Designing and Supporting Computer Networks
Instructor training in these two courses is planned for beginning the week of June 9, 2008. The courses will be offered through the Regional Academy at PGCC.

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. Instructors must complete this course before they can teach any course through the Cisco Networking Academy Program. During December 2007/January 2008, two instructors from DCPS completed this course through the Regional Academy at PGCC.

Guidance Counselor Workshop

A full day workshop occurred on September 27, 2007, held at the JHU Building in Columbia, MD in partnership with MD and VA State Departments of Education. The workshop focused on educating 63 counselors on current and future career options for students in Information Assurance, Information Security, Cybersecurity and Digital Forensics, what's expected (i.e., clearances) and how to get there.

The morning included insight from Lynn McNulty, CISSP, Director of Government Affairs of (ISC)^2, discussing current labor stats, sharing with the audience the need for filling the IT/IA/IS pipeline, current and future career trends, and provided an opportunity to describe the landscape through the eyes of an organization dedicated to certifying IS professionals. Mr. McNulty was followed by Ralph Coppola, Director of Worldwide Education-PTC who again shared the need for increasing the IT pipeline from an engineering opportunity perspective. Davina Pruitt-Mentle then moderated a panel discussion with the primary topic being academic tracks and outside programs in this area. Panel members represented 2 year tracks and certification programs, 4 year programs, MD Internet Crimes Division, and large and small companies (Northrop Grumman, Convergence and Montani). Luncheon keynote was Carroll McGillin, National Initiatives Manager with Cisco Systems' Networking Academy Program who spoke about the IS/IA need in Maryland and opportunities through Cisco Academy Programs. The afternoon sessions included Detective Sgt Robert Smolek who discussed opportunities in the area of digital forensics and Bruce George who spoke on the topic of "Demystifying Clearances Lingo". Davina Pruitt-Mentle ended by sharing what resources are available through the CyberWATCH Center and website.

Additionally, stipends @$100.00 were made available through NSF (National Science Foundation) funding for 20 guidance counselors based on 1) first come first serve basis and 2) stipend participants were asked to create recruitment brochures/ fliers based on workshop content that will then be shared with students and parents (and other GC), and to present materials and/or new resources with faculty and/or parents at their school. Stipend awardees were required to attend the stipend briefing. Materials are currently being added to the website for others to view, utilize and share.

Presenter materials and an overview of the event have been archived at:
http://www.edtechpolicy.org/Cyberwatch/gcworkshop.html

Cyberethics, Cybersafety and Cybersecurity (C3) Conference

The Annual C3 Conference focuses on Cyberethics, Cybersafety and Cybersecurity as related to the educational setting (K-20). NSF funding has allowed additional participants to attend and provided for enhancements to the Cybersecurity programming. School districts budgets are increasingly constrained, and the funding allows for teachers to participate in the program. Additionally, we have focused efforts on Cybersecurity issues for the user services and IT support staff, and paid for their attendance. 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. NSF supported 100 attendees (recruited from local school system, private/charter school and area 2-4 year college IT departments). They had access to both days of the conference, speakers, and workshops, a CD of course material, and numerous handouts. Additional monetary support came from the National Cyber Security Alliance, (ISC)^2 , Symantec, Northrop Grumman and CyberSmart!, and workshop sponsorships from The Center for Safe and Responsible Internet Use, NetSmartz, and the C3 Institute, enabling us to deliver a high quality, well received conference that addressed the needs of the educational community. Over the two days we had 233 attendees, from Maryland, Virginia, New Jersey and Delaware school districts in addition to representatives from Higher Education, Non-profits, Business and Government/Law enforcement. The conference website can be found at: http://www.edtechpolicy.org/C32007/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 2008 conference will be held October 2 & 3. CyberWATCH funding will support the conference in year 4, with several security related activities being planned, in coordinated with the Digital Forensic and Network Lab. Tentatively, a Cybersecurity Summit and MD K-20 Academic Integrity Summit are being planned around the 2008 C3 conference.

Cybersecurity topics included: **State's Attorney, Mr. Gansler** overview of Maryland's C.L.I.C.K.S. initiative - Community Leadership in Cyber Knowledge & Safety - an educational outreach program designed to equip Maryland's community leaders with the resources to teach students and their parents about Internet safety. Security topics (highlighting identity theft) were also covered, **First Sergeant Robert Smolek** an 18-year veteran of the Maryland State Police, currently assigned to the Criminal Investigation Division where he supervises the Computer Crimes Unit, discussed the federally funded, multi-agency, multi-jurisdictional virtual task force designed to increase the capacity of Maryland law enforcement to respond to computer facilitated crimes against children, **Trooper First class and MD State Police Investigator E. Cohen** finished the session with an overview of educator and end user "do and don'ts" for Internet Safety, **Dara Gordon Murray**, CISSP and Director, IT Security Staff, CISO and Sr. Sec. Advisor to the Assistant Sec. for Program Support U.S. Health and Human Services shared with the audience *Protecting Your Children and Home Computer*, **Ron Teixeira**, Executive Director, National Cyber Security Alliance shared the recently released (October 2007) *McAfee/NCSA Study Findings*, **Bob Kirby**, Senior Director for K-12 Education**,** CDW-G reviewed the recent (summer 2007) CDW-G School Safety and Security Index, **Nancy Willard,** Center For Safe and Responsible Internet Use Cyber-Safe Kids, Cyber-Savvy Teens, Cyber-Secure Schools. The session provided an overview of youth risk online issues, influences on youth online behavior, an analysis of Internet safety approaches that are not working, and guidance on more effective school-based strategies, and **Iris Beckwith** from iKeepSafe reviewed the iKeepSafe & Symantec Mobile Truck Partnership initiative and resources, and more about Internet Keep Safe Coalition. **Second Day: Selected/Added Cybersecurity breakout session**: Cybersecurity: the forgotten element.

High School Student Entry Points

Student Internships/Jobs

> **NVC Concern**
>
> *With internships being such a valued activity for CyberWATCH, the NVC is not convinced that the Metropolitan Washington Council of Governments (COG) is the right vehicle to manage student internships. Very few internships have been made available to the entire CyberWATCH service area to date. There is also a question on a sustainability plan for COG's role in the Center. The NVC recommends a thorough review of the entire internship process. If there are college cooperative education departments who could take on this activity at the campus lever, that might prove more effective.* (NVC Report, April 2007)

In reaction to this concern, CyberWATCH has made internships/job opportunities the major focus of the Strategic Planning meeting that took place in Summer 2007. The internship process originally conceived as a centralized model led by the Metropolitan Washington Council of Governments (COG) is changing to a new **decentralized and multi-faceted model.**

The Pilot Internship Model – This is a centralized administrative coordination and communication model with region specific business partner and student internship assignment and tracking.

In late August 2007 a CyberWATCH Internship Team, led by Howard Community College was formed to address and properly plan for this change in approach. After MWCOG shared their lessons learned and documents developed, a pilot proof of concept program was deployed in September of 2007. Howard Community College, Anne Arundel Community College, Community College Baltimore County and Cisco, participated in this pilot program.

Cisco's work in bringing its business partners to the conversation was instrumental in helping CyberWATCH shape the internship process. They provided assistance in identifying the skill set our two year students could meet. Students from the three pilot program schools were organized, categorized, prepared for interviews, and matched to job descriptions supplied by the Cisco business partners. Three students from HCC and one student from AACC have since been placed in internships with three Cisco based partners. Additional three HCC students have been placed in internships with non Cisco based business partners in the Columbia Maryland area. Status and success metrics will be gathered to make sure both the business partners and students are satisfied with the program's outcomes. In addition, a more comprehensive deployment of this program will be made after lessons learned are reviewed and corrective actions are made.

Internship Research and Virtual Job Fair - in order to execute this shift in strategy, Dr. Costis Toregas from the Computer Science department at George Washington University was engaged to conduct research designed to improve the communications and placement capacity of the CyberWATCH program. He brings to CyberWATCH experience in managing job fairs for national CS/IA student programs, and also an appreciation of extended network management for collaborative outcomes. His work is already enhancing the entire process by grounding it in needs analysis and strong stakeholder engagement, both from students' and employers' vantage points, as well as the participating institutions.

The GWU engagement has produced a Phase I report which established and presented a number of strategies for CyberWATCH to pursue. The chosen strategy is one of a decentralized approach led by a small number of interested institutions, and results from their experimentation is then expected to be made available to the entire network. The institutions involved in Phase II include Anne Arundel Community College, Howard Community College, Community College Baltimore County and University of Maryland University Campus. In addition to those four institutions, the Cisco resources are also brought in to further strengthen the effort.

During Phase II, several principles have been developed that are used to optimize job development efforts; they include:

- emphasize the competitive advantages of member institutions and the region; given the importance of a strong secure IT infrastructure and the economic contributions of IT start ups to the region, the employer focus will be small IT firms, and the assistance of County departments of economic development will be solicited.
- use internet-based strategies to improve effectiveness of participants; established cyber fair software using avatars, resume exchanges and promotions is being investigated in order to excite and interest students and employers alike in a cyber event.
- develop a strong brand of a CyberWATCH student, especially targeting mistaken impression that graduates of two-year colleges do not have adequate skills for CS/IA jobs
- Even in a decentralized network like CybeWATCH, it is important to provide centralized planning and the creation of strategies for experimentation; GWU, one of the network institutions, is providing this role currently, and one of the evaluation foci after the end of Phase II will be to evaluate the benefits from having an assigned network-wide resource in this important network-wide function of placement.

Internal Internship Model - Since partner institutions of high education have information security offices for their institutions, CyberWATCH is exploring the possibility of leveraging these offices in the student internship program. PGCC has placed an intern with the Director of Security Services during the last half of spring semester, 2008. This experience will be documented and shared with the other consortium members. If successful, the model can be replicated at the other institutions, both 2 and 4-year.

The Joint Educational Opportunities for Minorities (JEOM) summer intern program (a Department of Defense office of High Performance Computing Modernization program) is another possible internship model being investigated. This program uses an interesting model that CyberWATCH business partners may be able to adapt to suit their own needs for high achieving students interested in doing summer internships. Instead of the standard “headhunter” approach of matching students with openings, JEOM solicits widely for applications for their internships, setting a high grade point average as a minimum qualification. Students apply for the internships online. DoD seems to be viewing this mechanism as a way to recruit the best and the brightest for this program, which they hope will serve as a steppingstone to careers with their organization for many of these students. This topic is scheduled to be discussed with two CyberWATCH partners, Cisco and Lockheed Martin in the near future.

Additional internship opportunities – recent conversations with professionals from Computer Associates (CA), Northrop Grumman, and the Information Assurance Technology Analysis Center (IATAC), indicated strong interest on their part in acquiring student interns from CyberWATCH institutions. In the first two years of its existence CyberWATCH has built a foundation for a robust internship program in the future.

The work and research on internships so far revealed the need to develop a standard student profile / resume that would have a major component be common to all institutions and provide a "branding" component for CyberWATCH. Each school would put their own touch to reflect culture and tradition, but CyberWATCH participation would have a consistent "look and feel" to it, including a statement on articulation and mapping of course work to NSA and other standards. An additional idea is the notion of building a sustainable revenue source for promoting CyberWATCH through fees charged to potential employers in cyberfairs and other recruiting events. This revenue source, while not major, could offset branding costs irrespective of NSF funding and could help maintain the CyberWATCH name and reputation strong and attractive for the employer marketplace, as well as provide a stream of program candidates from those who see it and are moved by it.

Security Awareness

Security awareness is a key focus that CyberWATCH uses to support its mission of expanding the quality and quantity of the information and network security workforce. Because the consortium is so diverse, it’s been a challenge to implement security awareness initiatives on a consortium wide basis. Many campuses are conducting activities in this area, but we felt it was important for CyberWATCH as a whole to have a presence in this area. So the first Security Awareness Contest, open to all college students, got underway the spring of 2008. The contest solicits security awareness print materials such as posters and brochures. We decided to concentrate on printed materials since Educause, a national organization that is one of our partners, has conducted a security awareness video contest. Actually, Educause is not having a contest again until 2009 and has expressed interest in partnering with CyberWATCH at that time to give students a choice in media of video or printed materials. We will be providing Educause with information about our experience with this contest.

CyberWATCH plans to use the winning materials in an outreach campaign. Students, professors, and others in the consortium will have access to quality handouts designed by students to use in formal and informal presentations concerning computer and network security to various groups. This effort will help raise the profile of cybersecurity and, by extension, spotlight the need for computer security professionals.

Dissemination

Presentations

- Margaret Leary participated in a national-level Community College Homeland Security Curriculum Development Conference April 12 – 14th, 2007, hosted by Pikes Peak Community College in Colorado Springs, Colorado. The conference was sponsored by the Homeland Security and Defense Education Consortium and was attended by approximately 12-15 representatives of Community Colleges with programs in homeland security who discussed the process of curriculum development; challenges associated with obtaining program approval; issues associated with program implementation; lessons learned; and recommendations for curriculum guidelines, options, and minimum core courses and contents.

- Sally Sullivan, Margaret Leary, and Kevin Reed presented a workshop discussion session on "Multiple Perspectives on Developing and Maintaining Faculty Technical Skills" at the 14th National ATE Principal Investigator's Conference in Washington, D.C. October, 2007.

- Vera Zdravkovich, as a part of the panel presentation, discussed CyberWATCH as a model for collaboration at the 14th National ATE Principal Investigator's Conference in Washington, D.C. October, 2007.

- Casey O'Brien participated in a panel at the CISSE conference in Boston, MA (June, 2007), along with Sujeet Shenoi and Erich Spengler. His presentation was titled, "Enriching Community College Information Assurance Curricula Through Student Competitions." It focused on the value of the Mid-Atlantic Regional Collegiate Cyber Defense Competition in the community college student's academic experience.

- Casey O'Brien presented at the 5th Annual C3 Conference at the University of Maryland on October 6, 2006. His session, "Information Security in Today's World" provided an overview of what information security is; the challenges to information security; the latest trends; best practices to help protect your digital assets; the need for Information Security professionals; and CyberWATCH.

- Casey O'Brien spoke to a group of Young Scholars at Joppatowne High School on July 19, 2007 about Career Options and Pathways in Information Assurance and connected the job opportunities with the upcoming MSDE pilot Homeland Security Career and Technology High School Program to begin in the Fall 2007-08 school year.

- Ajay Gupta spoke to a group of Young Scholars at William Wirt Middle School on July 23, 2007 about Career Options and Pathways in Information Assurance and talked about starting a small business in this same field.

- Davina Pruitt-Mentle participated in several state and national level educational technology conferences, including:

  - ➢ Safe Community Coalition's 2nd Annual Cyber Summit, Mclean, VA
  - ➢ National Cyber security Conference, National Press Club, Washington, D.C.
  - ➢ 20th Annual MICCA Conference held April 24 and 25th, 2007 in Baltimore
  - ➢ National NECC Conference held in Atlanta Georgia in June.
  - ➢ C3: Cyberethics, Cybersafety and Cybersecurity – her presentation allowed attendees to learn more about the ethical, legal, safety, and security implications of technology use. Participants also learned how to get more actively involved in the 2008 National Cyber Security Awareness Month Initiative. She also included recruitment materials for the Summer Young Scholars Program, and the Guidance Council workshop. Materials including proceedings from the University of Maryland's 6th annual C3 Conference and the National Cyber Security Alliance Awareness Toolkit were provided.

- Vera Zdravkovich was invited by NSF to discuss CyberWATCH with participants at the NSF Research Meeting in Baltimore in February 2008.

- Vera Zdravkovich and Robert Spear gave a presentation about CyberWATCH at the FISSEA (Federal Information Systems Security Educators' Association) 21st Annual Conference on March 12th in Gaithersburg, MD. As a result Holyoke Community College, MA and Wilmington University, DE expressed interest in becoming partners in CyberWATCH.

- Fred Klappenberger gave a presentation about CyberWATCH at the Committee on National Security Standards (CNSS) in March 2008. As a result a discussion about creation of an IA workforce in collaboration with CyberWATCH and local middle and high schools took place.

- Vera Zdravkovich gave a presentation about CyberWATCH at the annual Federal Office Systems Exposition (FOSE) Conference on April 3, 2008

The following future presentations have been scheduled:

- VCCS New Horizons 2008: Partnerships for Learning Conference, Roanoke, VA April 2008 "Effectively Serving Two Masters: Winning Models for Educator Externships"

- Colloquium for Information Systems Security Education Conference (CISSE), Dallas, TX June 2008

Promotion

- Northern Virginia Community College (NVCC) developed postcards and information DVDs that are being distributed at seminars, workshops, and across NVCC campuses. The DVDs discuss the CyberWATCH mission and include comments from faculty, college administrators, and industry.

- NVCC Workforce Development and Continuing Education showcased and promoted the CyberWATCH program and its network security courses at the Government's Training Officers Conference, a regional workforce training conference, in April 2007. More than 450 government training and human resources personnel doing work with the federal government were in attendance. Approximately 200 individuals stopped to view NVCC's CyberWATCH presentation while 75 individuals asked questions about the program and took away literature. CyberWATCH literature was also distributed at the Veterans Administration Education Fair and the Federally Employed Women's Conference. At both, attendees took CyberWATCH information to give to their human resources departments.
- CyberWATCH has been exhibited at the ATE Conference in Washington, DC in October 2007; at the National Science Foundation Workshop and Exhibition in January 2008; and at the Annual AACC Convention in Philadelphia in April 2008.

Events

- On December 3, 2007 presidents of three community colleges, Anne Arundel Community College, Community College of Baltimore County, and Prince George's Community College signed articulation agreements in Information Security program with University of Maryland University College. Attendees included business/agency representatives from the region.

Publications

- NVCC published articles in its Intercom newsletter about a trip to Oxford related to CyberWATCH and about NVCC's participation in the CCDC.

- White Wolf Security published several pieces about the CCDC on their blog (http://whitewolfsecurity.typepad.com/).

- Casey O'Brien and Tim Rosenberg submitted a paper for the 2008 CISSE Conference titled "The Growth of the Mid-Atlantic CCDC: Public-Private Partnerships at Work" which has been accepted.

Website

NVC Recommendation

Website: *Now that the website is functional, the NVC recommends that a specific planning session be held to map out a strategy for using the site effectively.* (NVC Report, April 2007)

Now that the CyberWATCH Website is up and functioning, emphasis has been placed on using the site as a dissemination tool. For example, the CyberWATCH A.A.S. Model curriculum is posted online. Interested parties can browse the list of courses, prerequisites, modules/lab exercises available for each course, and download syllabi and common course outlines for inclusion in their IA program(s). Reports and newsletters are also available online. In addition to using the site for dissemination purposes, we have also used the site for evaluation purposes by posting links to online Faculty Development evaluation forms, as well as allowing faculty to sign up for workshops online.

Evaluation

The NVC report expressed a few concerns and recommendations regarding future evaluation activities, which were amplified in CyberWATCH's internal NVC Debriefing comments document. These concerns have been addressed to date as follows:

Quantitative statistics for the 2007-08 pre-visit report: Now that CyberWATCH institutions have available quantitative statistics on a full year of course offerings, these can be found in the Evaluation Report.*Program effectiveness measures*: The evaluation plan developed in 2006 contained many effectiveness measures for various CyberWATCH activities; however, most of these measures could not be implemented in previous years because activities had not sufficiently progressed or related data was not available. For this year's report, there are effectiveness measures available for a larger number of programs. In addition, the CyberWATCH project management team discussed how to collect this data as part of its strategic planning process. This discussion contributed to the process of developing and refining related evaluation measures.

The evaluation plan and report format have been revised to include specific indicators for tracking how NVC questions and recommendations have been addressed. This includes advance submission of evaluation documents to the NVC. The strategic planning process also identified steps to assure that project participants take a more active role in integrating evaluation processes into their activities. These included utilizing the CyberWATCH website as another distribution channel for evaluation surveys and data (currently in progress), and forming a working group to identify strategies for gathering post-program outcome data.

New Developments

A CyberWATCH supplemental proposal for the **Digital and Network Forensics Lab (DNFL)** at the University of Maryland College Park (UMCP) has been funded in February 2008 in the amount of $127,818 (Award No. DUE-0749366). The lab will provide a multitude of benefits to CW students and faculty:

- Training of CW faculty in the use of the lab and the use of the Virtually Accessible Case Study Archive
- The use of the DNFL as the test bed for the development of new methodologies and procedures
- The use of DNFL as the location for student forensics exams and for student involvement
- The DNFL will serve as the location for the CW high school forensics competition
- DNFL will provide impetus for the curricular developments in the digital forensics field