2010 NSA/DHS CAE Principals Meeting

CyberEd/K-12

Working Group Session
Final Report

Table of Contents

2010 NSA/DHS CAE Principals Meeting CyberEd/K12 Working Group
14-17 November, 2010

Wrap up Report by Dr. Davina Pruitt-Mentle

I. Introduction

The 2010 Annual NSA/DHS CAE Principals Meeting was held at the Hyatt Regency St. Louis at The Arch on November 14-17, 2010. The first CyberEd/K-12 working group session took place on Tuesday afternoon, November 16, 2010 from 2:00PM – 5:30PM in the Grand Ballroom B. In addition to the main speakers and organizers, 24 participants attended the session, including representatives from 2 and 4 year institutions, K12 and the federal government. The working group session agenda and list of attendees are enclosed at the end of this report. This unclassified event was held under non-attribution rules; hence the report that follows summarizes main points from each panel without reference to persons or affiliation.

II. Discussion Points:

The Internet consists of one network infrastructure that must be maintained and protected. Businesses spend a significant portion of their annual information technology budgets on high-tech computer security. But the dollars spent on firewalls, vaults, bunkers, locks and biometrics can be easily pierced by attackers targeting untrained, uninformed or unmonitored users. Education is key; education for cyberawareness and cybersecurity workforce development. There are several efforts taking place by multiple stakeholders, government, industry, nonprofit, and academia to address Cybersecurity awareness. There are few, although ever increasing in number, efforts underway to address workforce development. At present, each entity operates separately, very few know about each other's efforts and there is limited evaluation on effectiveness.

There is broad consensus that dialogue on K12 Cybersecurity education, formal and informal, is imperative and overdue. Many look for the CAE and CAE2Y to take the initiative, perhaps initially with a small group. However, the CAE and CAE2Y members should also initiate dialogue with other major cybersecurity education efforts, non-profit and industry cyberawareness efforts, academic projects and formal high school Career Technology Education tracks (CTE). Multilateral discussions on successful activities and metrics will provide open and real-time understanding of cybereducation for the general citizenry and for career development.

The first requirement when seeking to coalesce cybersecurity education is the recognition that spoken and written words form the foundation of our understanding of cybereducation. As such we need to come up with clear definitions of terms if effective collaborations are to exist. We also need a common lexicon and broader understanding of what constitutes cybersecurity education.

The CAE/CAE2Y community needs to federate monitoring efforts not just among members but also across the public-private divide. By sharing operational information and working in close coordination, such federations will more effectively leverage the tools they have to impact recruitment and retention to cybersecurity careers. Collaboration can also have related positive effects on other efforts generally; a good example being Regional ATE Centers sharing existing K-12 Cybersecurity curriculum, groups and projects, which has already fostered cross-site collaboration of K12 Cybersecurity stakeholders. In order to properly do monitoring, we need to have a trained workforce which begins in K-12 and continues through higher education. The working group members shared that a variety of items in this area can be characterized to specific types.

There are eight general categories of existing cybersecurity education activities – summer camps, cyber defense and related competitions, after school/out of school clubs and programs, in school programs or extension units, cybersecurity content injection modules, cybersecurity content across the curriculum, special events and formal CTE tracks and pathways.

A multitude of programs are being created within these categories, but there is no mechanism to share these programs with others. Additionally, there are many existing efforts to recruit and retain students in other STEM fields. Becoming aware of these programs is critical to designing high impact programs. There are decades of well established work already implemented and documented, and community would be remiss if they did not explore the existing scholarly work already done in this area. In addition, existing standards and STEM related organizations have well established and research supported efforts that the community can learn from and/leverage for their own benefit. Meshing the National STEM Agenda with the National Initiative for Cybersecurity Education Strategic Plan can further incentivize close cooperation and cybersecurity advances. Collaboration among existing K12 organizations and programs can work from the outside in to get the larger K12 community to embrace cyber security content. This includes embracing cybersecurity topics within cyberawareness efforts, reinterpreting existing standards to address cybersecurity topics, and building upon the formal CTE and Programs of Study.

Another important step is the development of program knowledge awareness in understanding where programs of study are housed and what skill sets are needed upon entry into the programs whether two or four year.

III. Key Ideas:

Discussion has started around the possible development of a set of K12 standards to address Cybersecurity education. The efforts neglect to explore the existing standards at both the technological level and the educational technological level, in addition to new sets of media literacy and 21st century skills. Participants agreed yet another set of standards is not the path to take. Standards take several years to develop and even longer to pilot, edit, test and then adopt, not to mention by the time they are ready for implementation they are outdated. Three groups, the computer science, technology and engineering fields have developed standards which while making small inroads in local locations have been aggressively blocked by the K12 educational community. A promising alternative approach would be to develop content that addresses existing

standards in content areas and focus efforts toward reinterpretation of existing technology related standards to help states better define Cybersecurity skills needed by all students. In addition, several states, usually in partnership with higher education institutions (many CAE/CAE2Y) have already designed their student technology standard competencies and outcomes (to meet the NCLB mandate to have students technologically literate by 8th grade) to include Cybersecurity awareness and skills.

There are existing programs, activities, articulations and competitions that are ready for wider distribution. There is a need to share these materials and resources. The CAE application requirement requires evidence of outreach efforts and many scholarship for service grants are awarded with K12 elements. Unfortunately, few know what they are, if, or what metrics are used to determine success, what successes have been documented and what impact would come about if distributed to a wider audience. There is a need to archive this information for others to examine and learn from so we are not continually reinventing the wheel.

Besides programs and competitions there is a real dilemma in reaching parents, students, educators and the broader general public regarding what Cybersecurity is, what careers it entails, and what pathways are available. Even a quick search of CAE institutions reveals little to the lay person (or even those in the working group with experience) in terms of what school or departments the CAE/CAE2Y programs are housed in, what degree programs or certificates are offered, what courses are required within their programs and what articulations are in place. In order to attract students to this burgeoning career, we must define and explain the multiple pathways to students, educators and parents.

IV. Conclusions and Recommendations

This first NSA/DHS CAE PI working group session focused on the three Regional ATE centers sharing programs, projects, competitions, articulations and other events that their membership was involved in. This provided a means to start closing the knowledge gap. This is a useful model for the future, and we recommend future CyberEd/K12 working sessions. We also recognize the existing work with other K12 working groups;

CISSE and CACE, and will work to align efforts so that we can “share the workload,” support each other’s efforts, minimize duplication, and gather information from a larger and broader audience.

There is a large gap in members’ understanding of what is taking place across the US related to cybereducation; cyberawareness and Cybersecurity workforce development. There is a need for higher education partners to learn more about existing research related to the K12 arena in areas such as STEM recruitment and retention, and attracting more women and minorities to STEM fields. There is also a need to share existing K12 standards related to technology skills.

The concerted effort made to hear perspectives from multiple stakeholders such as CAE, CAER, CAE2Y, K12 and the federal space paid off and was welcome by all participants. We should build on this experience to start a dialogue that can inform U.S. policy makers.

V. Panel Highlights

Spotlight 1 – Cyber Security Education Consortium (CSEC): Sheryl Hale

The Cyber Security Education Consortium is a National Science Foundation ATE Regional Center dedicated to building an information security workforce. CSEC incorporates five key entities: Oklahoma's Career and Technology Education System, three of Oklahoma's largest two-year colleges (Oklahoma City Community College, Oklahoma State University-Okmulgee, and Rose State College); and the University of Tulsa, an NSA-designated national faculty development center, which serves as the principal training provider and mentor to the two-year institutions.

Oklahoma has adopted the National 16 Career Clusters Model and believes that Career Clusters offer many benefits and should be used as a basis for high school reform. The state views Career Clusters as an infrastructure for a seamless educational transition between all learner levels. Career Clusters are also seen as a tool for career guidance,

a structure to organize instruction around, a way to align Workforce and Economic development, and as an overall means to improving the quality of CTE.

In order to effectively implement Career Clusters, Oklahoma has integrated Career Clusters into the state plan and adopted a strategic vision paper that supports Career Clusters. In addition, the state is incorporating the Governor's Council on Workforce and Economic Development. Numerous strategies have been used to support the implementation of Career Clusters. For example, Oklahoma has used them to support effective transitions between secondary and postsecondary education. In addition the state has required local Perkins plans to incorporate Career Clusters, and for accountability information to be collected by Career Clusters. Finally, the state benchmarks existing program standards against Career Cluster knowledge and skill statements, redirects state resources and personnel, and sponsors pilot sites.

Several delivery methods are being used to implement Career Clusters, including career academies, High Schools That Work, and Tech Prep.Oklahoma offers dual enrollment, concurrent/transcripted credit, and Alliance College Credit to ease the transition from secondary to postsecondary.

Oklahoma has statewide articulation agreements in the following clusters:

- 15 of the 16 clusters
- Oklahoma has Alliance Agreements between all shared time technology centers and community colleges in 15 of the 16 Career Clusters

As part of the Cooperative Alliance Project, some higher education institutions, in partnership with Oklahoma's career technology centers, have been approved to allow high school students to enroll in technical programs and courses under separate admission standards. This allows an 11th- or 12th-grade student enrolled in an accredited high school or a student who is at least 16 years of age and receiving high school-level instruction at home or from an unaccredited high school to be admitted to a college or university in the Oklahoma State System of Higher Education that offers technical AAS and certificate programs and enrolled in technical courses only. Students must meet the following standards:

Regional Universities and Community Colleges

Option 1 - ACT: 19

Option 2 - ACT PLAN: 15

Option 3 - High School GPA: 2.5

(The required ACT score is the composite score without the writing component.)
In addition to meeting the requirements above, students must provide a letter of support from the high school counselor and written permission from a parent or legal guardian. All other concurrent admission policy requirements remain in effect for technical students, including retention standards.

Alliance partners must establish joint student services such as financial aid and academic advisement, and must develop a business plan that includes guidelines for resource allocations, personnel needs, a joint marketing plan for their alliance project, etc. Partners must identify and report performance measures that result from their alliance, and establish shared goals for expansion of offerings. Partners must also align agreements to support a statewide transfer matrix being developed.

http://cteworks.careertech.org/state-profile/details/oklahoma

http://www.okcareertech.org/alliances/index.htm

Sheryl also provided the recommendation to allow a non-degree granting entity become a CAE, such as Oklahoma Career Tech.

Spotlight 2 –Center for Systems Security and Information Assurance (CSSIA): John Sands

The Center for Systems Security and Information Assurance (CSSIA) is a Regional Advanced Technological Education (ATE) Center for Cyber Security and Information Assurance led by Moraine Valley Community College in Palos Hills, IL .

CSSIA advances Cyber Security education programs at the secondary and post-secondary levels by providing innovative teaching and learning opportunities through

skills based student competitions and faculty professional development. Skills based competitions promote problem solving and teamwork skills, provide an opportunity for students to showcase their talents, and offer a unique opportunity for students and faculty to interact with Cyber Security professionals.

CSSIA has developed a successful model for partnering with industry and academia in developing and operating innovative skills based competitions. These competitions result in program improvements and support the capacity building necessary to meet the critical national need for Cyber Security technicians.

CSSIA supports a number of K12 outreach events and programs to include:

- GirlTech
    - Madison Area Technical Collge
    - Moraine Valley Community College
- Geek University (Geek-U)
    - Inver Hills Community College
- Technology Fridays and LAN101
    - Moraine Valley Community College
- Community Computer Health Fair
    - Moraine Valley Community College
- We are IT (Sponsor-Ohio)
    - Rhodes State College
    - Owens Community College

Girl Tech is a Summer Camp targeting incoming 6^{th} -9^{th} grade girls, and includes 3 full days of technology related careers to include: Wireless, Animation, Welding, Robotics, Law Enforcement and Auto Mechanics.

The Geek University program is designed to delivery content to high school students by using equipment, classrooms/labs and community college faculty, through a summer introduction awareness course followed by two, eight week courses that meet twice a week. The courses are as follows:

Computer Geek U (awareness)		
This course provides an excellent intro to the IT industry and interactive exposure to personal computers, hardware, and operating systems. Individuals participate in hands-on activities and lab-based learning to become familiar with various hardware and software components and discover best practices in maintenance and safety.	4 days	9:00-3:00 PM (M-TH)
Basic Computer Technology I		
The PC Hardware & Software Course provides a comprehensive overview of computer fundamentals and an introduction to advanced concepts. It allows individuals to gain practical knowledge on how computer works. Individuals who complete this course will be able to describe the internal components of a computer, assemble a computer system, install an operating system, and troubleshoot using system tools and diagnostic software. This will also be to connect computers to the internet and share resources in a networked environment. Chapters 1-10 cover the following skills & competencies: • Core competencies in the latest hardware and software technologies information security skills • Safety and environmental issues • Soft skills for career development	35 hrs 2 days per week	3:30-5:30 PM 8 weeks
Basic Computer Technology II		
The PC Hardware & Software Course will help individuals prepare for entry level IT positions within various environments. It will also help individuals develop greater skills and confidence in working with desktop and laptop computers. In addition, PC hardware and software covers the following new topics: Laptops and portable devices, wireless connectivity, security. Safety and environmental issues and communication skills. Chapters 11-16 cover the following skills and competencies: • Advanced troubleshooting skills • Prepare for all three CompTIA job environments certification exams • Advanced installation of computers, peripheral devices, networks and security components	35 hrs 2 days per week	3:30-5:30 PM 8 weeks

CSSIA also supports a GenSys high school outreach program that includes an intensive summer program, followed by one-year internships with Chicago area concerns (banks, hospitals, etc.). In addition, CSSIA supports several defense type competitions and activities to include:

- NetRiders – HS competition, w/ mentors. Sponsored by Cisco,
- WILAs – Web-based Immersive Learning Activities. Build a library of 40 WILAs, incl IA exercises, using Web 2.0,
- High School Network Security Competition designed to promote problem solving, critical thinking, and teamwork skills, showcase student talents, interact with Cyber Security professionals, and help promote information technology and network security programs. The competition has been designed to test students' knowledge, critical thinking skills, and trouble-shooting skills. This is accomplished through a three-part structure:
    - Part I is comprised of a quiz bowl in which students have 30 minutes to complete 50 web-based questions.
    - Part II is a project in which students have 45 minutes to demonstrate their ability to design and configure 12 course skills in network security using the simulation software, Cisco's Packet Tracer.
    - Part III is a trouble-shooting exercise where students solve problems in a virtual environment, NetLabs.

http://cssia.org/
http://cae2y.morainevalley.edu/Compete/index.htm

Spotlight 3 – CyberWatch (CW)/ CyberWatch K12 Division: Davina Pruitt-Mentle

ETPRO extends the CW mission to the K-12 community addressing four primary goals. These include increasing: the Cybersecurity workforce pipeline, community awareness of Cybersecurity workforce needs, community awareness of Cyberethics, safety and security, and security of K-12 IT systems. ETPRO has created a robust cybersecurity program for K-12 students through the following:

- Expanded its STEM programs to address Cybersecurity pathways through its *Mindtools* and *CyberSTEM* after school and extension unit activities. Creating content in partnership with MSDE to embed within the state curriculum subjects and Common Core.
- Developing a CyberSecurity CTE track and Program of Study based on CW coursework with articulations between high schools and CW member institutions.
- Originated, developed and presents the *Annual Careers in Cybersecurity Workshop for Guidance Counselors and STEM Coordinators* and developed a tool kit allowing other states to replicate.
- Originated, developed and presents the *Annual Cool Careers in Cybersecurity for Girls Summit*, hosting 450+ middle school girls. The full day of interactive digital crime solving activities allow girls to learn from women in diverse companies and agencies about what it takes to navigate the professional pipeline in the field of Cybersecurity, and other science, technology, engineering, and mathematics (STEM) fields.
- Originated, developed and presents the *Annual Cyberethics, Cybersafety and Cybersecurity (C3) Conference*—now in its 10th year with over 500 educators in attendance. The *Annual C3 Conference* unites educators, industry, government, non-profits, and students for a two day event held at the University of Maryland, College Park and delivers information about both established and new programs, best practices, awareness issues, and individual perspective on Cyberethics, Cybersafety, and Cybersecurity. In 2011, the Day 2 event served as a DHS STOP THINK CONNECT Citizen Forum.
- Developed the HS model curriculum and delivery for the USCC HS Summer Cyber Camp.
- Developed the high school shadowing and expo in conjunction with the Mid Atlantic CCDC.
- Serve as the regional rep for CSSIA's National High School Network Security Competition.

- Work in collaboration with MSDE to develop an online Cybersecurity technology literacy course to meet MD state tech HS graduation requirements.
- In collaboration with MSDE and the MD Society of Educational Technology (MSET), developed an online toolkit related to C3 topics distributed to all 2700 public school administrators.
- In collaboration with MSDE and MSET developed an online PD module related to C3 topics distributed to all 8700 MD educators.
- Developed an online C3 course with PGCPS for MSDE CEU credit approval.

http://www.cyberwatchcenter.org/

http://www.edtechpolicy.org/cyberk12/index.html

Appendix A: Agenda

CyberEd/K-12

Tuesday, November 16, 2010
2:00PM – 5:30PM
Grand Ballroom B

Overview

Currently, several K12 Cybersecurity efforts throughout the country are starting to appear. Unfortunately, there are few possibilities to share programs or collaborate on existing efforts. In addition, as addressed at the 2009 CISSE conference, while much effort has gone into Cybersecurity education "awareness" programs, only limited activities have been dedicated to advancing strategies and programs that recruit and retain students to the Cybersecurity workforce.

A K-12 Working Group will allow CAE members throughout the country to come together to share ideas and brainstorm collaborative projects with a common focus: *Create a Competent Cybersecurity Workforce for the Digital Age.*

Objectives

Our working group session is designed to meet five objectives:

(1) Learn about other K-12 Cybersecurity curriculum, groups and projects,

(2) Foster cross-site collaboration of K12 Cybersecurity stakeholders,

(3) Synthesize current programs and gap analysis (if any)

(4) Develop consensus regarding key findings and recommendations about

- The key issues, concepts, and constraints
- The most promising strategies and practices

- Recommended success measures

(5) Develop consensus regarding recommendations and next steps for possible best practices of local and national initiatives

Desired Outcomes

By the end of the session participants will have:

- Received updates regarding existing programs, projects and activities (or those in development)
- Developed a scheme of current programs and gap analysis (if any)
- Developed a consensus regarding key findings and recommendations about
  - The key issues, concepts, and constraints
  - The most promising strategies and practices
  - Recommended success measures
- Developed consensus regarding recommendations for possible best practices or local and national initiatives, and
- Identified and finalized recommendations for the NSA/DHS Principals Meeting K-12 Working Group Report

Tentative Schedule

2:00 PM	**Session Opens / Overview / Introductions**
2:15 PM	**Panel Discussions – Existing Programs**
2:45 PM	**Group/Table Discussions**
3:30 PM	**Group/Table Synthesis-Top 5 recommendations for each question**
3:45 PM	**BREAK**
4:00 PM	**Topic Report Outs to the Room**
4:30 PM	**Next Steps/Summary/Adjourn**
5:00 PM	**Creation of WG Slide presentation**

PLEASE make sure you sign the attendee sheet. The sheet will be located either in the back of the room or near the room moderator

Appendix B: Attendee List

First	Last	Affiliation
Luc	Longpre	UTEP
Tom	Candon	Dartmouth
Felicia	White	DoD CIO
Joyce	France	DoD CIO
Christine	White	NSA
Deborah	Penna	AACC
April	Tinson	DoD/NSA
Amita	Richmond	DoD/NSA
Deborah	Curry	NSA/ADET
Murray	Kenyon	DoD/NSA
Jill	Newton	NSA
Efstratios	Gavas	NYU-Poly
Dan	Stein	DHS
Lisa	Houck	DoD
Sarah	North	SPSU
Mark	Schmidt	St Cloud State
Jonathan	Graham	NSU
Alfredo	Cruz	PUPR
Carolyn	Tancocl	DoD
Al	Heitkamper	Oklahoma City CC
Sheryl	Hale	Oklahoma Dept of Career Tech
Brett	Landry	Univ of Dallas
John	Sands	CSSIA
Davina	Pruitt-Mentle	ETPRO/CW