Criteria For Measurement
Revised October 2009

National Centers of Academic Excellence in Information Assurance Education - Two Year (CAE2Y)

Applicant Submission
from
Anne Arundel Community College

Section 1 | Section 2 | Section 3 | Section 4 | Section 5 | Section 6

The National Information Assurance Education & Training Centers of Excellence Two Year program is open to nationally or regionally accredited 2-year Community Colleges or technical schools. The mission of the nationally accredited institution must be in the Information Assurance (IA) and/or Cyber education arena. Applications must be submitted electronically via the online application process. Applications are assessed against criteria, listed below, which are intended to measure the depth and maturity of programs of instruction in IA/Cyber education and training. Applicants must clearly demonstrate how they meet each of the six criteria. Minimum requirements for each of the criteria must be met in order to obtain designation. Successful applicants are designated as a National IA Education and Training Center of Excellence for a period of 5 years academic years, after which they must successfully reapply in order to retain the designation. The criteria is reviewed annually and strengthened as appropriate to keep pace with the evolving nature of IA/Cyber. (*Designation of National IA Education and Training Center of Excellence does not carry a commitment of funding from the National Security Agency or from the Department of Homeland Security*.)

Provide a link to the letter that was mailed to the NSA Program Office stating intent to apply for the CAE2Y program, verifying status as a 2-year institution, and providing evidence of national or regional accreditation. (You will be able to add the link just before formal submission after the 'Prepare for review' button is selected.)

http://

(There is a requirement that a letter of intent on official institution letterhead, signed at an appropriate level (Dean or higher), and a verifying the 2-year status and national or regional accreditation of the school must be mailed to the NSA Program Office prior to the due date for the CAE2Y application.) The mailing address follows:
National Security Agency
Attn: Ms. Christine Nickell
9800 Savage Rd., SAB3, Suite 6744
Ft. Meade, MD 20755-6744

Prerequisite: ***Prior to submitting an application for the National Centers of Academic Excellence in IA Education Program, IA courseware must be certified under the IA***

Courseware Evaluation Program (http://www.nsa.gov/ia/academia/iace.cfm?MenuID=10.1.1.1) as meeting the Committee on National Security Systems (CNSS) Training Standards (http://www.cnss.gov) and the certification must be current. Specifically, certification for CNSS Training Standard 4011 is required, and certification of at least one additional CNSS Training Standard (4012, 4013, 4014, 4015, 4016 or subsequent standards) is required.

Verify that your university has met the CAE2Y Program prerequisite by identifying the CNSS Training Standards to which you have mapped and the date of certification for each standard. (You will be able to add/update this information just before formal submission after the 'Prepare for review' button is selected.)

Standard	Date of Certification (mm/dd/yyyy)

1. *IA Partnerships:* Extending IA beyond the normal boundaries of the College/Institution and bringing current IA practitioners into the IA Center. Provide evidence of partnerships in IA education with 4-year schools, other Community Colleges, Two-Year Technical schools, K-12 schools, Industry Schools, Government Schools, Federal/State Agencies, Business, Industry or Non profit organizations. Evidence must be in the form of an articulation agreement, Memorandum of Agreement, letters of endorsement, etc. between the schools. Articulation Agreements must be specific to IA programs. Partnership(s) may include: Shared curriculum and resources (IA teaching materials provided); shared faculty (faculty on curriculum committee for more than one institution); and reciprocity of credits.
Overall Point Value: 10 minimum/20 maximum

a. Shared Curriculum (e.g., IA teaching materials provided to technical schools, universities, community colleges, K-12 schools, etc.)
Point Value: Up to 5 points

SUBMISSION:
Thank you for considering the Anne Arundel Community College (AACC) application to become a Center for Academic Excellence.
Letter of Application:
http://ola2.aacc.edu/CAEDocs1/CAELetterOfApplication.pdf

Secure elements of our application are in an ANGEL course entitled Center for Academic Excellence. To access this course, please use the following information.
Link: **[LINK REMOVED FOR CONFIDENTIALITY]**
LoginID: **[LOGINID REMOVED FOR CONFIDENTIALITY]**
Password: **[PASSWORD REMOVED FOR CONFIDENTIALITY]**

The Committee on National Security Systems and the National Security Agency have certified that Anne Arundel Community College meets the national standard for NSTISSI NO. 4011 and NSTISSI NO. 4013. See: http://www.nsa.gov/ia/academic_outreach/iace_program/iace_certified_institutions.shtml#md and for mapping, see:
http://www.aacc.edu/computertech/cis_infosec.cfm
Dates of notification of successful mapping:
4011 - re-certification notification - February 9, 2009 (valid through June 2014)
4013 - certification notification - April 20, 2008

Anne Arundel Community College is accredited by the Middle States Commission on Higher Education, 3624 Market Street, Philadelphia, Pa. 19104 (215-662-5606) and approved by the Maryland Higher Education Commission. See: http://www.aacc.edu/catalog/interactivecatalog/CollegeCatalog2009-2010_Color_001.htm

****

Anne Arundel Community College's (AACC) commitment to Information Assurance (IA) has always extended beyond academic classes. One aspect of this commitment is reflected in our IA education partnerships. AACC has forged multiple partnerships, as reflected by our articulation agreements, with K-12 school systems, community colleges, 4-year colleges and universities, as well as with non-profit organizations. In this response, you will find multiple links to articulations agreements at the K-12 level as well as the 4-year school level.

Another aspect of our commitment to Information Assurance has been our development and sharing of IA curriculum since 2005 on regional and national levels through CyberWATCH. First we will present evidence concerning our IA partnerships, then we will present links documenting our shared curriculum.

At the K-12 level, Anne Arundel Community College (AACC) has IA partnerships established through Program Pathways with the Anne Arundel County Public School (AACPS) System. By participating in this program, any Anne Arundel County Public School student can articulate credits toward AACC's Information Systems Security A.A.S. degree or an AACC Information Systems Security certificate.

More information concerning the AACPS to AACC Program Pathways, can be found at:
http://www.aacc.edu/techprep/CompNetwrkngTech.cfm

Articulation agreements between Anne Arundel County Public School System and Anne Arundel Community College can be viewed at:
https://www.aacc.edu/techprep/file/ComputerNetworkingTechnology%2009-10.pdf
and
http://www.aacc.edu/techprep/file/ComputerNetworkingTechnology.pdf
and
https://www.aacc.edu/techprep/file/AcademyofInfoTech%2009-10.pdf

At the 4-year school level, AACC has IA education articulation agreements with multiple institutions, including Capitol College, Strayer University, Towson University, the University of Baltimore, and the University of Maryland. These signed articulation agreements can be seen at:
http://www.aacc.edu/transfer/programspathway2.cfm

At the regional and national levels, AACC is a founding member of CyberWATCH which is an Advanced Technological Education (ATE) Center originally funded by the National Science Foundation. In CyberWATCH, AACC works in partnership with 36 member institutions including 23 community colleges and 13 universities. See:
http://cyberwatchcenter.org/index.php?option=com_content&view=article&id=50&Itemid=29
You may use the login id **[LOGINID & PASSWORD REMOVED FOR CONFIDENTIALITY]**

To document AACC's leading role in IA curriculum development and the college's efforts to share the curriculum within CyberWATCH, see: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CyberWatchProjectFUndedNov2005.pdf

The CyberWATCH Information Assurance degree and certificate are modeled on the Anne Arundel Community College programs approved by Maryland Higher Education Commission in academic year (AY) 2004-2005. Evidence of this early approval by the Maryland Higher Education Commission is provided in the AACC Fiscal Year 2005 Report to the Community http://ola2.aacc.edu/CAEDocs1/Support%20Documents/aaccannualreport0506.pdf#page=15. In the first CyberWATCH newsletter, Dr. Vera ZDravkovick a Principal Investigator for the NSF CyberWATCH grant, acknowledges the curriculum leadership role held by AACC stating "Anne Arundel Community College, the lead institution in curriculum development, hosted a Curriculum Kick Off to introduce the partner community colleges to the National Security Agency's 4011 IA standards." See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CyberWATCHvol1_issue1-2.pdf

---

b. Shared Faculty (e.g., Faculty on curriculum development committee for more than one institution)

Point Value: Up to 5 points

SUBMISSION:

Sharing AACC IA faculty and curriculum with CyberWATCH and other institutions represents a significant IA curriculum contribution. In this sharing, AACC has collaborated with other educational institutions as well as with governmental agencies such as the NSA.

One example of this collaboration took place in 2005 when AACC hosted the "Curriculum Kick-Off" that introduced CyberWATCH partners to the NSTISSI 4011 Information Assurance Training Standard and Anne Arundel Community College's MHEC approved Information Systems Security associate degree curriculum. At the Kick-Off, the NSA's Lynn Hathaway was a featured speaker. For further information concerning the curriculum Kick-Off at AACC, see the CyberWATCH newsletter referenced earlier at: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CyberWATCHvol1_issue1-2.pdf

As noted in the previously cited, CyberWATCH Newsletter, AACC's Professor Fred Klappenberger, a co-Principal Investigator for the NSF CyberWATCH grant, provided CyberWATCH with leadership in IA curriculum development. As chair of CyberWatch's curriculum committee, AACC's Professor Klappenberger shared the AACC MHEC approved Information Systems Security associate degree curriculum and led CyberWatch's Model IA curriculum program efforts.

In addition, AACC's curriculum sharing has been cited by CyberWatch's National Visiting Committee (NVC). In specific, the Volume 1, Issue III, CyberWatch Newsletter states:
"With regard to the curriculum development, the NVC stated "The adoption includes mapping the course content to NSA's 4011 standard. Of note is the development of a state-wide articulation of the IA degree program, benefiting all schools that adopt/adapt the [Anne Arundel Community College] curriculum."
The newsletter can be viewed here:
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CyberWATCHvol1_issue3.pdf

AACC's and Professor Klappenberger's IA curriculum has been recognized by the League for Innovation in the Community College. Specifically, in 2007, the League recognized AACC's Information Systems Security Program with an "Innovation of the Year" award. See: http://www.league.org/league/competitions/innovations/display2007.cfm#486

AACC shares its full-time faculty with multiple other educational institutions. Specific examples include:
[FACULTY INFORMATION REMOVED FOR CONFIDENTIALITY]

---

c. Use of distance education technology and techniques to deliver IA courses. (Distance education includes live/delayed broadcasts, videotapes/CDs, lectures, and web-based IA courses.)
Point Value: Up to 5 points

SUBMISSION:
The AACC Information Systems Security programs and courses utilize distance education technologies to facilitate traditional (face-to-face), hybrid, and online IA courses. These technologies include: 1. IA course-specific support technologies, 2. learning management systems technologies, and 3. commercially available hardware and software tools to assist faculty and students with learning and communicating in distance learning environments.

All of the IA required and elective courses are offered in the face-to-face format. Many are also offered in hybrid (approximately 50% online and 50% face-to-face) and/or online formats. The IA faculty have been proactive and innovative in rolling out hybrid and online versions of IA courses when quality and student success could be maintained. In the Fall 2009 semester, AACC offered the first two Cisco networking courses as online courses. This decision was made once Cisco could provide sophisticated simulation software to ensure the quality of learning. The courses filled very quickly this spring. The next two Cisco courses and the
CSI 270 Information Security Capstone (CISSP prep) course will be offered online beginning Fall 2010.

This list of required IA courses for the IA degree and certificate indicates which courses are offered in hybrid and/or online formats. Links to course descriptions can be found at http://www.aacc.edu/computertech/cae.cfm.
CSI 113 Introduction to Computers (hybrid, online)
CSI 130 Microcomputer Operating Systems (hybrid, online)
CSI 157 Networking 1 (hybrid, online)
CSI 158 Networking 2 (hybrid, online)
CSI 194 Ethics and the Information Age (online)
CSI 257 Networking 3 (hybrid; will be offered online Fall 2010)
CSI 258 Networking 4 (hybrid; will be offered online Fall 2010)
CSI 165 Network Security Fundamentals
CSI 194 Ethics and the Information Age (online)
CSI 217 Hardening the Infrastructure
CSI 219 Network Defense and Countermeasures
CSI 265 Windows 2003 Server
CSI 270 Information Security Capstone (will be offered online Fall 2010)

This list of elective IA courses for the IA degree and certificate indicates which courses are offered in hybrid and/or online formats. Links to course descriptions can be found at http://www.aacc.edu/computertech/cae.cfm.
CSI 135 Introduction to UNIX/LINUX (online)
CSI 207 Cyber Forensics

CSI 214 Information Systems Security (online)
CSI 266 Windows 2003 Networking
CSI 269 Wireless LANs
EET 160 Theory and Troubleshooting Microcomputers 1

IA Course-Specific Support Technologies:
AACC incorporates Cisco's Packet Tracer
http://www.cisco.com/web/learning/netacad/course_catalog/PacketTracer.html
technology in delivering online course content and assessments in its traditional, hybrid, and online Networking 1-4 courses (CSI 157, CSI 158, CSI 257, and CSI 258). Cisco's website describes Packet Tracer as "… a powerful network simulation program that allows students to experiment with network behavior and ask 'what if' questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities and facilitates the teaching and learning of complex technology concepts." Screenshots of PacketTracer exercises from the Cisco courses are included for review.
http://ola2.aacc.edu/CAEDocs1/DistanceLearning/CCNA4ver4practiceskillsassessment.pdf and
http://ola2.aacc.edu/CAEDocs1/DistanceLearning/Cisco%20curriculum%20Packet%20Tracer%20exercises.pdf.

To deliver and support its online, hybrid, and web-based offerings, AACC uses the ANGEL Learning Management System (LMS). This full-featured LMS incorporates content management, communication, assessment, reporting, and outcomes management. Because ANGEL can be used to make so many resources available to students, many of the IA instructors choose to offer their face-to-face courses as web-based courses within ANGEL, meaning that students meet in a classroom for class and have access to their course materials, resources, and grade book wherever they have access to the Internet. All faculty must complete training before teaching hybrid and online classes. Additional training is required for faculty who wish to develop hybrid and online classes.

Audio and screencapture tools are used by many of the ISS hybrid and online faculty to share course content and instructions with their students. The following link from CSI 194 Ethics and the Information Age, a required course in the ISS curriculum, features the use of Jing, a free audio and screencapture tool. This particular video provides students with an overview of the ANGEL LMS resources such as milestones, calendar, grade reports, and discussion tools and provides insight on how the LMS supports distance learners. http://ola2.aacc.edu/CAEDocs1/DistanceLearning/ANGEL.swf
Wikis are used in the distance learning courses to promote research, collaboration, and discussion.
http://ola2.aacc.edu/CAEDocs1/DistanceLearning/wikiCSI%20194%20Ethics%20and%20the%20Information%20Age.pdf

The following link contains screenshots from CSI 214 Information Systems Security. It shows the organization of content by week including the weekly lecture, assignment, quiz, and discussion. Discussion is an important part of learning and it is an integral component in the ISS distance learning courses.
http://ola2.aacc.edu/CAEDocs1/DistanceLearning/CSI%20214%20InformationSystemSecurityPDerdul%20Chapters.pdf

Narrated PowerPoint shows are used in hybrid and online classes to assist IA

distance learning students. The following is an example of narrated PowerPoints to assist students in the online CSI 157 Networking 1 course. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/LearningAidsNetworking1GettingStarted.pps

Additional examples of distance learning materials are available upon request.

Effective Fall 2009, all new AACC hybrid and online courses, including the IA courses, must meet the 17 essential Quality Matters (QM) standards. "Quality Matters (QM) is a national, faculty-centered, peer review process designed to certify the quality of online courses and online components." http://www.qualitymatters.org/. Two-thirds of the Computer Technologies faculty have completed "Applying the QM Rubric Training" and seven are certified QM Peer Reviewers. The following IA courses are currently under informal review for meeting the 17 essential QM standards: CSI 194 Ethics and the Information Age, CSI 157 Networking 1, and CSI 158 Networking 2.

---

d. Evidence the program is providing students with access to IA practitioners (Example: guest lecturers working in IA industry, government, faculty exchange program with industry and/or government, etc.)
Point Value: Up to 5 points

SUBMISSION:
AACC provides students with ongoing and consistent access to working IA professionals. This is accomplished through: 1. special one semester contracts with working IA practitioners, 2. a large pool of IA practitioners teaching IA courses as adjuncts, 3. a strong IA full-time faculty, 4. IA guests of the college, and 5. an internship program that places IA students in mentored IA positions.

The college has an innovative special contracts program that brings industry and government IA practitioners to campus for a minimum of 12 faculty load hours for a single semester to perform a variety of functions including teaching, advising, and curriculum development. These contracts provide our IA students and our IA faculty with more intensive interactions with IA practitioners than simple adjunct teaching contracts.

[INSTRUCTOR INFORMATION REMOVED FOR CONFIDENTIALITY]

Of the 28 full-time faulty in the Computer Technologies Department, several have extensive IA industry experience.
[FACULTY INFORMATION REMOVED FOR CONFIDENTIALITY]

Faculty curriculum vitae are provided in section 5b of this application (in the ANGEL CAE course section 5 **[LINK REMOVED FOR CONFIDENTIALITY]**

Each semester the college relies upon a group of ten or more IA practitioners to teach as adjuncts to bring critical real world experiences to our IA students. These include:
[FACULTY INFORMATION REMOVED FOR CONFIDENTIALITY]

A more complete list and faculty curriculum vitae are provided in section 5b of this application (in the ANGEL CAE course section 5 **[LINK REMOVED FOR CONFIDENTIALITY]**).

The department regularly holds events to enable IA students to interact with

IA practitioners. One previously cited example was the presentation by the NSA's Lynn Hathaway at the 2005 Curriculum Kick off as documented at: http://www.cyberwatchcenter.org/index.php?option=com_docman&task=doc_download&gid=2&Itemid=87
An example of a recruiting event held at AACC is the one held in conjunction with Cisco Partners. As a result of this event, one of our IA students was hired by Chesapeake Netcraftsman and she is now a regular adjunct for the IA program. In preparation for the recruitment, our jobs placement coordinator and IA faculty worked on resume writing and 1 minute interview skills with our IA students.
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/Section1d_CiscoNetworkRecruitment.jpg

Another way that AACC provides students with access to IA practitioners is through mentored internships. The college, through its STEM initiatives, has launched an internship program focused on supporting STEM internships. This program has placed IA students in internships with companies such as Booz Allen Hamilton, Eagle Alliance, Maryland Legal Aid, and DISA. Additional information is available in the ANGEL CAE course section 1d **[LINK REMOVED FOR CONFIDENTIALITY]**

Back to top

2. *IA Student Development:* The program provides development opportunities for students that lead to a two year associate's degree or a certificate in an IA discipline.
Overall Point Value: 14 minimum/28 maximum

a. Evidence of IA degrees/areas of study/track or certificates (For example: List of IA Associates degrees and/or certificates in IA curriculum as listed on the institution's website or catalog, list of all IA program courses with their descriptions).
Point Value: 5 points

SUBMISSION:
AACC's Associate of Applied Science Degree in Information Systems Security (AAS.CIS.ISS)
http://www.aacc.edu/catalog/interactivecatalog/CollegeCatalog2009-2010_Color_100.htm
and 40-credit Certificate in Information Systems Security (CRT.CIS.ISS)
http://www.aacc.edu/catalog/interactivecatalog/CollegeCatalog2009-2010_Color_105.htm
are detailed in the college catalog along with descriptions of each course.

AACC is a leader in the development of community college IA curriculum; making it available to its students since academic year (AY) 2005. The AACC ISS curriculum was one of the first community college IA programs to be approved and offered, and the very first community college program in the nation to map to the 4011 standard http://www.crime-research.org/news/2003/04/Mess1401.html. In 2007, the League for Innovation recognized the AACC ISS curriculum for its innovation in workforce preparation and development
http://www.league.org/league/competitions/innovations/display2007.cfm
From AY2005 to AY2006, the enrollment grew from 9 students to 71 students and continues to grow at unprecedented rates. In AY2009, there were 204 students enrolled in the ISS degree and certificate programs. Since academic year 2006, the enrollments in the degree and certificate programs have increased 187%. The corresponding FTE generated by these programs has increased by 277%. http://ola2.aacc.edu/CAEDocs1/ISSGrowthCharts.pdf

The following courses make up the IA program requirements and electives for the ISS degree and certificate.

IA Program Requirements (the following list and links to course descriptions can be found at http://www.aacc.edu/computertech/cae.cfm)
CSI 113 Introduction to Computers
CSI 130 Microcomputer Operating Systems
CSI 157 Networking 1
CSI 158 Networking 2
CSI 257 Networking 3
CSI 258 Networking 4
CSI 165 Network Security Fundamentals
CSI 194 Ethics and the Information Age
CSI 217 Hardening the Infrastructure
CSI 219 Network Defense and Countermeasures
CSI 265 Windows 2003 Server
CSI 270 Information Security Capstone

Electives (the following list and links to course descriptions can be found at http://www.aacc.edu/computertech/cae.cfm)

CSI 135 Introduction to UNIX/LINUX
CSI 207 Cyber Forensics
CSI 214 Information Systems Security
CSI 266 Windows 2003 Networking
CSI 269 Wireless LANs
EET 160 Theory and Troubleshooting Microcomputers 1

In place since AY2005, The AACC ISS curriculum is a mature curriculum that continues to expand in content based on strong funding support from the college and successful grant applications. For the Fall 2010 semester, the department will offer two new courses, Mobile Device Forensics and Certified Ethical Hacking largely with the help of funding from grants for equipment and curriculum development. Continued grant support is critical for expanding the IA curriculum and training.

In December 2009, AACC was awarded a MHEC BRAC grant to equip a lab and develop mobile device forensics courseware. See: http://www.gov.state.md.us/ltgovernor/pressreleases/091215.asp In coordination with the development of this new courseware, the college plans to offer a four-day national training event to government and educational institutions in June 2010 entitled "Handheld Device Forensics: Obtaining Evidence from Cell Phones, Smart Phones, and GPS Devices" to share this leading edge curriculum. Based on funding from a Perkins grant, the department is also developing Certified Ethical Hacking courseware.

---

b. Evidence of Copies of Articulation/Transfer agreements with 4 yr institutions offering a concentration or IA degrees/areas of study/track or certificates.
Point Value: 5 points

SUBMISSION:
AACC's Information Systems Security degree program maintains articulation agreements with the following 4 year institutions. Signed articulation agreements are available at http://www.aacc.edu/transfer/programspathway2.cfm.
Capitol College

Strayer University
Towson University
University of Baltimore
University of Maryland University College

Furthermore, AACC actively seeks new articulation opportunities for its students and is presently negotiating an articulation agreement with Wilmington University for its Bachelor of Science in Computer and Network Security.

Please note that through the University Consortium http://www.aacc.edu/aboutaacc/consortium/default.cfm and the Regional Higher Education Center (RHEC) located at AACC's Arundel Mills campus, UMUC offers its B.S. in Computer Information Technology, the program to which AACC's ISS program articulates, at AACC's Arundel Mills campus. As such, students can complete their bachelor degrees by attending classes only at an AACC campus. For articulations and signed agreement, see: http://ola2.aacc.edu/CAEDocs1/UniversityConsortiumAgreementUMUC/UniversityConsortiumAgreementForUMUC.pdf.

Additionally, AACC has begun discussions with UMUC to explore offering UMUC's new graduate program in information assurance at AACC's Arundel Mills location as well.

---

c. Articulation agreements with high schools to facilitate awareness and training for faculty/administration/students.
Point Value: 2 points per school / 6 pts maximum

SUBMISSION:
Strong articulation agreements exist between AACC and the Anne Arundel County Public School(AACPS)system, a very large school system serving the entire county and 74,000 students with 5,600 teachers, 12 high schools, and 2 applied technology centers http://www.aacps.org/aacps/boe/ADMIN/PINFO/fastfacts.pdf. These agreements are between the college and the entire AACPS system and not between AACC and individual schools thus making the agreements available to all AACPS students.

Anne Arundel Community College and Anne Arundel County Public Schools have developed what are known as Program Pathways to support the successful transition of students from high school programs to college programs and then to careers. Each Program Pathway is accompanied by an articulation agreement. One such program is the Computer/Network Technology pathway.
With the Computer/Network Technology Pathway http://www.aacc.edu/techprep/CompNetwrkngTech.cfm and accompanying articulation agreements https://www.aacc.edu/techprep/file/ComputerNetworkingTechnology%2009-10.pdf, Anne Arundel County Public School students may articulate up to sixteen (16) credits into AACC's Information Systems Security A.A.S. degree or Information Systems Security Certificate programs.
Additionally, through the Academy of Information Technology https://www.aacc.edu/techprep/file/AcademyofInfoTech%2009-10.pdf, high school students may articulate up to nine (9) credits into AACC's Information Systems Security program.

AACC also provides awareness activities for students and faculty through yearly (since 2004) Business and Technology Expos

http://ola2.aacc.edu/CAEDocs1/TechPrep/Agenda-Business&TechEdExpo%203-10-09.pdf, in which faculty from the Information Systems Security Program conduct hands on exercises in areas such as digital forensics, security and steganography. AACC also hosts events such as the November 20, 2009 Tech Mania Day, in which 130 public and private school 9th graders attended a series of hands on sessions
in information security, steganography and information assurance that were conducted by AACC faculty and industry practitioners. See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechManiaDayPresentationSummaryStudentsv2.pdf. The sessions were well received by the students as evidenced by the event survey results
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/Survey%20Results%20-%20Tech%20Mania%20-%20Fall%202009%20(2).xls

AACC strives to facilitate and provide significant IA awareness for AACPS high school faculty/administration/students through professional development and collaborative activities. For example, on the November 20, 2009 Tech Mania Day, 45 public and private high school teachers attended special faculty sessions on information assurance
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechManiaDayPresentationSummaryFaculty.pdf.
In addition, AACC, through Perkins grant funding, conducts annual Information Technologies Professional Development Day
http://ola2.aacc.edu/CAEDocs1/TechPrep/AGENDA-InfoTechProfDevDay2-24-09.pdf
for AACPS faculty. In 2009, one session focused on information security and another focused on digital forensics. For the tentative 2010 agenda including topics such as Internet security, security clearances, steganography, and digital forensics, see
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/DRAFTAGENDACompTechProfDevDay2_24_2010.pdf

Importantly, AACC also collaborates with IA industry partners and the Anne Arundel County Public School (AACPS) system on curriculum development. In collaboration with the Ft. Meade Alliance and AACPS, AACC created Project Scope http://project-scope.org, a website that provides information for students, parents, business and educators on security clearances. It also provides 7th, 9th and 11th grade curricula for educators to use in their classrooms. It is understood that the Maryland Department of Education will be rolling Project Scope out to other Maryland school systems outside of Anne Arundel County. AACC has collaborated with AACPS in other ways, such as by providing a curriculum module in digital forensics for the Meade High School Homeland Security Signature curriculum.

AACC facilitates IA awareness by serving as a Regional Cisco Networking Academy for the Anne Arundel County Public School system and several other community colleges. See:
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CiscoAcademyList.pdf. In this capacity, it provides technical assistance and training to Local Cisco Networking Academies. Last year, Anne Arundel County Public Schools became a Local Academy that reports to AACC's Regional Academy. As such, AACC has provided technical assistance to Anne Arundel County Public Schools, specifically the Center for Applied Technology - North (CAT-North) and the Center for Applied Technology-South (CAT-South), two AACPS high schools. Additionally, Professor Paul Derdul serves on the CAT-North Advisory Board for CAT-North's Cisco program. Other Local Academies to which AACC is available to provide support and training based upon each institution's needs are:

Center of Applied Technology North (part of the Anne Arundel County Public School system)
Center of Applied Technology South (part of the Anne Arundel County Public School system)
Baltimore City Community College
Chesapeake Community College
College of Southern Maryland
Community College of Baltimore County
Harford Community College
South Carroll Career and Technology Center
St. Mary's County Technical Center
Wicomico County Public Schools

AACC has also collaborated with Cisco Corporation to host training on its Discovery Curriculum for high school teachers. AACC was one of four sites world-wide to host Cisco's small market trial to review the new Cisco Certified Network Administrator Discovery Curriculum. Twenty high school faculty from around the U.S. attended the week-long training. See: http://www.gbc.org/old-news/718/. Professor Susanne Markowski, one of our full-time IA faculty was a technical editor for the Cisco publication, Designing and Supporting Computer Networks, CCNA Discovery Learning Guide. See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CiscoDiscoveryCurriculumS_Markowski_editor.pdf#page=2

---

d. Participation in Cyber/IA competitions.
Point Value: 2 points per each / 6 pts maximum

SUBMISSION:
AACC students participate in the Collegiate Cyber Defense Competition (CCDC) http://angeldrop.aacc.edu/flash/?video=CCDC.flv&width=546&height=300 and Cyber Dawn competition http://www.whitewolfsecurity.com/. Recently the ISS students have become involved with a second competition, the Department of Defense Cyber Crime Center (DC3)Digital Forensics Challenge http://dc3.mil/challenge/2010/

Anne Arundel Community College students have participated in the Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC) every year since its inception in 2006, and will again be fielding a team at the 2010 CCDC. In the 2006 CCDC, AACC students placed second.

The Mid-Atlantic Regional CCDC, as part of the National CCDC, is a three day event that 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.

For evidence of AACC IA student participation in the Mid-Atlantic Regional Collegiate Cyber Defense Competition (CCDC), see the following.
In 2006: placing second

http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=74:1st-mid-atlantic-ccdc&catid=50:ccdc&Itemid=110
In 2007:
http://www.cyberwatchcenter.org/index.php?option=com_content&view=article&id=75:2nd-mid-atlantic-ccdc&catid=50:ccdc&Itemid=110
In 2008: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CCDC2008.pdf

In 2009: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CCDC2009.pdf

Additionally, AACC participated in the first ever Cyber-Dawn live hacking exercise at Battlefield High School in Haymarket, Virginia on October 3rd and 4th of 2009 http://www.whitewolfsecurity.com/cyberdawn.php. Cyber-Dawn is a computer network attack and defend live-fire exercise designed to showcase both the defense skills of various schools and organizations, and the attacking prowess of some of the Maryland and Virginia area's finest penetration testers and security professionals.

During the current Fall 2009 semester, Anne Arundel Community College, met with members of the DC3 Forensics Challenge Team to establish an initial relationship between our two organizations. Those discussions resulted in DC3 providing AACC with sample forensic problems for use in the College's CSI 207 Computer Forensics course. The challenge forensics exercises were presented to the students as part a special class project. Based on student reaction and the inherent learning value of the exercise, AACC will make these exercises a part of the final exam process on an on-going basis. AACC will also be participating in next year's DC3 Cyber Challenge Exercise.

---

e. Courses containing "Hands-on" training or Lab training.
Point Value: 2 points per course / 6 pts maximum

SUBMISSION:
The following courses are core components of AACC's ISS programs and contain extensive "hands-on" laboratory components. Many of the courses comprise the courseware that has been certified to have mapped to the CNSS 4011 and 4013 standards.

CSI 130 Microcomputer Operating Systems
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=47822
Hands-On Labs Include:
- Disk Preparation, File Management Systems and Commands
- Data Backup and Restore Operations
- Command Shell Operations
- Malware Protection
- System Control, Printer Operations, Hardware/Software Installation
- Directory Management Commands
- Common System Utilities

CSI 157 Networking 1
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49526
Hands-On Labs include:
- Using NewTrace to View Internetworks
- Topology Orientations & Building a Small Network
- Using Wireshark to Vie Protocol Data Units
- Manage a Web Server
- Examining a Devices Gateway
- Examining ICMP Packets
- Address Resolution Protocol

• Establishing a Router Console Session with HyperTerminal
• Configuring Host Computers for IP Networking

CSI 158 Networking 2
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49527
Hands-On Labs Include:
• Establishing a Router Console Session
• Configuring a Router with basic IOS commands
• Using Advanced Telnet Operations
• Managing Router Configuration File
• Configuring Static Routes
• Configuring Dynamic Routing Protocols

CSI 257 Networking 3
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49532
Hands-On Labs Include:
• Configuring Static and Default Routing
• Basic & Advanced PPP Configuration Lab
• Basic & Advanced Frame Relay Connections
• Working with Security Configurations
• Configuring Access Control Lists
• Basic DHCP and NAT Configurations
• Network Troubleshooting

CSI 258 Networking 4
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49533
Hands-On Labs Include:
• Basic Switch Configuration IOS Setup
• Basic VLAN Configuration
• Working with VTP Configurations
• Configuring Spanning Tree Protocol
• Basic Inter-VLAN Routing
• Working with Wireless Configurations

CSI 165 Network Security Fundamentals
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49528
Hands-On Labs Include:
• Identifying Security Attacks
• Controlling Access to Computers
• Hardening Computers
• Hardening Networks
• Hardening Wireless Networks
• Managing Digital Certificates
• Designing Security Policies

CSI 217 Hardening the Infrastructure
http://www.aacc.edu/computertech/CSI217.cfm
Hands-On Labs Include:
• Capturing and Identifying IP Datagrams
• Capturing and Identifying IP, TCP ICMP Headers & Messages
• Creating & Implementing Access Control Lists
• Implementing FireWall Technologies
• Capturing & Analyzing IPSec Protocols
• Working with Host & Network Intrusion Based Systems
• Installing & Configuring Snort to Use a Database
• Installing & Auditing Wireless Networks

CSI 219 Network Defense and Countermeasures
http://www.aacc.edu/computertech/csi219.cfm
Hands-On Labs Include:
• Drafting a Security Policy
• Using MBSA to Scan multiple Computers
• Researching the TCP and IP RFCs
• Using a Symmetric Algorithm in Word 2003
• Developing a Security Strategy for Green Globe's Operations
• Installing and Configuring the IIS Lockdown Tool
• Creating a Linux Account
• Applying Security Policies to a Linux Server
• Configuring IAS
• Configuring Special Permissions and Registry Policies

CSI 265 Windows 2003 Server
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49534
Hands-On Labs Include:
• Working with IIS v6.0
• Installing Windows 2003
• Installing Active Directory
• Organizing Disks for Data Storage
• Configuring a Home Director
• Creating a Local User, Group Accounts, Creating Computer Acct
• Setting up a Network Printer using TCP/IP
• Installing Local Printers in Windows 2003 Server, Ownership and Printer Pools
• Working with Terminal Services
• Working with the Backup Utility

Electives
CSI 135 Introduction to UNIX/LINUX
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=47823
Hands-On Labs Include:
• Linux Configurations
• Working with the Linux File System
• Working with Passwords
• Setting Permissions
• Updating Linux
• Labs covering basic Linux Operations Working with IIS v6.0

CSI 266 Windows 2003 Networking
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=44012
Hands-On Labs Include:
• Network Overview Lab
• Configuring Network Protocols
• Configuring Dynamic Host Configuration Protocol
• Installing DNS Services
• Installing WINS Services
• Working with Remote Access
• Installing and configuring IP Routing
• Configuring IPO Security
• Setting up NAT Translation
• Configuring Certificate Services

CSI 269 Wireless LANs
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=49535
Hands-On Labs Include:

- Installing and Configuring a Wireless Adapter
- Planning and Deploying a Wireless LAN
- Conducting a Site Survey
- Implementing Wireless LAN Security
- Managing a Wrieless LAN
- Network Settings and Wireless LAN Troubleshooting
- Personal, Metropolitan, and WAN Wireless Networks

Back to top

3. *IA as multidisciplinary subject:* The academic program demonstrates that IA is treated as a multidisciplinary subject with elements of IA knowledge incorporated into various disciplines.
Overall Point Value: 10 minimum/15 maximum

a. Evidence that IA is taught as modules in existing non-IA courses and that non-technical/non-IA students are being introduced to IA (For example: Non-technical/non-IA students are being introduced to IA concepts; e.g. business courses teaching Information Security modules, health courses – HIPAA regulations)
Point Value: 5 points

SUBMISSION:
Information Assurance is embraced in many non-IA courses throughout AACC, including large enrollment general education classes as well as business, cybercrime, homeland security, and health professions courses.

A significant portion of students earning a degree at AACC will be exposed to information assurance modules contained in two general education courses: Computing and Information Technology CSI 112 and Introduction to Computers CSI 113 http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_278.htm. Both of these courses include modules dedicated to information/computer security. Because all AACC degree graduates are required to fulfill a general education Computer or Interdisciplinary Studies competency to graduate, most degree programs require either CSI 112 or CSI 113. As such, approximately 3000 students each year complete these courses. Notably, CSI 113 is part of the courseware that maps to the 4011 standard http://www.aacc.edu/computertech/file/aacc_2009_nstissi_4011_matrix3.pdf.

In addition to the general education introductory computer courses, Ethics in the Information Age CSI/PHL 194 http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_282.htm discusses the ethics of hacking and cracking and other issues associated with identity protection in an online environment. Because this course is designated as an Arts and Humanities and Interdisciplinary Studies general education course, students in any program of study can take it to fulfill an Arts and Humanities or Interdisciplinary Studies general education requirement.

This list is a sample of non-IA courses that include IA components.
1. BPA156 Electronic Commerce
2. CJS 207 Cyber Forensics
3. HLS 111 Introduction to Homeland Security
4. HLS 112 National Security Law
5. HLS 121 Protecting Critical Infrastructure and Key Assets Seminar
6. HLS 122 Emergency and Disaster Preparedness
7. HLS 211 Intelligence Analysis and Security Management
8. HLS 230 Intelligence Support to the Policy Maker and Military

9. HLS 240 National Security Challenges of the 21st Century
10. HLS 245 Intelligence Analytics Seminar
11. HLS 260 Terrorism/Counterterrorism (cross-listed as CJS 260)
Course descriptions can be found at http://www.aacc.edu/computertech/cae.cfm. Detailed course outlines are available for review in the ANGEL CAE course section 3a https://angel.aacc.edu/default.asp.

Information assurance is a component of the college's curricula for the Cybercrime A.A.S. degree http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_117.htm and certificate programs http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_118.htm. These programs of study require that a student complete Information Systems CSI 214 Security and Cyber Forensics CSI 207. CSI 214 is part of the courseware that maps to the 4011 standard http://www.aacc.edu/computertech/file/aacc_2009_nstissi_4011_matrix3.pdf.

Additionally, the Homeland Security Management degree and certificate programs http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_166.htm, http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_167.htm and http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_182.htm offering degree tracks in Homeland Security Management and Intelligence Analytics also extensively infuse information assurance into the curriculum.

Cyberlaw CJS/LGS 207 http://www.aacc.edu/search/course/crs_desc.cfm?courseId=48342, which discusses civil remedies and criminal actions associated with nefarious activities using information technology, is an elective in the Criminal Justice, Homeland Security Management and Paralegal Studies program and a required course in the Cybercrime program.

Within the business spectrum, the Business Management department offers a class in Electronic Commerce BPA 156 http://www.aacc.edu/search/course/crs_sect.cfm?termId=46&courseId=41275. This course contains significant components regarding risk management, firewalls, cryptography and authentication. This course can fulfill an elective requirement in the Business Management and Computer Information Systems programs of study.

Information Assurance is a significant component of AACC's health care programs of study. As such, the health care programs have collaborated to deliver a unified and comprehensive module on information assurance in health care. In Fall 2009, AACC's School of Health Professions, Wellness, and Physical Education developed this comprehensive module for the HIPAA Title II Administrative Simplification Act and Security rule. The purpose of the HIPAA module is to ensure that all students in the health professions, prior to entering clinical areas and accessing patient information, receive consistent and thorough training, including a post-training assessment. Learning module objectives are detailed and include the HIPAA mandate, patients' rights, and remedies under the law. The following link provides a screenshot and learning objectives from the HIPAA module http://ola2.aacc.edu/CAEDocs1/HIPAA/HIPAA_Module.pdf. The actual HIPAA module is available for review in the ANGEL CAE course section 3a **[LINK REMOVED FOR CONFIDENTIALITY]**. The strategy for initial implementation for the Fall 2009

semester targeted the Physician Assistant and Medical Assisting programs, totaling approximately 100 students. The second implementation phase beginning in the Spring 2010 semester will include, in addition to the physician assistant and medical assisting students, approximately 120 students from the School of Nursing registered and practical nursing programs.

Subsequent to the Spring 2009 roll out, the following health programs will be implementing online ANGEL HIPAA training:

- Emergency Medical Technician
- Health Information Technology
- Medical Laboratory Technician
- Patient Care Technician and Geriatric Nursing Assistant
- Pharmacy Technician
- Phlebotomy Technician
- Intravenous and Electrocardiogram Technician
- Radiologic Technology Program

Effective Fall 2009, the college launched a new Health Information Technology A.A.S. degree http://www.aacc.edu/healthprofessions/default.cfm. Students in the this degree http://www.aacc.edu/catalog/interactiveCatalog/CollegeCatalog2009-2010_Color_164.htm receive additional training pertaining to organizational policies, training methodologies, and the technical expertise needed to maintain and secure electronic patient medical records, such as electronic firewalls and anti-virus systems.

---

b. Evidence IA programs (certificate and/or degree programs) require non-technical courses of study; e.g. ethics, policy, and business.
Point Value: 5 points

SUBMISSION:
Both the ISS degree and certificate programs require non-technical courses that focus on ethics, policy and business. The ISS degree and certificate programs requires that students successfully complete Ethics and the Information Age CSI 194 http://www.aacc.edu/search/course/crs_desc.cfm?courseId=48184 (course outline is available for review in the ANGEL CAE course section 3b **[LINK REMOVED FOR CONFIDENTIALITY]**).

The Associate of Applied Science degree in Information Systems Security http://www.aacc.edu/catalog/interactivecatalog/CollegeCatalog2009-2010_Color_100.htm requires 24-26 credits in general education. These requirements include English, Arts and Humanities, Biological and Physical Science, Computer Technology, Health/Fitness/Wellness, Mathematics and Social and Behavioral Science. Specifically, Ethics and the Information Age CSI 194 (course outline is available for review in the ANGEL CAE course section 3b **[LINK REMOVED FOR CONFIDENTIALITY])** is required of all ISS majors as the Arts and Humanities general education course. This course focuses extensively on ethics and policy associated with information technologies, along with the propriety of business decisions made for profit but contravene consumer and public safety.

---

c. Availability of non-credit/credit professional development courses in IA (e.g. First responders, K-12 teachers)
Point Value: 5 points

SUBMISSION:
AACC, through its Center for Workforce Solutions and its Continuing and Professional Education divisions, offers extensive non-credit/credit professional development courses in IA.

The Center for Workforce Solutions (CWS) offers IA training and certifications at Arundel Mills, Glen Burnie Town Center, the Arnold campus, or on-site. For a list of the Cisco, CompTIA, Cybercrime and Network Security, and HIPAA Security offerings, see http://www.aacc.edu/cws/files/ComputerTech.pdf

Information Assurance related non-credit/professional development courses are also available through the Center for Workforce Solutions to any governmental entity through the General Services Administration Schedule. These courses include:
CNT454 Security + Certification
CNT455 Certified Information Security Manager (CISM)
CNT456 Certified Information Systems Auditor (CISA)
CNT457 Security Certified Network Specialist (SCNS) Tactical Perimeter Defense
CNT458 Security Certified Network Professional (SCNP) Strategic Infrastructure Security
CNT459 Security Certified Network Architect (SCNA) Advanced Security Implementation
For course descriptions, see:
https://www.gsaadvantage.gov/ref_text/GS02F0140S/0GOJLU.21253K_GS-02F-0140S_JUL282009.PDF

The School of Continuing and Professional Education offers many IA and IA related non-credit courses for information technology professionals, health care providers, legal professionals, law enforcement personnel and transportation and cargo workers. Links to some of the IA course offerings are provided here.
A+ Certification and PC Technician http://www.aacc.edu/IT/APLUS.cfm
CISSP Certification http://www.aacc.edu/it/CISSP.cfm
Network+ Certification http://www.aacc.edu/it/netplus.cfm
Cisco Certification http://www.aacc.edu/it/cisco.cfm
Introduction to PC Security
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=47483
Home PC Security
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=50911
Advanced PC Security
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=51160
HIPAA Compliance
http://www.aacc.edu/search/course/crs_desc.cfm?courseId=50994
HIPPA Privacy http://www.aacc.edu/search/course/crs_desc.cfm?courseId=51846

Anne Arundel Community has also partnered with New Horizons Computer Learning Centers using a “mentored learning” approach to offer the classes such as: Network+ / Security+, Windows Server, Exchange Server, SQL Server, Security, Cisco, and Project Management. See http://www.aacc.edu/it/mentored.cfm
In classes of no more than 12 students, a mentor blends traditional classroom instruction, hands-on lab exercises, one-on-one mentoring, reading and video-based instruction to prepare students for industry-recognized certification exams. Students who complete the courses receive continuing education units

(CEUs) and are eligible to sit for industry-recognized certification exams.

Additional non-credit courses offered by the School of Continuing and Professional Education focusing on or with components involving information assurance are listed below. Course information is available upon request.
OLN 339 Security, Surveillance and Access Control Systems
CTT 328 Network Security Fundamentals
TTA 499 Internet Safety
CMP 320 Introduction to Microcomputers
CMP 338 Computer Literacy
COU 312 Theory/Troubleshooting Microcomputers
CTT 324 Microcomputer Operating System
FTR 300 Exploring the Future
FTR 302 Globalization and Its Future
HNS 306 Nursing Home Law and Regulations
NRN 331 Legal Issues in Nursing
HTH 562 Preventing Workplace Violence in Medical Field
EXT 506 Hazmat Ground and Ocean Transportation
EXT 505 Hazmat in Grnd Transportation
EXT 504 Hazmat in Grnd/Air-Refresher
EXT 502 Hazmat in Grnd/Air- Transport
EXT 507 Hazmat in Grnd/Ocean Trans-
EXT 510 Hazmat Multi Modal Transp. Refr
EXT 509 Hazmat Multi Modal Transp.
EXT 503 Hazmat/Ground Transportation
RLT 306 Real Estate Ethics/ Professional
EXT 574 SCIF Construction: Project Management
EXT 575 SCIF Design and Contract Management
EXT 573 SCIF Overview
Conference Paralegal Boot Camp
Conference Hate In America Part 2: Gangs and Domestic Terrorism
Conference Gangland: America's Increasing Gang Problem

Back to top

4. *IA Outreach:* The academic program must demonstrate a strong collaboration with business, industry, government, and the local community.
Overall Point Value: 4 minimum/10 maximum

a. Evidence provided in the form of a Strategic Plan and/or general IA Awareness Program description (example: flyers, letters from sponsors, etc), and/or workshop accomplishments. (For example: sponsorship of workshops for K-12, senior citizen groups, community colleges, technical schools, state homeland security, first responders, industry, etc.)
Point Value: Up to 10 points

SUBMISSION:
There are many facets of AACC's IA Awareness activities. Many of these activities flow from AACC's Integrated Technology Plan. Goal 2, Student Experience, Strategy 2.4, that states the college will "Promote effective use of cyber security measures." See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechnologyPlanGoalsandStrategies.pdf#page=2.

On its main website, accessible to anyone, AACC provides Cyber Security awareness information http://www.aacc.edu/cybersecurity related to e-mail security, online shopping, online threats, protecting personal information,

protecting your PC, social networking and wireless security. Such information is provided in collaboration with StaySafeOnline.org

For its October 2008 and October 2009 monthly publications, the Information Systems department has made cybersecurity a focus raising the awareness of the entire AACC community during cyber security awareness month. See: http://www.aacc.edu/technology/file/CyberSecurityOct2009.pdf and http://www.aacc.edu/technology/file/October2008.pdf.

As indicated above, AACC also provides awareness activities for public and private high school students and faculty yearly (since 2004) Business and Technology Expos http://ola2.aacc.edu/CAEDocs1/TechPrep/Agenda-Business&TechEdExpo%203-10-09.pdf in which faculty from the Information Systems Security Program conduct hands on exercises in areas such as digital forensics, security and steganography. AACC also hosts events such as Tech Mania Day, in which 130 public and private school 9th graders attended a series of hands on sessions http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechManiaDayPresentationSummaryStudentsv2.pdf in information security, steganography and information assurance that were conducted by AACC faculty and industry practitioners. The sessions were well received by the students as evidenced by the event survey results http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechManiaSurvey%20ResultsFall2009.xls.

AACC strives to provide significant professional development for AACPS faculty. For example, on Tech Mania Day, 45 public and private high school teachers attended special faculty sessions on information assurance http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechManiaDayPresentationSummaryFaculty.pdf. AACC, through Perkins grant funding, conducted Information Technologies Professional Development Day http://ola2.aacc.edu/CAEDocs1/TechPrep/AGENDA-InfoTechProfDevDay2-24-09.pdf for AACPS faculty, in which one session focused on information security and another focused on digital forensics. It will continue such activities in the future.

Importantly, AACC also collaborates with AAPCS on curriculum development. In collaboration with the Ft. Meade Alliance and AACPS, AACC created Project Scope http://project-scope.org/ , a website that provides information for students, parents, business and educators on security clearances. It also provides 7th, 9th and 11th grade curricula for educators to use in their classrooms. It is understood that the Maryland Department of Education will be rolling Project Scope out to other Maryland school systems outside of Anne Arundel County. AACC has collaborated with AACPS in other ways such as by providing a curriculum module in digital forensics for the Meade High School Homeland Security Signature curriculum.

AACC publishes articles on information security and the college's programs and course offerings in information security. Such publications are directed at the community, existing students, prospective students, businesses, government, and alumni. They include the following:

Koermer, Kelly A., "Anne Arundel Works to Meet Regional Cybersecurity Workforce Needs," Community College Week, Fall Technology Supplement, 2009. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CmtyCollegeWeekCyberSecurityarticleKoermer.pdf

"Secure Your Data Against Cybercriminals," Workforce Solutions, Winter 2009. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/WorkforceSolutionsWinter2009ISS.pdf

Koermer, Kelly A., "ISS Program Trains Cyberwarriors," Workforce Solutions, Winter 2009. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/WorkforceSolutionsISSProgramTrainsCyberwarriors.pdf

Gross, Susan S.C., "AACC-Cisco Partnership Helps," Workforce Solutions, Winter 2009. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/WorkforceSolutionsWinter2009ISS.pdf

"They Speak Geek: AACC's Computer Information Systems Department Teaches Sophisticated and Introductory Technology", Community of Alumni and Friends, Anne Arundel Community College, 2006. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CommunityMagFall2006CT.pdf

"Initiatives that Meet BRAC Needs", Anne Arundel Community College 2009. http://ola2.aacc.edu/CAEDocs1/Publications/InitiativesMeetBRACNeeds.pdf

"More Recognition for AACC's Information Systems Security Program," print ad., Schedule of Classes. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/MoreRecognitionISSPrograms.pdf

The college also works with the press to have articles published about information assurance and its programs and courses related to information assurance. Examples of such are:

Parry, Marc, "Community Colleges Mobilize to Train Cybersecurity Workers," The Chronicle of Higher Education, June 26, 2009. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/ChronicleHEdJune2009CyberSec.pdf

Ulman, Danielle, "Maryland State Institutions Pumpin Up 'CSI for Real' Offerings, The Daily Record, June 2, 2008. http://ola2.aacc.edu/CAEDocs1/Support%20Documents/DailyRecordJune2008CSI.pdf

Logan, Rebecca, "Colleges and universities studying ABCs of BRAC," Baltimore Business Journal - BRAC Special Issue, May 30, 2008. <http://ola2.aacc.edu/CAEDocs1/Support%20Documents/BaltimoreBusJournalBRAC_May2008.pdf>

Additionally, ACCC faculty and staff have conducted workshops for the public, including http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/Outreach%20Audience%20Presentations.pdf, http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/backups.ppsx, http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/basic%20firewall.ppsx, http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/basic%20PC%20Security.ppsx, and http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/ID_Theft.ppsx

This spring there will be four seminars/webinars open to the public focusing on cyber technology

http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/CybertechnologySeminarsFlyer.pdf

AACC has also presented at the League for Innovation Conference on Information Technology 2008 on CyberWATCH and sharing best practices in developing cybersecurity and information assurance curricula. See CIT program, http://ola2.aacc.edu/CAEDocs1/Public%20Presentations/2008_CIT_Conference_Program.pdf#page=12.

AACC also conducts conferencing for legal professionals, including lawyers and paralegals. A conference held in April 2007, entitled Strategies for E-Discovery and E-Filing http://ola2.aacc.edu/CAEDocs1/Support%20Documents/E-Discovery%20conference%20forensics%20handouts%20color.pdf featured a Keynote Speaker from the Defense Cyber Crime Center on the topic of "The Power of Digital Forensics for E-Discovery." IT also had a hands-on demonstration of digital forensics. This conference was co-sponsored by the Anne Arundel Bar Association, Maryland State Bar Association and the Special Committee on Paralegals, and the Maryland Institute for Continuing Professional Education of Lawyers.

In May 2008, the college hosted a seminar for legal professionals on Electronically Stored Information (ESI) http://ola2.aacc.edu/CAEDocs1/Support%20Documents/ESI-Discovery,Admissabiity%20and%20Ethics.pdf. This conference was sponsored by the Maryland Institute for the Continuing Professional Education of Lawyers and featured discussions on discovery, admissibility and ethics associated with electronic information.

The college also offers summer "Tech Camps" through its Kids in College program. These camps have been designed to target underrepresented populations in technologies, specifically middle school girls. Also, during the summer of 2008, the college received Perkins funding which enabled us to offer camp scholarships to underrepresented minority students. Network security, instruction detection, cryptology, and digital forensics, including steganography, have been topics in such camps. A white paper on attracting girls to technology was also produced as a result of the camps http://ola2.aacc.edu/CAEDocs1/Support%20Documents/Attracting%20Girls%20to%20Technology%20Reach%20Them%20Before%20Turnoff.pdf .

Supporting documents include:

STEM summer camp schedule
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/STEM%20Technology%20Camp%20Schedule%20Summer%202009.pdf

Techno Sleuth summer camp topic list
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechnoSleuth%20Camp%202008.pdf

Camps recap for all technology camps from 2005 through 2009
http://ola2.aacc.edu/CAEDocs1/Support%20Documents/Camps%20Recap.pdf

Back to top

5. *IA Faculty:* Faculty assigned specifically to teach and/or develop IA courses/curricula/modules.

Overall Point Value: 11 minimum/15 maximum

a. Identify by name faculty member with overall responsibility for the IA instructional program. Provide evidence, i.e. verification letter and/or job description.
Point Value: 5 points (required)

SUBMISSION:
Professor Paul Derdul, as the IA Program Coordinator for Anne Arundel Community College, has overall responsibility for the Information Systems Security (ISS) and Computer Network Management (CNM) programs. His specific responsibilities include curriculum development, student advising, faculty training, initiating and maintaining articulation agreements with other educational institutions and outreach activities supporting government and industry workforce initiatives. He has managed unprecedented growth of 187% in ISS student enrollment from AY 2006 to 2009. Professor Derdul has been and continues to be the key faculty member in developing and delivering the content of programs in this critical area. College website information: http://www.aacc.edu/computertech/pderdul.cfm.

Evidence includes:
Verification letter from Dean Kelly Koermer:
http://ola2.aacc.edu/CAEDocs1/Section5/DerdulCoordinatorLetter.pdf

Description of AACC coordinator responsibilities:
http://ola2.aacc.edu/CAEDocs1/Section5/CoordinatorPositionDescriptions.pdf

List of programs and courses Professor Derdul is responsible for:
http://ola2.aacc.edu/CAEDocs1/Section5/ISSandCNM_Programs_and_Courses.pdf

[FACULTY INFORMATION REMOVED FOR CONFIDENTIALITY]

b. Identify by name additional IA faculty members teaching IA courses within the department that sponsors IA programs.
Point Value: 1 pt per name / up to 5 maximum

SUBMISSION:
Led by Professor Paul Derdul, coordinator of the Information Systems Security and Computer Network Management programs and courses, the following full time faculty members teach ISS courses beyond the entry-level CSI 112 and CSI 113 courses. (Curriculum vitae available for review in the ANGEL CAE course section 5b **[LINK REMOVED FOR CONFIDENTIALITY]**.)

Professor Jay Benson (CCNA, CCNP, CCAI)
Dr. Bruce George (CISSP)
Professor Cheryl Heemstra
Professor Susanne Markowski
Professor Joseph McQuighan (CCNA, PMP)
Professor Kasia Taylor

In addition to the full-time faculty, the programs are supported by the following adjunct faculty. (Curriculum vitae available for review in the ANGEL CAE course section 5 **[LINK REMOVED FOR CONFIDENTIALITY]**.)

[FACULTY INFORMATION REMOVED FOR CONFIDENTIALITY]

c. Provide evidence in the form of curriculum vitae supporting the faculty member's

qualifications to teach IA. At least one IA faculty member will be expected to be professionally certified with at least one of the IA certifications listed under DOD Directive 8570, such as CISSP, CPP, CISA, CISM, GIAC, etc. or a minimum of 9 hrs of graduate coursework and/or appropriate experience in a related field could be considered in lieu of a professional certification.
Note: Can be same individual as 5a.

CISSP: Certified Information System Security Professional
CPP: Certified Protection Professional
CISA: Certified Information Systems Auditor
CISM: Certified Information System Security Manager
GIAC: Global Information Assurance Certification
Point Value: 5 points (required)

SUBMISSION:
Anne Arundel Community College has highly credentialed professionals developing and teaching the information systems security curriculum. The Computer Technologies department has two full-time faculty members (Paul Derdul and Dr. Bruce George) with CISSP certifications and, depending on the semester, several adjunct faculty holding CISSP certifications. Curriculum vitae for the program coordinator and all faculty are available for review in the ANGEL CAE course section 5
[LINK REMOVED FOR CONFIDENTIALITY]

Back to top

6. Practice of IA encouraged throughout the Institution: The academic program demonstrates how the institution encourages the practice of IA, not merely that IA is taught.
Overall Point Value: 8 pts minimum/20 maximum

a. Provide a link to the institution IA security plan and/or policies
Point Value: Up to 5 points

SUBMISSION:
The AACC Integrated Technology Plan, Goal 2, Student Experience, Strategy 2.4, provides that the college will "Promote effective use of cyber security measures." See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/TechnologyPlanGoalsandStrategies.pdf#page=2.

In support of that goal, the college has numerous safeguards in place throughout the institution to protect resources, including information. Section A references the policies, procedures, and standards that are in place to support the goal of information security. Section B references audits and reviews that are in place to ensure adequate security of college systems and information. (The policies, procedures, audits, and reviews are available in the ANGEL CAE course section 6a: **[LINK REMOVED FOR CONFIDENTIALITY]**.)

Section A: AACC Information Security Policies, Procedures, and Standards

1.) Computer and Electronic Communication Access and Usage Policy: This is a board approved college wide policy that is published in the College Catalog. This policy outlines acceptable use of AACC Technology Resources and provides procedures for handling violations.

2.) Electronic Information Security Policy: This is a board approved college wide policy that is published in the College Catalog. This policy states that the college amasses an enormous amount of information in its day to day business, and the college community shall be prohibited from any unauthorized use, production, dissemination, alteration or destruction of this information.

3.) Identity Theft Protection Policy: This is a board approved college wide policy and will be published in the College Catalog. This policy provides for the creation of an Identity Theft Prevention Program to protect college students, employees and customer's identities in accordance with the Red Flags Rule standards issued by the FTC in accordance with the Fair and Accurate Credit Transactions Act, an amendment to the Fair Credit Reporting Act.

4.) FERPA Student Record Security: This is a policy effective within our Registrar's office that states that the college complies with all federal regulations of the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended. This document also outlines the Procedures for Maintaining Student Records in Accordance with FERPA.

5.) Password Standards: This document outlines the standards for secure passwords that are required by college systems.

6.) AntiVirus Standards: The College has standards requiring Anti-Virus protection for all servers and workstations. The evidence for this can be found in the following two documents: Server Antivirus Standards and Procedures and Desktop Security.

7.) Patch Management Standards: The College has standards requiring regular patching of systems. The evidence for this can be found in the following two documents: Server Patch Management and Desktop Patch Management.

8.) Equipment Disposal and Destruction of Sensitive Data: This procedure is used to ensure that college equipment and media do not contain information of a confidential nature before they are transferred outside the college facility for surplus or destruction.

Section B: AACC Audits and Security Reviews In Place to Ensure Adequate Security of College Systems and Information

1.) AACC Security Audit Scope of Work: The college regularly hires an outside firm to audit all aspects of information security with deliverables of an executive summary and a detailed report of findings. This document defines the scope of work for the audit that is currently underway.

2.) Annual Financial Audit Review of IT Systems: The college annually hires an outside firm to audit the college's financial systems. This audit includes a review of the College's IT infrastructure to conclude whether electronic data processing controls are properly designed and are operating effectively. In addition the College's auditors evaluate application controls as part of the internal control assessment. This document provides an outline of the components reviewed by the financial systems audit.

3.) IS Account Auditing - Information Services regularly performs audits of user accounts. These audits consist of an audit of user accounts and access

privileges provided by those accounts. This is performed in conjunction with the owners of the systems and/or data. The evidence for this can be found in the following four documents: Administrative Active Directory Account Management, Student Active Directory Account Management, Datatel Account Management, and Luminis Webadvisor Sirsi and ANGEL Account Management.

4.) IS Firewall Auditing – Information Services performs quarterly audits of all firewall rules and has procedures in place to ensure adequate documentation of all firewall rules. The evidence for this can be found in the following two documents: Firewall Auditing Procedure and Firewall Change Management Procedure.

5.) Vulnerability Scanning and Remediation – Information Services performs regular scans of network systems to ensure the security of our systems. The college also has contracted Security Metrics to perform quarterly external scans of our public facing servers per PCI DSS requirement. The evidence for this can be found in the following two documents: Vulnerability Scanning and Remediation Process and External PCI Compliance Scan and Remediation Procedure.

---

b. Institution designated Information System Security Officer or equivalent. Provide name, position and job description for person or persons responsible for information security.
Point Value: 5 points

SUBMISSION:
Scott Kramer serves as the college's Information Systems Security Officer. His official title is Systems Engineer- Network Security Engineer Information Services. Mr. Kramer's essential functions include working with various IS team members to raise security awareness and provide security guidance during the requirements, development and implementation stages of hardware/software purchasing and implementation decisions. The position is responsible for understanding complex security issues and communicating these issues to both technical and nontechnical peers and management. This position provides input in the development and enforcement of enterprise-wide policies and provides innovative suggestions to improve existing processes or create new ones where necessary to improve the security posture of the College. (His full job description is provided for review in the ANGEL CAE course section 6b **[LINK REMOVED FOR CONFIDENTIALITY]**)

---

c. Provide evidence of the implementation of the institution IA security plan to encourage IA awareness throughout the campus. (Example: Students and faculty/staff are required to take computer based training or on-line tutorials; a security banner statement present on institution computers; security related help screens are available; institution-wide seminars are held on the importance of IA, etc- 2pts awarded per item)
Point Value: 2 minimum / 10 maximum

SUBMISSION:
As referenced in section 6a of this application, AACC's Integrated Technology Plan Goal 2, Student Experience, Strategy 2.4, provides that the college will "Promote effective use of cyber security measures." See: http://www.aacc.edu/technology/file/Technology%20Plan%20-%20Goals%20and%20Strategies.pdf.

AACC includes the following evidence of the implementation of its IA security plan to encourage IA awareness throughout the campus.
1.) Required training for all faculty and staff: AACC faculty and staff are

required to complete an online Security Awareness training course and pass assessments for each module. Continuation of employment is contingent upon successful completion of such training. The Security Awareness training course is available for review in the ANGEL CAE course section 6c **[LINK REMOVED FOR CONFIDENTIALITY]**

2.) Logon Security Banner on all AACC Computers: As part of the security policies and procedures, when students, faculty, and staff attempt to logon to college computers, they see a security banner and must agree to comply with the college policies in order to access any computer resources. The following document shows a copy of the login banner. See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/LogonSecurityBanner.pdf

3.) Security Related Awareness and Help on the College Website: On its main website, accessible to anyone, AACC provides cyber security awareness information related to e-mail security, online shopping, online threats, protecting personal information, protecting your PC, social networking and wireless security. Such information is provided in collaboration with StaySafeOnline.org See: http://www.aacc.edu/cybersecurity/

4.) Security Related Awareness and Help on the Secure Password-Protected MyAACC Portal: The secure MyAACC portal supports students, faculty, and staff processes such as salary, pay advices, registration, record review, access to courses, and access to grades. A tab is devoted to cyber security. Through this tab, AACC provides cyber security awareness information related to e-mail security, online shopping, online threats, protecting personal information, protecting your PC, social networking and wireless security. Such information is provided in collaboration with StaySafeOnline.org. See: http://ola2.aacc.edu/CAEDocs1/Support%20Documents/CyberSecurityTabMYAACC.pdf

5.) Institution-Wide Communication Regarding IA Awareness: As part of its college website, AACC provides the public with information regarding its Integrated Technology Plan, IS Annual Reports (with descriptions of cyber security planning and implementations), InfoTech Newsletters (often include cyber security information), awards, and a lengthy list of Technology Resources available at AACC. See: http://www.aacc.edu/technology/
The October 2009 IS InfoTech newsletter is entirely devoted to cyber security awareness. See: http://www.aacc.edu/technology/file/CyberSecurityOct2009.pdf

Back to top

Total MINIMUM Point Requirement: 57
Total MAXIMUM Points Available: 108
MINIMUM POINTS REQUIRED TO QUALIFY AS AN IA CENTER OF ACADEMIC EXCELLENCE: 57
Minimum points must be met for each of the six criteria.