National IA Education and Training Center of Excellence
Program for 2 Year Institutions
Criteria for Measurement – October 2009

The National Information Assurance Education & Training Centers of Excellence 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

PGCC Application Letter (click here to view)

(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 IA Education and Training Center of Excellence 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 the 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)
4011	**Date: 06/01/2007**
4012	Date
4013	**Date: 06/01/2009**
4014	Date
4015	Date
4016	Date

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

Section 1a. (as well as several of the other sections in this application) can first be addressed by describing Prince George's Community College's (PGCC's) various efforts over the past four (4) years leading the NSF CyberWatch Center (http://www.cyberwatchcenter.org/) which includes thirty-six (36) academic institutions in fifteen (15) states and twenty-eight (28) Government, Industry, and Professional Organization partners that are focused on building and maintaining a stronger Information Assurance (IA) workforce. PGCC has greatly benefited from CyberWatch programs and efforts, such as:

1. consortium participants' collaboration to share best practices, methodologies, curricula, and course materials and modules
2. faculty IA training through CyberWatch-supported seminars, workshops, and short courses

3. tuition reimbursement to faculty for taking graduate level IA courses that lead to an IA Certificate or graduate IA degree (PGCC faculty participants included Bob Spear, Sally Sullivan, Michael Burt, and Trang Nguyen)
4. articulation agreements development between two (2) year colleges and four (4) year institutions for IA certificates and degree programs
5. articulation agreements development between high schools and two (2) year colleges
6. student IA contests in cyber defense (CCDC), digital forensics, and security awareness
7. scholarships, internships, and job fairs
8. an extensive and robust K-12 program for teachers, counselors, and students
9. significant outreach and dissemination initiatives to the public
10. aggressive marketing program to attract new members
11. support to CyberWatch members for creating IA programs, developing their curriculum, and guidance on mapping their programs to CNSSTS 4011 and 4013 standards.

Specific examples of PGCC faculty and staff participating in strategic partnerships to share curriculum with other institutions include:

1. Michael Burt, a PGCC full-time faculty and a member of the CyberWatch Leadership Team, is working with CyberWatch, BRAC, and MAISA. As a member of the CyberWatch Leadership Team, Michael Burt is responsible for:
    a) Coordinating all local PGCC CyberWatch activities
    b) Coordinating consortium-wide efforts for the CyberWatch Faculty Graduate Program, Student Internship Program, and Video/Poster Security Awareness Contest
    c) Being an active member on the following CyberWatch committees:
        1) Curriculum Development
        2) K-12 Program
        3) Student Competitions
        4) Marketing
        5) Outreach
    d) Attending all CyberWatch Leadership, Advisory Board, Consortium, and National Visiting Committee meetings
    e) Conducting formal and informal CyberWatch presentations to other academic institutions (including (K-12), Industry, and the general public.
    f) Working with other CyberWatch consortium academic faculty members in supporting the CyberWatch K-12 Principal Investigator (PI), Dr. Davina Pruitt-Mentle, develop IA curriculum and activities for area high schools and middle schools (just recently meeting with Joppatowne High School (POC: Leah Skica) which included Michael Burt and Bob Spear from PGCC) to discuss how to utilize a portion of CyberWatch curriculum materials into their high school curriculum.
2. Sally Sullivan, a PGCC full-time faculty and CIS Department Chair, served for the past two years as the CyberWatch Project Manager and a member of the

CyberWatch Leadership Team. She was in charge of all activities that Michael Burt assumed last year.

3. Ajay Gupta working with other academic institutions, professional organizations, and local, state, and federal government agencies
    a) Letter of Appreciation for participating in the C3 Conference for K-12.
4. Barry Bugg working with the BRAC grant developing an online version of CIS 1700 ***(****CyberWatch common course equivalent: CW 130).*
5. Bill Lauffer, along with several other PGCC ENT faculty, operating a CISCO Regional Academy that has trained all of the current Cisco instructors for Prince George's County Public Schools, District of Columbia Public Schools, and for other schools and colleges. Mr. Lauffer's PGCC faculty team have provided update training for all the local academies when the Cisco curriculum undergoes major updates and have a formal articulation agreement with the Prince George's County Public Schools that enables high school students to receive college credit for their Cisco courses.
6. Bob Spear, Current PI and Director of CyberWatch, working to expand the CyberWatch Consortium to its current thirty-six (36) academic institutions and twenty-eight (28) partners from industry, government agencies, and professional associations.

These faculty have been working in close partnership with CyberWatch faculty on the development of the common shared IA curriculum. Currently they are involved in revising the model curriculum, an effort that is involving several business members of the CyberWatch Advisory Board.

b. Shared Faculty (e.g., Faculty on curriculum development committee for more than one institution)
Point Value: Up to 5 points

As outlined in the general CyberWatch description in section 1a., PGCC is involved with thirty-six (36) academic institutions across the nation in developing IA curriculum which is shared with all members. Michael Burt, from PGCC, is on the CyberWatch Curriculum Committee and is currently working on curriculum revisions to the CW 235 (CIS 1660 Network Defense and Countermeasures) course as well as supporting other faculty members from other institutions working on other CW course revisions. In addition, Mr. Burt and Barry Bugg from PGCC worked on the BRAC grant with faculty from other academic institutions to conduct IA curriculum development, specifically transforming all IA certificate required courses to an online format to be shared with all Maryland Online members. Another example is Ajay Gupta working with other academic institutions, professional organizations, and local, state, and federal government agencies.

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

As previously mentioned in section 1a and 1b, all of the PGCC IA certificates required courses (along with many of the electives) have now been converted to online format which allows a student to finish either of the IA certificates completely online.(the final three courses were converted by Michael Burt (PGCC), Barry Bugg (PGCC), and Paul Derdul (AACC) through the BRAC grant. Seats in these courses are also made available to all Maryland Online members. The CyberWatch Curriculum Committee is currently working on ensuring that all CyberWatch curriculum courses are available online. In addition, Mr. Burt is one of a few PGCC faculty members piloting a synchronous lecturing technology with all of his online courses. PGCC has integrated the Wimba web application suite into the institution's Blackboard system and allows instructors to provide weekly live lectures that are recorded for the students unable to attend the live lectures or for students who wish to listen to the lectures again. The following are screenshots from previous online courses taught by Michael Burt that utilized Wimba:

1. Blackboard Fall 2009
2. Blackboard Spring 2009
3. Blackboard Summer 2009
4. Wimba Live Classroom

In addition, PGCC has an extensive online training system for all faculty and staff through the Skillsoft product Skillport (http://www.skillport.com/products/SkillPort/default.asp) that offers a variety of online training that includes many information assurance topics including information security, network security, risk management, and prep courses for many professional IA certifications ($(ISC)^2$, Cisco, CompTIA, PMI, Microsoft, etc.). The following are screenshot examples from the PGCC Skillport online catalog:

1. http://academic.pgcc.edu/cios/CAE2YR/skillport01.pdf
2. http://academic.pgcc.edu/cios/CAE2YR/skillport02.pdf

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

As described in the general CyberWatch description above in section 1a., PGCC working with other CyberWatch Consortium members are actively involved in providing IA students with internships, industry and academic mentors, and access to IA practitioners in a variety of ways.

Specific examples of PGCC providing students with access to IA practitioners include:

1. In October of 2009 PGCC students, in preparation for the 2010 CCDC, participated in the Cyber Challenge called Cyber Dawn which was held in Haymarket, VA. In addition to competing, students were given the opportunity to interact with several IA industry and government experts who included the IA experts from White Wolf Security who made up the Red Team Attackers that the student had to defend their network systems during the exercise.

2. In December of 2009 PGCC students participated in a CCDC practice session that was hosted at Towson University and comprised of four (4) CyberWatch academic member institutions battling each other to protect their own systems and attack the IT assets of the other teams.
3. Ajay Gupta participated in Computer Career Forum
4. On more than one occasion Allen Berg from Capitol College was a guest lecturer at PGCC through the STEM Collegian Center and CyberWatch talking with students about IA careers in the Intelligence field.
5. Another STEM Collegian Center activity involved a field trip to the Cryptology Museum at Fort Meade to learn more about this field and job opportunities at NSA.
6. PGCC faculty/staff have directly served as guest speakers on a number of occasions at a variety of events; for example:
    a) Ajay Gupta - presented at C3 conference (3 years)
        1) Letter of Appreciation for participating in the C3 Conference
    b) Ajay Gupta – presented at middle and high school programs (careers in IA)
    c) Michael Burt – presented at IA career pathway event (BRAC grant)
    d) Sally Sullivan - presented at IA career pathway event (BRAC grant) and Guidance/Career counselor workshop
    e) Bob Spear – presented at the HI-TEC Conference (July 2009, Phoenix, Arizona), Mid-Pacific ITC Conference (San Francisco, January 2009), National Career Pathways Network Conference (Atlanta, Georgia, October 2009), University of Cape Coast Faculty Colloquium (Cape Coast, Ghana, September 2008), National University of Rwanda Faculty Colloquium (Butare, Rwanda, October 2008), FISEA Conference (2009).

---

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

PGCC offers the following degrees/certificates:

1. Information Security - A.A.S. Degree (page 69 in PGCC 2009/2010 catalog (page 71 in linked PDF file))
2. Information Security - Certificate (page 69 in PGCC 2009/2010 catalog (page 71 in linked PDF file))
3. Information Security Management - Certificate

The above degree/certificates are comprised of the following IA program courses:

1. **CIS 1010 Computer Literacy. 3 Credits**
   (CyberWatch common course equivalent: CW 120.). Computer literacy is a survey course in evolving computer technology and its relevance to individuals and society. The societal issues stressed include: privacy, security, ergonomics, accessibility, intellectual property, pervasive computing, as well as other timely topics such as new laws impacting computer use. Becoming fluent in necessary technology applications is integrated into the course and may include such topics as word processing, use of e-mail and Web browsers, spreadsheets, distance learning platforms and others.
   (page 105 in PGCC 2009/2010 catalog (page 107 in the linked PDF file))

   This course was used for NSTISSI 4011 mapping

2. **CIS 1400 Introduction to Local Area Networks. 3 Credits**
   An overview of local area networks and the role these systems play in complete information systems. Emphasis will be placed on LAN hardware, software, standards and protocols Prerequisite: CIS 1010 or ENT 1770.
   (page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

   This course was used for NSTISSI 4011 mapping

3. **CIS 1700 Understanding Operating Systems. 3 Credits**
   (CyberWatch common course equivalent: CW 130.). Provides basic working knowledge of computer operating system commands, functions and management using the DOS, Windows, Linux and Unix operating environments. Topics include: memory management, process management, device management, file management and operating system tools. Introduces command structures and explores operations using GUI and Command Language Interfaces. Students will demonstrate proficiency by completing various task-related laboratory assignments. Focus also is on the main topics covered in the A+ Operating Systems Technologies Examination. Prerequisites: Reading proficiency; CIS 1010 or ENT 1770. 2 class/2 lab hours.
   (page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

   This course was used for NSTISSI 4011 mapping

4. **CIS 1620 Computer Security, Security+. 3 Credits**
   (CyberWatch common course equivalent: CW 160). This introduction to security systems will give students a solid foundation of understanding in different computer security concepts, functions and applications. The course maps to Comptia Security+ exam objectives which cover general security concepts, communication security, infrastructure security, basics of cryptography and operations/organizational security. Upon completion of this course, students will

be prepared to take Comptia's vendor neutral Security+ exam. Security+ certification is globally recognized as equivalent to an entry-level security specialist. The Security+ exam is accepted as one of the security certification exams by Microsoft toward its MCSA and MCSE certification. Prerequisite: CIS 1010; CIS 1700 recommended. 2 class/2 lab hours.
(page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

This course was used for NSTISSI 4011 and 4013 mappings

5. **CIS 1630 Securing the Network Infrastructure. 3 Credits**
(CyberWatch common course equivalent: CW 225). Provides the skills needed to implement security in an existing network. The course covers operating system hardening, router security, firewall systems, intrusion detection systems, virus protection, virtual private networks (VPN), TCP packet analysis and disaster recovery. Prerequisites: CIS 1620 and CIS 1700. 2 class/ 2 lab hours. (This course is undergoing content modification and name change to Tactical Perimeter Defense and prepares the student for taking the Tactical Perimeter Defense exam (SC0-451) for the Security Certified Network Specialist (SCNS) certification)
(page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

6. **CIS 1660 Network Defense and Countermeasures. 3 Credits**
(CyberWatch common course equivalent: CW 235). Focuses on the understanding of the network security architecture. The course covers network attacks and defenses, firewall systems, network design and configuration, virtual personal networks (VPN) configuration, intrusion detection system design and configuration, intrusion signatures and network security policies and configurations. Prerequisite: CIS 1630. 2 class/2 lab hours. (This course is undergoing content modification and name change to Strategic Infrastructure Security and prepares the student to take the Strategic Infrastructure Security exam (SC0-471) for the Security Certified Network Professional (SCNP) certification.)
(page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

This course was used for NSTISSI 4013 mapping

7. **CIS 2300 Windows Network Operating System Administration. 3 Credits**
(CyberWatch common course equivalent: CW 232). Students will learn basic Windows network operating system administration and configuration. Topics covered include installing/configuring the Windows operating system, troubleshooting, network protocol implementation and basic system security. This course charges an additional $32.00 per credit hour Information Technology Certification fee. Prerequisites: CIS 1010. CIS 1400 recommended. 2 class/2 lab hours.
(page 107 in PGCC 2009/2010 catalog (page 109 in the linked PDF file))

8. **CIS 2310 Windows Server Administration. 3 Credits**
   (CyberWatch common course equivalent: CW 230). Students will learn Windows Server administration and configuration. Topics covered include installing Windows Server operating system, configuring network services, managing system access, troubleshooting devices, monitoring and optimizing system performance, implementation of virtual private networks (VPNs) and system security configuration. This course charges an additional $32.00 per credit hour Information Technology Certification fee. Prerequisite: Recommended—CIS 2300 completed or concurrent. 2 class/ 2 lab hours.
   (page 107 in PGCC 2009/2010 catalog (page 109 in the linked PDF file))

   This course was used for NSTISSI 4011 mapping

9. **CIS 2690 Information Security Capstone. 3 Credits**
   (CyberWatch common course equivalent: CW 270). This capstone course in the Information Security A.A.S. degree program should be taken near the end of the student's program of study. Students will be required to analyze, research, design, and develop a fully-documented network attack strategy. Functioning in teams, students will design a strategy for attacking a fictitious network. The teams will defend their network attack strategy during class presentations. Prerequisite: CIS 1620; CIS 1660 recommended. 2 class/2 lab hours. (This course is undergoing a name change to CISSP Prep)
   (page 108 in PGCC 2009/2010 catalog (page 110 in the linked PDF file))

   This course was used for NSTISSI 4011 and 4013 mappings

10. **CIS 2720 UNIX/Linux Operating System. 4 Credits**
    (CyberWatch common course equivalent: CW 140). An introduction to the features of the UNIX/Linux operating system, including the file system, with an emphasis on programming using a UNIX/Linux shell. The course is conducted on an IBM System zSeries mainframe computer. Prerequisite: CIS 1030 or CIS 1130 or CIS 1200. 3 class/3 lab hours. .
    (page 108 in PGCC 2009/2010 catalog (page 110 in the linked PDF file))

11. **CIS 2760 UNIX/Linux System Administration. 4 Credits**
    (CyberWatch common course equivalent: CW 241). An introduction to the procedures and concepts related to the functions of a UNIX/Linux system administrator. Topics include interdependencies of file systems, backups and restores, management of user accounts, peripheral devices, troubleshooting and security. The course is conducted on an IBM System zSeries mainframe computer. Prerequisite: CIS 1700. 3 class/3 lab hours.
    (page 108 in PGCC 2009/2010 catalog (page 110 in the linked PDF file))

12. **CIS 2840 Systems Analysis. 4 Credits.** A structured approach to analysis, design and development of computer information systems, including a team project and research assignment. This capstone course in the Computer Information Systems

A.A.S. and Information Science A.S. programs should be taken near the end of the student's program of study. Prerequisites: Students should have completed a minimum of 18 credits of CIS coursework prior to enrolling in this course. 3 lecture/3 lab hours. (This course has undergone content modification and name change to Systems Analysis and Project Management)
(page 108 in PGCC 2009/2010 catalog (page 110 in the linked PDF file))

13. **ENT 1940 Router Technology I: Network Fundamentals. 4 Credits**
(CyberWatch common course equivalent: CW 150). First of a four-course sequence to prepare for CCNA certification. TCP, UDP and IP protocols; Ethernet concepts and operation; network subnetting; basic router configuration commands. This class charges an additional $32.00 per credit hour Information Technology Certification fee. 3 class/2 lab hours.
(page 119 in PGCC 2009/2010 catalog (page 121 in the linked PDF file))

14. **ENT 1950 Router Technology II: Routing Protocols. 4 Credits**
(CyberWatch common course equivalent: CW 151). Configuration of RIPEIGRP and OSPF routing protocols; configuration of static routes. Design, configuration and troubleshooting of VLSM networks. This course charges an additional $32.00 per credit hour Information Technology Certification fee. Prerequisite: ENT 1940. 3 class/2 lab hours.
(page 119 in PGCC 2009/2010 catalog (page 121 in the linked PDF file))

15. **ENT 1960 Router Technology III: LAN Switching and Wireless. 4 Credits**
(CyberWatch common course equivalent: CW 250) Design, configuration and troubleshooting of switched LANs, including virtual LANs, trunking and spanning tree. Design, configuration and troubleshooting of wireless networks, including security and privacy components. This course charges an additional $32.00 per credit hour Information Technology Certification fee. Prerequisite: ENT 1950. 3 class/2 lab hours.
(page 120 in PGCC 2009/2010 catalog (page 122 in the linked PDF file))

16. **ENT 1970 Router Technology IV: Wide Area Networks. 4 Credits**
(CyberWatch common course equivalent: CW 251). Configuring NAT, PAT and DHCP to increase usable addresses. Access lists and other security measures. Design, configuration and troubleshooting of wide area networks using PPP or frame relay. This course charges an additional $32.00 per credit hour Information Technology Certification fee. Prerequisite: ENT 1960. 3 class/2 lab hours.
(page 120 in PGCC 2009/2010 catalog (page 122 in the linked PDF file))

This course was used for NSTISSI 4011 mapping

17. **ENT 2190 Wireless LANs. 3 Credits**
(CyberWatch common course equivalent: CW 245). Principles of wireless communications, protocols and standards used to build, configure, secure and troubleshoot WLANs. Covers basic and extended WLANs (BSS, IBSS and ESS)

Preparation for CWNA certification. Prerequisite: ENT 1890 or ENT 1940 completed. ENT 2730 recommended but not required. 2 class/2 lab hours.
(page 120 in PGCC 2009/2010 catalog (page 122 in the linked PDF file))

18. **FOS 2600 Computer Forensics I. 3 Credits**
(*CyberWATCH common course equivalent: CW 170).* The investigation of computer-related crime, such as threatening e-mail, child pornography and Internet-related crimes. (Formerly FOS 160.) Students may not receive credit for both FOS 160 and FOS 2600. Prerequisites: CIS 1010 and FOS 2500. 2 class/2 lab hours.
(page 124 in PGCC 2009/2010 catalog (page 126 in the linked PDF file))

19. **FOS 2610 Computer Forensics II. 3 Credits.** An examination of advanced concepts in computer forensic analysis and computer-related crime, including data hiding techniques, encryption, electronic password cracking and password recovery tools. Prerequisite: FOS 2600. 2 class/2 lab hours.
(page 124 in PGCC 2009/2010 catalog (page 126 in the linked PDF file))

20. **MGT 1900 Introduction to Public Administration. 3 Credits**. An overview of public administration and its principles, evolution and current issues. Examine the role of government and nonprofit organizations in society.
(page 131 in PGCC 2009/2010 catalog (page 133 in the linked PDF file))

21. **MGT 2860 Cyber Law. 3 Credits**. Examines current and emerging cyber law issues that are critical to business, government and individuals. Students will examine jurisdiction; protection of intellectual property; contracts and licensing agreements; sales tax; raising equity capital online; privacy; obscenity in cyberspace; defamation; internet and information security; computer crime; and ethics. The goal is to address these issues in a practical, business-oriented manner and to advance sophistication in the field. As this is a dynamic discipline, subject areas and course materials may vary, as needed, with future developments in the field. Prerequisite: Reading proficiency. BUS 1220 recommended.
(page 132 in PGCC 2009/2010 catalog (page 134 in the linked PDF file))

22. **MGT 2880 Disaster Recovery and Risk Management. 3 Credits.** Provides individuals and organizations with tools to prepare for and recover from both natural and man-made disasters. Students will gain an understanding of risk and crisis management, the need for business continuity and information assurance planning, as well as addressing the leadership, human, organizational and public policy components of disasters. The final project will be a disaster recovery management plan. Prerequisite: Reading proficiency.
(page 133 in PGCC 2009/2010 catalog (page 135 in the linked PDF file))

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

PGCC has articulation agreements with the following institutions and alliances of institutions:

1. Capitol College (click here to view agreement)
2. Maryland Alliance for Information and Security Assurance (MAISA)
    a) (click here to view agreement)
    b) (click here to view list of alliance members)
3. Towson University (click here to view agreement)
4. University of Baltimore (click here to view agreement)
5. University of Maryland University College (see page 6 of the UMUC 2009-2010 Undergraduate Catalog (page 8 in the linked PDF file)) (click here to view agreement)

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

In addition to being a Cisco Local Academy, teaching our own PGCC students, PGCC is also a Cisco Regional Academy (follow link and type in PGCC zip code "**20774**"), responsible for training and evaluating Local Academies. Our regional academy has trained all of the Cisco current instructors for Prince George's County Public Schools, District of Columbia Public Schools, and for other schools and colleges. We have provided update training for all the local academies when the Cisco curriculum undergoes major updates. We also have an articulation agreement with the Prince George's County Public Schools that enables high school student to receive college credit for their Cisco courses.

Although no other formal articulation agreements have been formed with high schools, CvberWatch and PGCC support several annual events geared towards facilitating IA awareness and training for K-12 faculty, administrators, and students which include:

1. the Annual Cyberethics, safety and security (C3) conference
2. the Annual Careers in IS/IA/Digital Forensics workshop for guidance Counselors
3. the Annual Cool Careers in Cybersecurity for Girls Workshops

Finally, PGCC and CvberWatch in partnership with the University of Maryland and CvberWatch supported Digital Forensics Lab has hosted several Digital Forensic workshops for faculty, law enforcement and K12 system administration.

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

PGCC has established a long legacy of instilling a desire for academic competiveness in our students beginning several years ago with Math competitions and evolving now into the IA discipline with the following competitions:

1. Security Awareness Contests (PGCC student placed 2nd in national Educause competition 2009)

2. Forensic Cup Competition - PGCC placed first in 2008 (see page 7)
3. Forensic Cup Competition - PGCC tied for first in 2009
4. In October of 2009 PGCC students in preparation for the 2010 CCDC participated in Cyber Challenge called Cyber Dawn which was held in Haymarket, VA. In addition to competing students were given the opportunity to interact with several IA industry and government experts who included the IA experts from White Wolf Security who made up the Red Team Attackers that the student had to defend their network systems during the exercise.
5. In December of 2009 PGCC students participated in a CCDC practice session that was hosted at Towson University and comprised of four (4) CyberWatch academic member institutions battling each other to protect their own systems and attack the IT assets of the other teams.
6. In January 2010 PGCC participated in CCDC

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

Almost all of the technical courses in the IA degree and certificate programs include hands-on training in the curriculum. Not only do the following courses include weekly hands-on lab exercises but the courses are geared toward preparing the student to take Industry approved certification exams such as the Security+, SCNS, and SCNP certifications:

1. **CIS 1620 Computer Security, Security+. 3 Credits**
   (CyberWatch common course equivalent: CW 160). This introduction to security systems will give students a solid foundation of understanding in different computer security concepts, functions and applications. The course maps to Comptia Security+ exam objectives which cover general security concepts, communication security, infrastructure security, basics of cryptography and operations/organizational security. Upon completion of this course, students will be prepared to take Comptia's vendor neutral Security+ exam. Security+ certification is globally recognized as equivalent to an entry-level security specialist. The Security+ exam is accepted as one of the security certification exams by Microsoft toward its MCSA and MCSE certification. Prerequisite: CIS 1010; CIS 1700 recommended. 2 class/2 lab hours.
   (page 106 in PGCC 2009/2010 catalog (page 108 in linked PDF file))

   The CIS 1620 course utilizes a commercial web-based application to tunnel in to virtual machines that have live internet connections and allow the students to perform a variety of IA lab assignments.

2. **CIS 1630 Securing the Network Infrastructure. 3 Credits**
   (CyberWatch common course equivalent: CW 225). Provides the skills needed to implement security in an existing network. The course covers operating system hardening, router security, firewall systems, intrusion detection systems, virus protection, virtual private networks (VPN), TCP packet analysis and disaster

recovery. Prerequisites: CIS 1620 and CIS 1700. 2 class/ 2 lab hours. (This course is undergoing content modification and name change to Tactical Perimeter Defense and prepares the student for taking the Tactical Perimeter Defense exam (SC0-451) for the Security Certified Network Specialist (SCNS) certification) (page 106 in PGCC 2009/2010 catalog (page 108 in linked PDF file))

The CIS 1630 face-to-face course is taught in a computer lab classroom where each student has access to computer with multiple operating systems installed which they can download a variety of IA software tools to use in their lab assignments. The online course version of CIS 1630 offers the instructor two options for providing students hands-on experience. The course can be taught in a hybrid format where students can come to campus to use the same computer lab classroom with the face-to-face course or the instructor can provide the online students with Live CDs for them to use for the lab exercises.

3. **CIS 1660 Network Defense and Countermeasures. 3 Credits**
(CyberWatch common course equivalent: CW 235). Focuses on the understanding of the network security architecture. The course covers network attacks and defenses, firewall systems, network design and configuration, virtual personal networks (VPN) configuration, intrusion detection system design and configuration, intrusion signatures and network security policies and configurations. Prerequisite: CIS 1630. 2 class/2 lab hours. (This course is undergoing content modification and name change to Strategic Infrastructure Security and prepares the student to take the Strategic Infrastructure Security exam (SC0-471) for the Security Certified Network Professional (SCNP) certification.)
(page 106 in PGCC 2009/2010 catalog (page 108 in linked PDF file))

The CIS 1660 utilizes the same hands-on instruction methods as described in the previous CIS1630 course.

4. **CIS 1700 Understanding Operating Systems. 3 Credits**
(CyberWatch common course equivalent: CW 130.). Provides basic working knowledge of computer operating system commands, functions and management using the DOS, Windows, Linux and Unix operating environments. Topics include: memory management, process management, device management, file management and operating system tools. Introduces command structures and explores operations using GUI and Command Language Interfaces. Students will demonstrate proficiency by completing various task-related laboratory assignments. Focus also is on the main topics covered in the A+ Operating Systems Technologies Examination. Prerequisites: Reading proficiency; CIS 1010 or ENT 1770. 2 class/2 lab hours.
(page 106 in PGCC 2009/2010 catalog (page 108 in the linked PDF file))

The CIS 1700 face-to-face course is taught in a computer lab classroom where each student has access to a computer with multiple operating systems installed

which they use for their lab assignments. For the online version of this course the instructor provides the students with Live CDs for them to use for the lab exercises.

---

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

In every course in which students produce work in electronic files such as documents, spreadsheets, presentations, etc., emphasis is placed on Information Assurance when students learn to maintain the integrity of their files by being aware of malware that could damage their files. Courses in the Liberal Arts in particular incorporate this information when students work with electronic files in their courses.

Accounting courses, particularly those after the first course, emphasize controls that maintain data integrity and confidentiality. These controls facilitate having the correct accounting information available to those whose job requires it. Another practice that students learn about is the separation of duties, which is a core concept of Information Assurance.

The college offers degrees in Criminal Justice and in the Health Sciences, where Information Assurance concepts are important in areas such as evidence collection, HIPPA compliance and the like.

A final example is from the education programs:

In education courses, students focus on confidentiality of student records, testing information, and student/family information. This includes hard copy information as well as online information.

The education classes referenced above include:

1. ECE 1560: Introduction to Early Childhood Special Education
   on page 113 in PGCC 2009/2010 catalog (page 115 in linked PDF file))

2. ECE 1540: Observing and Recording Child Behavior
   on page 113 in PGCC 2009/2010 catalog (page 115 in linked PDF file))
3. ECE 1050: Principles and Practices in Early Childhood Education
   on page 112 in PGCC 2009/2010 catalog (page 114 in linked PDF file))
4. EDU 2000: Foundations of Education
   on page 115 in PGCC 2009/2010 catalog (page 117 in linked PDF file))
5. EDU 2030: Introduction to Special Education
   on page 115 in PGCC 2009/2010 catalog (page 117 in linked PDF file))

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

The following non-technical courses of study are electives in the Information Security Management Certificate (http://academic.pgcc.edu/cios/Degrees.htm#ISMC):

1. **MGT 1900 Introduction to Public Administration. 3 Credits**. An overview of public administration and its principles, evolution and current issues. Examine the role of government and nonprofit organizations in society.
   (page 131 in PGCC 2009/2010 catalog (page 133 in linked PDF file))

2. **MGT 2860 Cyber Law. 3 Credits**. Examines current and emerging cyber law issues that are critical to business, government and individuals. Students will examine jurisdiction; protection of intellectual property; contracts and licensing agreements; sales tax; raising equity capital online; privacy; obscenity in cyberspace; defamation; internet and information security; computer crime; and ethics. The goal is to address these issues in a practical, business-oriented manner and to advance sophistication in the field. As this is a dynamic discipline, subject areas and course materials may vary, as needed, with future developments in the field. Prerequisite: Reading proficiency. BUS 1220 recommended.
   (page 132 in PGCC 2009/2010 catalog (page 134 in linked PDF file))

3. **MGT 2880 Disaster Recovery and Risk Management. 3 Credits.** Provides individuals and organizations with tools to prepare for and recover from both natural and man-made disasters. Students will gain an understanding of risk and crisis management, the need for business continuity and information assurance planning, as well as addressing the leadership, human, organizational and public policy components of disasters. The final project will be a disaster recovery management plan. Prerequisite: Reading proficiency.
   (page 133 in PGCC 2009/2010 catalog (page 135 in linked PDF file))

4. **General Education Requirements.** Maryland statue requires community colleges to include general education requirements in all degree programs in the five areas of English composition, humanities, mathematics, science, and social science. PGCC conducted a Self-Study analysis and Chapter 12 of that report best describes how all degree-seeking students are exposed to values, ethics, and

diversity in the general education courses. General Education courses are listed in the PGCC 2009/2010 catalog beginning on page 28 (page 30 in linked PDF file).

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

The following are examples non-credit/credit professional development courses in IA:

1. Non-Credit/credit courses include:
    a) Cyber Security
        1) CISSP prep taught non-credit by Ajay Gupta
    b) CISCO Networking
        1) CNT 305, 306, 307, and 308 taught by ENT faculty in CIS Department
2. Many professional development opportunities are offered to faculty, K-12 educators, guidance counselors and law enforcement personnel. These include:
    a) The Careers in IS/IA/Digital Forensics workshop is done in partnership with the Maryland State Department of Education. Counselors are given continuing education credit for attendance and follow up activity requirements (literature development and/or presentation)
    b) Some LEA from Maryland and all from New Jersey give continuing education credit for attendance at the C3 Conference
    c) Several two and four year institutions give faculty development compensation for attending the digital forensics workshops.

---

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

The following are examples of PGCC IA Outreach activities:

1. As mentioned above in 1a. CyberWatch has a very strong outreach activities program and PGCC's CyberWatch Outreach Committee member is Michael Burt
2. In addition to the CyberWatch Outreach Committee and as previously describe above, the CyberWatch K-12 program supported by PGCC faculty and staff conduct extensive outreach activities, for example:

a) Ajay Gupta – presented at middle and high school programs (careers in IA)
b) Michael Burt – presented at IA career pathway event (BRAC grant)
c) Sally Sullivan - presented at IA career pathway event (BRAC grant) and Guidance/Career counselor workshop
d) The Annual Cyberethics, safety and security (C3) conference
    1) Ajay Gupta - presented at C3 conference (3 years) Letter of Appreciate for participating in the C3 Conference
e) The Annual Careers in IS/IA/Digital Forensics workshop for guidance Counselors
f) The Annual Cool Careers in Cybersecurity for Girls Workshops

3. Ajay Gupta working with other academic institutions; professional organizations; local community; and local, state, and federal government agencies
4. Ajay Gupta representing PGCC at the Incident Management Strategies for Colleges and Universities Workshop for first responders (see page 7).
5. In addition to being a Cisco Local Academy, teaching our own PGCC students, the college is also a Cisco Regional Academy (follow link and type in PGCC zip code "**20774**"), responsible for training and evaluating Local Academies. Our regional academy has trained all of the Cisco current instructors for Prince George's County Public Schools, District of Columbia Public Schools, and for other schools and colleges. We have provided update training for all the local academies when the Cisco curriculum undergoes major updates.
6. Flyer mailed to high schools, colleges, businesses, and government agencies inviting them to a presentation at PGCC to market our new Information Security Management Certificate.

---

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)

Michael Burt

1. click here to view assignment memo from CIS Acting Department Chair
2. click here for Mr. Burt's curriculum vitae

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

The following individuals are all teaching IA courses at PGCC. They include five (5) full-time faculty, one (1) adjunct faculty, and one (1) administrative employee who also teaches as an adjunct faculty.

1. Sally Sullivan (faculty website)
2. Trang Nguyen (faculty website)
3. Melanie Walker (faculty website)
4. Barry Bugg (faculty website)
5. William Lauffer (faculty website)
6. Patricia Okorie
7. Ajay Gupta

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.*
Point Value: 5 points (required)

1. Michael Burt (CISSP and 33 IA graduate credit hrs)
2. Sally Sullivan (CISSP and 12 IA graduate credit hrs)
3. Trang Nguyen (15 IA graduate credit hrs)
4. Melanie Walker (MS Degree in IA)
5. Patricia Okorie (15 IA graduate credit hrs)

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

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 minimum / 20 maximum

---

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

The following are the pertinent PGCC security policies:

1. PGCC Technology Policies (Revised 7/18/07)
2. PGCC Technology Policies: Sec 3 Learning Technology Policy (changes)
3. PGCC Technology Policies: Sec 4 Administrative Technology Policy (changes)
4. PGCC Technology Policies: Sec 2.6 and Sec 6 Email Policies (changes)
5. PGCC Website Usage Policy

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

PGCC appointed Ajay Gupta as the Director of IT Security Services responsible for establishing and maintaining the security of enterprise resource planning system, mainframe, computing systems, networks, data, and workstations throughout the college.

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

1. All newly hired Faculty and Staff are required to take a Security Awareness Training Course that is administered online through the Skillsoft product Skillport (http://www.skillport.com/products/SkillPort/default.asp. In addition, the PGCC Skillport system has an extensive library of online training modules available to all faculty and staff that offers a variety of online training in information security, network security, risk management, and prep courses for many professional IA certifications ($(ISC)^2$, Cisco, CompTIA, PMI, Microsoft, etc.). The following are screenshot examples from the PGCC Skillport online catalog:

    a. http://academic.pgcc.edu/cios/CAE2YR/skillport01.pdf
    b. http://academic.pgcc.edu/cios/CAE2YR/skillport02.pdf

2. Ajay Gupta presents workshops to faculty and staff at the beginning of each semester and on PGCC's Professional Development Day (presentation slides used)
3. Security Banner on PC systems in the open labs
4. Security Banner on PC systems in the staff and faculty offices
5. Online GroupWise Email and Identity Theft Document
6. Winning Security Awareness Posters form the Educause national competition have been printed and are displayed throughout the PGCC campus buildings and were distributed to both CyberWatch member academic institutions as well as CyberWatch Industry/Government Agency partners.

Total MINIMUM Point Requirement: 57
Total MAXIMUM Points Available: 108
MINIMUM POINTS REQUIRED TO QUALIFY AS A CAE2Y: 57

Minimum points must be met for each of the 6 criteria.