College of Southern Maryland

National Centers of Academic Excellence for Information Assurance Education and Training Program for 2 Year Institutions (CAE2Y) Criteria for Measurement – October 2010

The National Information Assurance Education & Training Centers of Excellence program is open to nationally or regionally accredited 2-year Community Colleges, technical schools, state or federally endorsed IA/Cybersecurity training centers or U.S. Government IA/Cybersecurity training centers. 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.)

(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: NIETP Program Office
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 06/01/2009
4012	Date
4013	Date 06/01/2010
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

- As a member of the CyberWatch Consortium since its inception, CSM works closely with the consortium having utilized its model curriculum as the basis for our Information Systems Security (ISS) degree program.

- CSM has developed IA related curriculum which it has shared with the following partners:

    - The Corporate Center at CSM shares its Security+ and CISSP curriculum with corporate partners including:
        - Naval Air Systems Command

        - Naval Surface Warfare Center-Indian Head Division

    - Stay Safe in Cyberspace Workshop Materials shared with leaders of youth organizations, teachers and mentors as a part of outreach initiatives. (Example: Stay Safe in Cyberspace Presentation)

        - Calvert County Public School Teachers
        - Calvert Youth Downloading Inc. Mentors
        - Blessed Hope House Inc. Afterschool Program Mentors
        - Girls Scout Troop Leaders

- CSM serves as a Cisco Academy making available Cisco curriculum to credit and non-credit students.

- As the #1 technical training provider in Southern Maryland, CSM shares IA curriculum across its credit, non-credit, corporate-training and kids-college departments.

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

- Renee Jenkins–Professor of Business & Technology (serves as lead IA degree

program faculty member)
  - CyberWatch Liaison and Student Development Committee Member

- Jean Runyon – Adjunct Professor of Business & Technology (serves as an adjunct instructor for IA degree program)
  - Institute for the Future Advisory Team at Anne Arundel Community College Advisor
  - 2010-2012 Instructional Technology Council Chairperson

- Nicolas Valltos – Associate Professor of Criminal Justice (serves as law enforcement advisor for IA initiatives and degree program; teaches CJS-1050: Legal Issues in Security for the IA program)
  - Forensic Training Services and Police Training Services Trainer & Advisor
  - Southern Maryland Criminal Justice Academy Training Liaison

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

- Using WebCT, CSM currently offers the following web-based IA credit courses:
  Current list of online credit courses

  ITS-2090 Computer Security
  ITS-2940 Cyber Ethics
  ITS-2500 Ethical Hacking
  ITS-2545 Information Systems Security

- Using WebCT, CSM currently offers the following web-hybrid (blended) IA credit courses:
  Current list of web-hybrid courses

  ITS-2090 Computer Security
  ITS-2510 Cisco Networking 1
  ITS-2515 Cisco Networking 2
  ITS-2520 Cisco Networking 3
  ITS-2525 Cisco Networking 4

- In partnership with Ed2go, CSM currently offers the following web-based /IA non-credit courses:
  Current List of Online Non-Credit Courses

  ITS-8550 CompTIA Security+ Certification Prep
  ITS-8280 Introduction to PC Security
  ITS-8540 Advanced PC Security

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

- The following IA practitioners have been invited to speak to ITS2090, Introduction to Computer Security, classes:
  - Charles Baker (CSM Graduate & CSM Technology Specialist/Network Administrator, Topic: network security administration)
  - Rhonda Jenkins (Telecommunications Specialist, Topics: telecommunications and security)
  - Nicholas Valltos (Law Enforcement Trainer & Criminal Justice Instructor, Topics: homeland security, security clearances and the demand for computer forensics law enforcement officers)

- In partnership with Naval Air Systems Command, Robert Murphy, a IA Project Leader, serves as an adjunct IA/ISS faculty member.

- CSM students are provided opportunities to attend activities featuring IA speakers as well as IA technology demonstrations. This includes:

  - CSM Computer Users Group IA Show and Tell Sessions sponsored by IS and IA faculty members
    - Spring 2008 Session Topic: Essential Computer Security Tools sponsored by Renee Jenkins with help from Charles Baker
    - Spring 2009 Session Topic: How Networks Work sponsored by Daphne Powell & Bernice Brezina

  - Cyber Bullying Movie and Empowerment Workshop @ Human Rights Day 2010 Prince Frederick Campus

    Coordinator and presenter: – Associate Professor of Sociology, Lisa Lynk Smith

  - Technical Expositions like FOSE and the CSI Annual Conference

  - Women in Technology Day (2006-2008)-Janelle Martin (CSM graduate and former Calvert Memorial Hospital Web Administrator). Janelle demonstrated web development and security technologies as well as provided career information to students as well as other participants.

    Event sponsored by IA Instructors Renee Jenkins and Daphne Powell

  - Women in Math Day (2007-2010) featured IA Presenter: Julie Ryan PH.D.

    GWU Lead Professor, Information Security Management

    Dr. Ryan has taught cryptography workshops and provided career advice as a part of panel discussions.

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

- Information Systems Security A.A.S. Degree
  - Current Degree Description on website
  - Current Degree Description in catalog
    (page 122 in CSM 20100-2012 catalog; page 78 in linked PDF file)
- *Two certificates are pending academic approval: Cisco Networking and Network Security Administration.*

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

ITS Course Descriptions can be found on pages 206-211 in CSM 20100-2012 catalog.

ITS-1015 - THE INFORMATION AGE: EMERGING TECHNOLOGIES (3)
Prerequisite: RDG-0800 or placement
(CyberWatch common course equivalent: CW 120.). Students learn the core concepts of information technology and its rapidly expanding role in solving problems and influencing decision making. The course focuses on emerging technologies through discussion and demonstrations utilizing technology-based instructional material. Topics include the functions and applications of computer systems, hardware components, software basics, electronic databases, communication networks, computer graphics, and security. Independent exploratory learning projects are required.
Credit for this course may be earned through CLEP or DSST (formerly DANTES).

ITS-1020 - OPERATING SYSTEMS CONCEPTS (3)
Prerequisite: RDG-0800 or placement
(CyberWatch common course equivalent: CW 130.).Students are introduced to the principles of various types of microcomputer operating systems. Topics include system resources, memory management, processor management, user interface, and operating system functions. Major emphasis is placed on how the user, hardware, and software interface with the operating system. Various current operating systems will be covered in this course.
Credit for this course may be earned through departmental examination.

ITS-1960 - INTRODUCTION TO UNIX (3)
Prerequisite: ITS-1020
Students learn the basic concepts of the Unix operation system as it relates to computer hardware, software, and operations, and are introduced to basic Unix operation system commands, command syntax, file management and

maintenance, and the troubleshooting of user problems.

ITS-2090 - COMPUTER SECURITY (3)
Prerequisite: ITS-1015
(CyberWatch common course equivalent: CW 160.).This course covers the fundamentals of operational security, network security, managing a public key infrastructure (PKI), authentication, access control, external attack, and cryptography. Students learn about the security procedures to protect data in computer environments, the different network attack scenarios, the many tools and procedures used by organizations to protect their resources, and the ethical issues raised by computer security in the business world.
The course helps prepare students for the CompTIA Security+ exam. The vendor neutral CompTIA Security+ certification is the industry-acceptable, entry-level security certification and is also accepted as one of the security specialization exams required for the Microsoft MCSE 2003 track.
This course was used for NSTISSI 4011 and 4013 mappings.

ITS-2190 - MICROSOFT WINDOWS SERVER ENVIRONMENT (3)
Prerequisite: ITS-2120 or ITS-2185 or ITS-2510
(CyberWatch common course equivalent: CW 230.).This course teaches all skill sets related to the current Microsoft server including deployment, management, maintaining and monitoring of the server, and maintaining high availability of the servers in a network. This course will prepare a student to pass Microsoft exam 70-646 - Window Server Administration.

ITS 2230 - DESIGNING SECURITY FOR MICROSOFT WINDOWS SERVER 2003 NETWORK (3)
Prerequisite: ITS 2190
Course Grandfathered In 2006-2008 Catalog
Students gain the knowledge and skills to design a secure network infrastructure. Topics include assembling the design team, modeling threats, and analyzing security risks in order to meet business requirements for securing computers in a networked environment.

ITS 2240 IMPLEMENTING AND ADMINISTERING SECURITY IN A MICROSOFT WINDOWS SERVER 2003 NETWORK (3)
Prerequisite: ITS 2190
Course Grandfathered In 2006-2008 Catalog
Students learn to implement, manage, maintain, and troubleshoot security in a Windows Server 2003 network infrastructure and plan and configure a Windows Server 2003 PKI.

ITS-2500 - ETHICAL HACKING (3)
Prerequisite: ITS-2190, ITS-2530, ITS-2940
Students learn how intruders, including hackers, attack systems and networks as well as best ethical practices for scanning, auditing, penetration testing, and securing assigned systems. In addition, students will explore how intruders escalate privileges, strategies for preempting attacks and the legal and ethical nature of security countermeasures. Students can also use the course to prepare for Certified Ethical Hacker (CEH) exam.

ITS-2510 - CISCO NETWORKING I (4)
Prerequisite: ITS-1015 taken in the same or a previous semester
(CyberWatch common course equivalent: CW 150.).Students learn Cisco networking fundamentals and network terminology in this first of a four-course series of the Cisco Networking Academy Program leading toward Cisco Certified Network Associate (CCNA) designation. Topics covered include open system interconnection (OSI) model, ethernet technologies, network media, basics of TCP/IP, and IP addressing. Training is provided in the use of networking software and tools that are required to troubleshoot network problems.
This course was used for NSTISSI 4011 mapping.

ITS-2515 - CISCO NETWORKING 2 (4)
Prerequisite: ITS-2510
(CyberWatch common course equivalent: CW 151.).Students learn Cisco router and routing basics in this second of a four-course series of the Cisco Networking Academy Program leading toward Cisco Certified Network Associate designation. This course provides students with an understanding of TCP/IP, basic router configuration, installation of routing protocols, network troubleshooting skills, and configuration of Cisco IOS software and routing protocols. Training is provided in the use of networking software and tools that are required to troubleshoot network problems.

ITS-2520 - CISCO NETWORKING 3 (4)
Prerequisite: ITS-2515
(CyberWatch common course equivalent: CW 250.).Students learn Cisco switching basics and intermediate routing in this third of a four-course series of the Cisco Networking Academy Program leading toward Cisco Certified Network Associate designation. Topics covered include Ethernet switching, switch concepts, and configuration of switches using command-line interface. Training is provided in the use of networking software and tools that are required to troubleshoot network problems.

ITS-2525 - CISCO NETWORKING 4 (4)
Prerequisite: ITS-2520
(CyberWatch common course equivalent: CW 251.).Students learn WAN technology and terminology in this final course of a four-course series of the Cisco Networking Academy Program leading toward Cisco Certified Network Associate (CCNA) designation. Topics include ISDN and DDR, Frame Relay technologies, configuring PPP, level 1 troubleshooting service, DHCP for dynamic address management, and address translation with NAT and PAT. Training is provided in the use of networking software and tools that are required to troubleshoot network problems.

ITS-2530 - HARDENING THE INFRASTRUCTURE (3)
Prerequisite: ITS-2090
(CyberWatch common course equivalent: CW 225.).Students learn how to manage and apply technologies to protect networks. An understanding of security technologies including firewalls, IDS, virus protection, TCP packet sniffing and analysis, VPN (virtual private networks), disaster recovery, and operating system hardening will prepare the student to implement and maintain adequate protection of the infrastructure.

ITS-2535 - NETWORK DEFENSE AND COUNTERMEASURES (3)
Prerequisite: ITS-2530
(CyberWatch common course equivalent: CW 235.).Students gain a strong understanding of the structure for network defense in order to prepare for the Security Certified Network Professional Certification. The course focuses on the components dealing with network defense including VPN (virtual private network) configurations, firewalls, attacks and defense against networks, and devising and constructing intrusion detecting systems.

ITS-2545 - INFORMATION SYSTEMS SECURITY (3)
Prerequisite: ITS-2090
Students learn the management principles of information security. The course will cover many aspects of security including hardware, software, communication, and physical security. Security policy, legal and ethical issues will also be covered. The relationship between course topics and CISSP domains are also highlighted.
This course was used for NSTISSI 4011 and 4013 mappings.

ITS-2550 - DIGITAL FORENSICS (3)
Prerequisite: ITS-1020 and ITS-2090
This class will focus on essential components that a forensic investigator must know to investigate digital crime incidents. Students learn techniques behind digital forensic investigations and evidence collection and cover the fundamental steps of the traditional computer forensic methodology. Topics include building forensic workstations, collecting evidence, extracting artifacts, identifying unknown files, and reassembling evidence from network packet captures. This course is designed as hands-on sessions where evidence will be presented for digital forensic evaluation.

ITS-2900 - CAPSTONE EXPERIENCE (3)
Prerequisite: completion of 15 credits toward an Information Services Technology or Information Systems Security degree, in which 12 credits must be ITS courses; plus permission of division chair.
(CyberWatch common course equivalent: CW 270.).This capstone course provides hands-on and problem-solving experience in many areas of information technology. Students consolidate knowledge and skills gained in coursework in this capstone experience. This course focuses on working with actual business problems as represented in a major case study. Students will be required to complete an individual project, system, program, or research paper, which will enhance their skills and marketability.
This course was used for NSTISSI 4011 and 4013 mappings.

ITS-2910 - COOPERATIVE EDUCATION I: COMPUTER (3)
Prerequisite: completion of 15 credits toward an Information
Services Technology certificate or degree of which 12 credits must be ITS courses, plus permission of the division chair.
Cooperative education allows students to combine academic study with on-the-job experience by working on training assignments coordinated by departmental faculty. The major objective of cooperative education is the application of classroom theory in a work environment. This course is intended for students

who are pursuing a degree in information technology. Grading in this course is pass or fail.

ITS-2940 - CYBER ETHICS (3)
Prerequisite: RDG-0800 or placement
(CyberWatch common course equivalent: CW 110.).Students consider the safe and ethical use of computer technology including the Internet. They study the role of technology in today's society, cyber protection issues, and the moral challenges we face in using technology including cyber space. Topics to be included are: privacy, intellectual property, cyber abuse/crime, codes of conduct, policy development as well as the digital divide. In addition, students consider how the global and anonymous nature of the Internet makes it difficult to transfer standard rules of conduct to this virtual environment.

Non ITS Courses

CJS-1050 - LEGAL ISSUES IN SECURITY (3)
Prerequisite: none
Students study the major legal issues in criminal and civil law impacting the private security industry. Topics include self incrimination, search and seizure, electronic eaves-dropping, use of cameras, coerced confessions, right to counsel, illegal detention, use of deceptive devices, interrogation techniques, and professional ethical responsibilities.
(page 181 in CSM 20100-2012 catalog; page 15 in linked PDF file)

COM-1450 - GROUPS, TEAMS, AND LEADERSHIP (3)
Prerequisite: ENG-0900 and RDG-0800 or placement
Students learn leadership skills by working in teams to design and complete group projects. Students learn to plan, conduct, and participate in meetings. Student work includes working in groups outside of class, participating in service learning projects, and observing public groups and meetings.
(page 179 in CSM 20100-2012 catalog; page 13 in linked PDF file)

ENG-1010 - COMPOSITION AND RHETORIC (3)
Prerequisite: ENG-0900 and RDG-0800 or placement
Students receive instruction in planning, organizing, and developing a variety of compositions. They review the conventions of Standard American English, gain information literacy skills, and learn research and documentation techniques. Upon completion, students should be able to write unified, coherent essays nearly free of mechanical or structural errors, conduct online and print research, and document sources correctly. Students should refer to the schedule of classes for sections of this course taught in a computer lab and/or using an online writing lab. Computer-assisted sections will have an additional lab fee.
Credit for this course may be earned through CLEP or Advanced Placement Examination.
(page 192 in CSM 20100-2012 catalog; page 26 in 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

Due to changes in personnel, CSM is still in the process of finalizing articulations with the following 4 year institutions:

- Capitol College – Proposed Agreement (CC contact: Ken Crockett)
- University of Maryland University College – Proposed Agreement (UMUC contact: Jeff Tjiputra)

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 IA faculty and academic advisors participating in career fairs, open houses, tech prep meetings, etc. to facilitate awareness of Cisco tech prep opportunities, CSM academic advisors identify Cisco tech prep students that qualify for course credits. Currently, CSM program coordinators provide documented tech prep course equivalencies to academic advisors and tech prep coordinators. Student requests for tech prep credits are forwarded by academic advisors to Cisco Academy Coordinator for review.

General Tech Prep Information:
Cisco Tech Prep Agreement Letters

- Calvert County Public Schools
- Charles County Public Schools
- St. Mary's County Public Schools

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

- Johns Hopkins University's Annual Digital Forensics Competition 2009 Winners
- EDUCAUSE Information Security Awareness Poster & Video Contest 2011 Students enrolled in Fall 2009 courses have submitted posters.

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

The following required technical courses in the ISS degree and proposed certificate programs include hands-on training with several courses having been certified to have mapped to the CNSS 4011 and 4013 standards. In addition, many courses are geared towards helping students to prepare for industry certifications including A+, Security+, Linux+, MCSE and CCNA certifications. Other elective courses contain hands-on training or lab training as well.

- ITS-1020 - OPERATING SYSTEMS CONCEPTS
  This course is taught in both traditional, web hybrid, and web only

formats. Therefore, students utilize computer labs and own computers to complete weekly lab assignments. In addition students are taught to create Live CDs as well as virtual machines using Windows and Unix operating systems.

- ITS-2090 - COMPUTER SECURITY
  This course is taught in both web hybrid and web formats. Web Hybrid students are taught in computer labs. All students use online virtual lab simulation environment, Security+ LabSim.

- ITS-2190 - MICROSOFT WINDOWS SERVER ENVIRONMENT
  This course is taught in a traditional format in a dedicated MCSE computer lab. Along with learning to install and use server software, students are also taught to create virtual machines for use at home.

- ITS-2510 - CISCO NETWORKING 1
  This course is taught in both traditional and web hybrid formats. Students are taught in a dedicated Cisco computer lab as well as Cisco's online network plus router simulation environment, Packet Tracer.

- ITS-2515 - CISCO NETWORKING 2
  This course is taught in both traditional and web hybrid formats. Students are taught in a dedicated Cisco computer lab as well as Cisco's online network plus router simulation environment, Packet Tracer.

- ITS-2520 - CISCO NETWORKING 3
  This course is taught in both traditional and web hybrid formats. Students are taught in a dedicated Cisco computer lab as well as Cisco's online network plus router simulation environment, Packet Tracer.

- ITS-2525 - CISCO NETWORKING 4
  This course is taught in both traditional and web hybrid formats. Students are taught in a dedicated Cisco computer lab as well as Cisco's online network plus router simulation environment, Packet Tracer.

- ITS-2530 - HARDENING THE INFRASTRUCTURE
  This course is taught in both traditional and web formats. In traditional classes, students are taught in computer labs. Online as well as traditional students are given as well as taught to create own Live CDs, virtual machines and virtual networks.

- ITS-2535 - NETWORK DEFENSE AND COUNTERMEASURES
  This course is taught in both traditional and web formats. In traditional classes, students are taught in computer labs. Online as well as traditional students are given as well as taught to create own Live CDs, virtual machines and virtual networks.

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

The following is a sample of the degree programs in which non-technical/non-IA students are introduced to IA concepts:

- Accounting requires courses in computer applications and business law.
  - Computer application courses: lessons in cyber ethics as well as Internet, hardware, software and network security
    - BAD-1335
    - ITS-1015
  - BAD-2070 Business Law I; lessons in intellectual property, cyber and e-commerce law

- Business Administration requires courses in computer applications and business law.
  - Computer application courses: lessons in cyber ethics as well as Internet, hardware, software and network security
    - BAD-1335
    - ITS-1015
  - BAD-2070 Business Law I; lessons in intellectual property, cyber and e-commerce law

- Environmental Management requires courses in accounting practices, business management, and business ethics.
  - ACC-1015 Fundamentals of Accounting Practice; lessons in accounting data security standards and laws
  - BAD-1210 Principles of Management; lessons in role of management in information security and personnel management
  - PHL-1430 Business Ethics; lessons in technology/systems control, cyber law, cyber ethics, cyber crime, intellectual property, privacy law and dimensions of information security

- Homeland Security requires courses in homeland security and cyber ethics.
  - HLS-1015 Introduction to Homeland Security; lessons in law enforcement responsibilities, laws, policies and procedures related to cyber crime, information privacy and securing public technology infrastructure
  - ITS-2940 Cyber Ethics; lessons in dimensions of information security, privacy, intellectual property, cyber abuse/crime, codes of conduct, policy development and social implications of cyber security

- Hospitality Management requires a course in information systems.
  - HPM-2310 Management Information Systems for the Hospitality Industry; lessons in secure configuration of hardware, software, networks and applications as well as dimensions of information security
- Medical Coding Specialist (Certificate) requires courses in health information and computer applications.
  - HIT-1103 Introduction to Health Information; lessons in medical information security including confidentiality and compliance with HIPAA privacy regulations as well as AHIMA domains related to information security
  - ITS-1015 The Information Age: Emerging Technologies; lessons in cyber ethics as well as Internet, hardware, software and network security

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 Information Systems Security Degree program requires students to complete the following non-technical courses:

- 3 credits in Biological or Physical Science (AST, BIO, CHE, ENV, GEO, GRY, PHY)
- 3 credits in Communications (COM-1450 - Groups, Teams, and Leadership)
- 3 credits in English (ENG-1010 - Composition and Rhetoric)
- 3 credits in Math (MTH)
- 3 credits in Social/Behavioral Science (ECN, ENV, POL, SOC)

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

The following courses are offered as professional development courses for business professionals, healthcare providers, IT professionals, managers in occupational trades, military personnel, law enforcement personnel, etc.

- Healthcare Providers
  Both courses provide lessons in medical information security including confidentiality and compliance with HIPAA privacy regulations as well as AHIMA domains related to information security
  - HIT-1103 Introduction to Health Information (credit)
  - HTH 9600 Getting Ready for Electronic Medical Record Technology (non-credit)

- Information Security for Employees
  - BAD-7600 Corporate Employee Security and Safety (non-credit); lessons in identity theft and best cyber security practices
- Law Enforcement Personnel

- CJS-1020 Introduction to Security (credit); lessons in protecting information systems assets, disaster and recovery planning as well as cyber law
- CJS-1050 Legal Issues in Security (credit); lessons in cyber crime, cyber law, cyber ethics and electronic surveillance

- Managers in Occupational Trades
  - TEC-9910 Principles of System Safety (non-credit); lessons in information systems security risk management, software safety and security planning
  - TEC-9970 System Safety: Software Safety Relation I (non-credit); lessons in building and management of safe information systems
- Military & IT Personnel
  Both courses help students prepare for CISSP exam.
  - ITS-2545 Information Systems Security (credit)
  - ITS-7890 Preparations for the CISSP Exam Systems (non-credit)

- Military & IT Personnel
  All courses help students prepare for Security+ exam.
  - ITS-2090 Computer Security (credit)
  - ITS-8460 Security + (non-credit)
  - ITS-8550 CompTIA Security+ Certification Prep (non-credit online)

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

In keeping with its strategic plan and mission to serve as a community resource by providing "quality learning opportunities for intellectual development, career enhancement, and personal growth", the College of Southern Maryland has provided the following support to community groups, public schools, and businesses:

- Information Security Awareness Workshops, Speakers and Demonstrations
  - Calvert County Youth Summit 2006–IA Workshops–Stay Safe in Cyberspace conducted by IA/ISS faculty member: Renee Jenkins
  - Calvert County Career 2008 Day @ Mount Harmony Elementary–IT and Cyber Security Careers Info & Demonstrations conducted by IA/ISS faculty member: Renee Jenkins
  - Calvert County 5th Grade Visitation Day 2010–IA Workshops–Becoming a Cyber Superhero conducted by IA/ISS faculty member: Renee Jenkins
  - Computer Mania Day 2009–Volunteer Workshop Support–Cyber Security: What Parents Should Know support provided by IA/ISS faculty member: Renee Jenkins
  - CSM Open Houses and Career Fairs (2006-Present)–IA Exhibit and Career Info Tables manned by Business and Technology Division Chairperson: Jeff Tjiputra and IA/ISS faculty members: Renee Jenkins and Daphne Powell
  - Girls Investigating Finance, Technology, & Science (GIFTS) Mentoring 2009-2010 Program–Cyber Security Lessons mentored by Renee Jenkins
  - Girls Investigating Finance, Technology, & Science (GIFTS) Mentoring 2010-2011 Program–Cyber Security Lessons mentored by Renee Jenkins

    Internet Safety and Security Tips for Parents
  - North Point High School – Briefing of Principal About CyberPatriot HS Competition conducted by Jeff Tjiputra resulting in two teams from the school participating in the competition

    Human Rights 2010 Day – Cyber Bullying Movie & Empowerment Workshop sponsored by Lisa Lynk Smith

- Smart Money 2010 Community Seminar–Identity Theft Workshop sponsored by CSM in partnership with St. Mary's County Chamber of Commerce and the Rotary Club of St. Mary's County

- Training of Law Enforcement Personnel –IA Awareness Topics conducted by Nicholas Valltos

- Women in Math Days 2007-2010–IA Workshops and Panel Speakers including Renee Jenkins, Daphne Powell, and Dr. Julie Ryan

  Topics spotlighted include: cryptography, network security; remote access software; Staying Safe in Cyberspace; basic security software and IA career information.

  - Women in Math Day 2007–IA Workshops & Panel Speakers
  - Women in Math Day 2008–IA Workshops & Panel Speakers
  - Women in Math Day 2009–IA Workshops & Panel Speakers
  - Women in Math Day 2010–IA Workshops & Panel Speakers

- Women in Technology Days 2006-2008–IA Workshops and Demonstration Tables. Events coordinated by Renee Jenkins and Daphne Powell with support from Business and Technology Division Faculty as well as IST/ISS students. Topics spotlighted include: essential computer security skills and software; network security; steganography software; Staying Safe in Cyberspace; Internet security software and IA career information. Male as well as female ISS and IST students attended and served as volunteers.

  - Women in Technology Day 2006–IA Workshop & Hands-on Demonstration Table
  - Women in Technology Day 2007–IA Hands-on Demonstration Table
  - Women in Technology Day 2008–IA Workshop & Hands-on Demonstration Table

- Youth in Technology Summits 2008-2010 sponsored by Vyalex Management Solutions in partnership with CSM's Business and Technology Division along with industry as well as government partners including the Patriots Technology Training Center, LLC; the Naval Surface Warfare Centers-Dahlgren Laboratory, Indian Head Division; the Naval Explosive Ordnance Disposal Technical Division and IA/ISS technology, career and program information distributed by CSM and other partners.

  - Youth in Technology Summit 2008–IA Career Info & Demonstrations
  - Youth in Technology Summit 2009–IA Career Info & Demonstrations

        - Youth in Technology Summit 2010–IA Info & Demonstrations

- IA Discovery Workshops sponsored by Kids College
    - Computer Forensics Teen Conference
    - Saturday Discoveries: Science and Technology (Cyber Security)

- Service Learning–Community Outreach IA Projects
    - ITS1015-43700 The Info Age Spring 2007 Course – IT Students Created Posters/Magnets for Distribution at Calvert County 2007 Youth Summit & Other Outreach Events taught by Renee Jenkins
        - Selected Posters/Magnets
    - ITS2545-75916 IS Management Fall 2009 Course – IA Students Help Organizations Improve IA Plans & Practices taught by Renee Jenkins
    - ITS2545-83727 IS Management Fall 2010 Course – IA Students Help Organizations Improve IA Plans & Practices taught by Renee Jenkins
    - ITS2900/2910 Coop Education and Capstone Courses– IA Related Outreach Projects taught by Wendy Hume, Daphne Powell, and Rob Murphy
    - ITS2940-85745 Cyber Ethics Fall 2010 – IA Students Created Posters/Magnets for Distribution @ Outreach Events taught by Renee Jenkins

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)

Renee Jenkins
Professor
Business and Technology Division
Coordinator since January 2008

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

- Wendy Hume – Professor
- Robert Murphy – Adjunct Instructor
- Daphne Powell – Associate Professor

- Jean Runyon – Adjunct Instructor
- John Wilson – Professor

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)

- Wendy Hume (Security+) – Full Time
- Renee Jenkins (CISSP, 24 IA graduate hours, industry experience) – Full Time
- Robert Murphy – (CISSP, military experience) – Part Time
- Daphne Powell – (CCSI, industry experience) – Full Time
- Jean Runyon – (Business and IT education) – Part Time
- John Wilson – (MCSE Degree, military experience) – Full Time

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

- Employee Usage of Technology Policies
- Guidelines for Reporting Cyber Violations
- Information System Security Request Process (related form used to request new and changes to employee accounts)
- Password Reset Policy
- Policy on Disclosure of Student Records
- Student Handbook 2010-2011 (Student Code of Conduct Section)

  The Student Code of Conduct stipulates a range of IA related policies and consequences for violations
  including:
  - Standards for Academic Integrity
  - Standards for Use of Facilities and Property
  - Standards for Use of Software and Hardware
  - Policy against Harassment

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

David Marek
Network Manager and Acting Network Security Administrator

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

- Employee Usage of Technology Policies
- Guidelines for Reporting Cyber Violations
- Information System Security Request Process (related form used to request new and changes to employee accounts)

- Password Reset Policy
- Policy on Disclosure of Student Records
- Student Handbook 2010-2011 (Student Code of Conduct Section)

  The Student Code of Conduct stipulates a range of IA related policies and consequences for violations including:
  - Standards for Academic Integrity
  - Standards for Use of Facilities and Property
  - Standards for Use of Software and Hardware
  - Policy against Harassment

- Faculty and Staff
  - All employees are required to attend orientation during which and overview of IT/IA policies and practices reviewed.
  - All employees are given an Administrative Handbook includes policies listed above. Handbook is also made available on intranet.)
  - IA related announcements are posted in the weekly employee newsletter, The Friday Report. In addition, notices are sent via email as needed. Example Newsletters:
    - June 19, 2009 Newsletter–Contains identity theft prevention tips.
    - May 21, 2010 Newsletter – Notice of new security policies, upgrades and training course.
  - Online IA training and awareness articles are made available on the college's intranet
  - Ongoing IA training courses are offered by the Human Resource(Information Technology Services Departments
    - Information System Basics
    - Advanced Information Security

- Students
  - Majority of degree seeking students are required to take a basic information technology course, ITS1015-Information Age. The course includes multiple lessons in cyber ethics and cyber security as they relate to Internet, hardware, software and network usage.
  - The acceptable use policy is displayed as a login banner upon opening web browsers on lab computers.
  - Acceptable use posters are displayed in computer labs.
  - Student handbooks containing student code of conduct are distributed each semester.

- Academic integrity and appropriate use of technology policies outlined in student code of conduct are noted by instructors as well as documented in course syllabi.
- Cyber security awareness posters and handouts are displayed as well as distributed during National Cybersecurity Awareness Month, career fairs, transfer fairs, social awareness week, and other student events.
-

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.