National Centers of Academic Excellence for Information Assurance Education and Training
Program for 2 Year Institutions (CAE-2Y)
Criteria for Measurement – July 2011

The National Security Agency (NSA) and Department of Homeland Security (DHS) National Centers of Excellence in Information Assurance (IA) Education & Training 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 IA and/or Cybersecurity 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/Cybersecurity 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 NSA/DHS National Center of Excellence in 2 Year IA Education (CAE-2Y) for a period of 5 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/Cybersecurity. (Designation of NSA/DHS National CAE-2Y does not carry a commitment of funding from the National Security Agency or from the Department of Homeland Security.)

(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 CAE-2Y 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 NSA/DHS National Center of Academic Excellence in IA Education and Training Program, IA courseware must be currently 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). 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 CAE-2Y 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
4012	Date
4013	Date
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

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

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

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

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

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

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

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

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

3. IA as a multidisciplinary discipline: 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: business courses teaching Information Security modules or, health courses incorporating HIPAA regulations)
Point Value: 5 points

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

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

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 (for 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

5. IA Faculty: Faculty assigned specifically to teach and/or develop IA courses/curriculum/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)

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

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, CISA, CISM, CEH, etc. (see attached DoD 8570 list). A minimum of 15 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)

CISSP: Certified Information System Security Professional
CISA: Certified Information Systems Auditor
CISM: Certified Information System Security Manager
CEH: Certified Ethical Hacker

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's IA security plan and/or policies
Point Value: Up to 5 points

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

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

Total MINIMUM Point Requirement: 57
Total MAXIMUM Points Available: 108
MINIMUM POINTS REQUIRED TO QUALIFY AS A CAE-2Y: <u>57</u>

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