National Centers of Academic Excellence in Cyber Defense
Two-Year Education Program (CAE2Y)
Criteria for Measurement

Jointly Sponsored by the
National Security Agency (NSA) and the Department of Homeland Security (DHS)

Goal

The goal of the CAE2Y program is to proactively increase our understanding of robust cyber defense (CD) technology, policy and practices that will enable our Nation to effectively prevent and respond to a catastrophic cyber event. This program will contribute significantly to the advancement of state-of-the-art CD knowledge and practice.

Vision

Establish a process that will:

- Provide programs that commit to excellence in the field of Cyber Defense education at community and technical college and government training institutions.
- Strengthen the cybersecurity workforce by providing CD education and training through degree and certification programs at community and technical colleges and government training centers.
- Build an effective education pipeline model with K–12 schools to encourage students at an early age to enter CD fields of study.
- Provide the Nation with a pipeline of qualified students poised to become the future skilled technical workforce.
- Continuously improve the quality of CD programs, curriculum, faculty, students and other institutions.

CAE2Y Program Eligibility and Summary

The CAE2Y Program is open to current regionally accredited two-year community colleges, technical schools, state or federally endorsed Cybersecurity training centers or U.S. Government Cybersecurity training centers. All institutions must hold current regional accreditation as outlined by the Department of Education (http://ope.ed.gov/accreditation).

Overall CAE2Y requirements include:

- **KU Mapping** – Mapping of the institution's curriculum to the two-year core Knowledge Units (KUs, 11 total) and demonstrate that a student can reasonably complete the necessary course of study to include all KUs identified.
- **Program Requirements** – Demonstration of CD Center establishment and maintenance, CD program of study, CAE2Y curriculum path, student development, CD faculty, and outreach.

Focus Area (FA) Designation (Optional):

All CAEs have the option to apply for one or more CAE CD Focus Area designations.

- Successful mapping of the institution's curriculum to all of the KUs identified in the Focus Area.
- Demonstration that a student can reasonably complete the necessary course of study to include all KUs identified in the Focus Area and the Core KUs.
- The institution must provide student certificates to those that complete the FA course of study. The certificates must clearly identify the specific Focus Area achieved.

Application Submission and Evaluation

- Applications shall be submitted via the CAE Application website – www.iad.gov/nietp.
- Re-designating CAE institutions that will expire in 2018 must submit **no later than 15 January 2018**.
- Applicants that already have a CAE application account and have been actively gathering information may continue with their submission and submit by 15 January 2018.
- Applicants that are new to the CAE process may start by completing a New Applicant Inventory to ascertain readiness to apply (https://www.iad.gov/NIETP/CAERequirements.cfm).
- Inventories will be reviewed, and applicants that opt to receive support will be referred to one of two assistance paths:
    - Institutions needing further development of programs and/or curriculum, or those with programs that have not reached maturity, will be referred to a CAE Regional Resource Center (CRRC) for assistance.
    - Institutions assessed to be within one year of meeting curriculum (KU) and programmatic criteria will be referred to the Application Assistance path for mentorship. Any institution wishing to apply for designation after 15 January for the 2018 Submission Cycle must complete their application in coordination with a designated mentor. Submissions must be received no later than 1 May 2018. The CAE Program Office requires the endorsement of the mentor to process applications.
- Applicants that choose to opt out of Application Assistance must acknowledge that they do not wish to receive support via the New Applicant Inventory.

Qualified Cyber professionals and Subject Matter Experts from CAE Academic Institutions, NSA, DHS, and other government and industry partners will assess applications. By submitting an application, an institution grants consent to having its application reviewed by assessors approved by the CAE Program Office. New institutions applying for designation will receive at least three independent reviews. Re- designating institutions will receive at least two independent reviews. Institutions not meeting requirements will receive reviewer feedback at the time of notice. Reviewer feedback is available upon request for approved submissions by contacting the program office at AskCAEIAE@nsa.gov. Incomplete applications will be returned without comment.

CAE2Y Designation:

Qualifying applicants will be designated as CAE2Y for a period of five academic years, after which they must successfully re-apply in order to retain the designation. Future criteria (including KUs and FAs) will continue to be reviewed annually and strengthened as appropriate to keep pace with the evolving nature of Cyber Defense. Designation as a CAE2Y does not carry a commitment of funding from NSA or DHS.

0. **Letter of Intent and Endorsement** – and statement of CAE2Y mission and purpose.
Provide official notice of institutional endorsement and intent to participate in the CAE2Y program. The letter must:

- Be written on official institution letterhead, signed by the Provost or higher
- Express institutional commitment to excellence in the cyber defense field and support of the program the institution is submitting for CAE designation
- Identify the CAE point of contact (POC) from the institution
- Provide institutional support of an official Cyber "Center" within the institution
- Identify regional accreditation information
- List pertinent accomplishments in the cyber defense field
- The letter shall be addressed to:

National Security Agency
Attn: CAE Program Manager
9800 Savage Road
Ft. Meade, MD 20755-6804

The Letter of Intent must be uploaded within the CAE-2Y application. Do not mail. **This is a mandatory requirement.**

1. **Cyber Academic Curriculum Path is Robust and Active**
The Cyber Defense (CD) curriculum path must have been in existence for at least 3 years. Evidence must show one (1) year of students that complete the curriculum path with recognition. The institution must have a mature program path in place that leads to a two-year associate's degree or a certificate in a related cyber discipline. The curriculum path is defined as a series of courses that meet all the mandatory core Knowledge Units. The institution must show its curriculum path and demonstrate that students are enrolled and successfully complete the path and receive recognition. Applicant institution must provide a list of courses (number and title) included in meeting the cyber defense curriculum path and provide data showing when each course was last taught.
Overall Point Value: 10 mandatory (15 mandatory if pursuing a Focus Area)

a. **Cyber Defense Program of Study**
Describe the CD curriculum path offered by the institution. This description must contain the following:
   - List curriculum path(s) – must contain all courses mapped to KUs. Courses must be identified in current course catalog.
   - Department(s) where curriculum path resides.
   - If more than one path, each must be mapped separately and meet all the mandatory KUs. If application is approved, only the CD curriculum program path(s) identified in this criterion are allowed to be marketed as designated CAE2Y Curriculum Path(s).

   (5 pts – mandatory)

b. **Student Participation in curriculum path**
   - Student enrollment for last 3 years in curriculum path.

- Number of students that have received a degree or certificate and completed the Cyber Defense program path within one (1) year of submission
- Provided at least three redacted student transcripts – ***preferred***. Highlight the courses taken that meet the Cyber Defense curriculum path. All courses mapped to the KUs ***must*** be present ***or***
  Official endorsement on Registrar letterhead specifically detailing that at least three (3) students have completed the Cyber Defense. The Registrar's letter must state the number of students, date of completion and courses taken in the path. All courses used to map to the KUs must be present
- Sample certificate or notation on transcript issued to students completing the CD program path

(5 pts – mandatory)

c. **Optional - Student Participation in Focus Area (FA) curriculum path -** Optional Focus Area (FA) submission must contain all core KUs and mandatory optional KUs plus FA KUs.
- Student enrollment in courses that meet all mandatory KUs plus the courses that were used to map to the Focus Area
- Redacted student transcripts, dated within the last three (3) years and clearly highlight the courses taken that meet the FA program path (preferred). All courses used to map to the mandatory KUs and FA must be present, ***or***
  Official endorsement on Registrar letterhead detailing that students have completed the Focus Area path. The Registrar's letter must state the number of students, date of completion and courses taken in the path. All courses used to map to the KUs must be present
- Please note - If institution does not have or is not applying for a Focus Area Designation, notate 'N/A' in the justification of this criterion

(5 pts – mandatory if FA submitted)

2. <u>Student Skill Development and Assessment</u>

The institution must show how it fosters student development and assessment in the field of Cyber Defense. This criterion focuses on STUDENT-based skills development as it contributes to evolution of theory and practice in the field of Cyber Defense and how students are assessed. Skills development shall relate back to one or more of the mapped KUs.

(13 pts mandatory, up to 20 pts)

a. Students assessed by one or more methods: Provide actual papers, projects, test questions, etc. from students in the curriculum path (**<u>must</u>** be courses in the curriculum path – eliminates the need for attaching syllabi again). Papers/projects, etc. must be clearly identified with course title, course number, and date of submission.
(1 pt per paper/project, etc/from at least 3 different courses/5 pts mandatory)

b. Students assessed by: Lab assignments/hands on activities – provide examples of the lab assignments (**<u>must</u>** be courses in the curriculum path – eliminates the need for attaching syllabi again) and describe how the lab enforces curriculum taught in the path.
(1 pt per lab assignment/from at least 3 different courses/5 pts mandatory)

c. Evidence of student participation in cyber competitions.
   - Provide evidence of participation in Cyber Defense related exercises and competitions for students enrolled in applying institution within the last 3 years (e.g., link to team roster on the competition website, link to social media about the exercise, etc.)
   - Explain the benefit of participating in the Cyber Defense Exercise/Competition. How did the team place? What were the lessons learned? What basic cyber content was reinforced by participating on a team?

   (1 pt per competition/up to 5 pts)

d. Cybersecurity Practitioners/Industry Partnerships
   - Provide evidence that the program is providing students with access to cybersecurity practitioners (e.g., Guest lecturers working in the Cybersecurity industry, government, faculty exchange program with industry and/or government, internship opportunities, etc.). Provide fliers, posters, etc.

   (1 pt per partnership/up to 5 pts)

3. <u>"Center" for CD Education</u>

The institution must have an officially established entity (either physical or virtual) serving as the focal point for its cyber curriculum and practice.

(8 pts mandatory/10 pts max)

a. The center shall provide the following services:
   - Information about the CD program of study and faculty
   - Program guidance and oversight
   - "Center" points of contact
   - Links to student CD activities available to students at the institution and beyond
   - Include both internal and external CD news. Internal news should highlight CD activities and efforts at the institution and/or other CD activities of students and faculty representing the institution. External CD news should highlight up-to-date trending CD information
   - Institutional security resources and awareness
   - Up-to-date links to key CD resources such as other academic institutions, government sites, conferences, workshops, and cyber competitions
   - Center Website (url) - visible within the institution and the external community at large (mandatory)

   (6 pts mandatory/8 pts max)

b. The department that houses the Cyber "Center" must have an external board of advisors – local/national industry professionals, faculty from other institutions, etc. to provide programmatic guidance over the activities of the center and the program as a whole.

   (2 pts mandatory)

4. Cyber Faculty and Courses Taught

The institution must demonstrate that it has faculty responsible for the overall CD program of study and sufficient faculty members, either full- or part-time to ensure continuity of the program. The criterion requires a link or attachment to the biography, curriculum vitae or resume for each faculty member with school affiliation clearly identified. It must be possible to locate all permanent faculty members by searching the Institution website.
(10 pts mandatory/15 pts max)

a. Head of the Cyber program (if CV includes qualifications, courses taught, links to research papers, presentations, etc., no other evidence is needed)
(5 pts mandatory)

b. Must provide a permanent faculty as a designated alternate for notices-CV/resume required.
(1 pt mandatory)

c. Additional permanent faculty members (if CV includes qualifications, professional societies, courses taught, links to research papers, books, presentations, etc., no other evidence is needed)
(1 pt mandatory)

d. At least one faculty member must have at least one professional certification, such as CISSP, CISA, CISM, or CEH, ***or*** have a minimum of 15 hours of graduate coursework ***and/or*** experience in a related field.
(1 pt mandatory)

e. Faculty support to Cyber Student activities, Clubs, Competitions, etc.
•Provide evidence that CD faculty members support their students by serving as mentors or advisors to student led activities. Evidence must include links to student clubs, cyber defense exercises, etc.
•Provide evidence of participation in or sponsorship of CD exercises and competitions within the last 3 years, (e.g., link to team roster on the competition website, link to social media about the exercise, etc.) This can be an in-class competition. Applicable evidence must be provided.
(1 pt per item/2 pts mandatory)

5. Cyber Defense is a Multidisciplinary Practice at the Institution

The institution must demonstrate that Cybersecurity is not treated as a separate discipline, but integrated into additional degree programs within the institution. Courses cannot be from the department that mapped to the Knowledge Units.
(7 pts mandatory/15 pts max)

a. Provide evidence that students in other departments are exposed to cyber concepts. Provide at least 3 syllabi with cyber content clearly highlighted

(1 pt per course/3 pts mandatory/5 pts max)

b. At least one paper/project/test questions from each of those courses (cyber content clearly highlighted).
(1 pt each/3 pts mandatory/5 pts max)

c. Provide evidence (catalog, syllabi, class schedule) of the availability of non- credit/credit Cyber related professional development courses (e.g., First responders, K- 12 teachers)
(1 pt per course/5 pts max)

6. Institutional Security Plan

The objective of system security planning is to improve protection of information system resources. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. (An example of a government-based IA security plan may be found at: http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf.) This is an example and not intended to replace an existing institution security plan.
(6 pts mandatory/9 pts max)

a. **Security Plans**
Provide links or attachments to the high-level IS Security Plan(s) for the institution to show how it practices institutional security. IS Security Plan must include how the Information System infrastructure of the institution is protected and how the plan is implemented, not just policies on use of the system.
(2 pts mandatory)

b. **Security Officer – provide name and job description**
Provide the name, title and job description for the individual responsible for the institution IS program. If there is a committee to oversee IS security, please explain duties and implementation.
(2 pts mandatory)

c. **Implementation of Cyber Security Practices**
Provide evidence of how the institution implements it's IS Security plan through awareness, training and tutorials, log in security banners, user acknowledgements, on-line help and good security practice guides. (e.g., Students, faculty and staff are required to take computer based training or on-line tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc.)
Provide screen shots, links to mandatory training, good password practices, etc.
(2 pts mandatory/5 pts max)

7. <u>Cyber Outreach/Collaboration *Beyond* the Institution</u>

The institution must demonstrate how Cyber Defense practices are extended beyond the normal boundaries of the institution. Show how CD principles developed at the Institution are shared with others or how industry theory and practice are incorporated into curriculum.
(10 pts mandatory/25 pts max)

a. **Faculty Involvement in Sharing Expertise** (can be information from 5b)
   - Provide evidence of how the institution shares Cyber related curriculum and/or faculty with other schools, to include K-12 schools, other community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge within the last 3 years
   - Provide specific information about sponsorship or participation in CD curriculum development workshops or colloquia or faculty sharing events for any of the types listed above within the last 3 years

   (1 pt per event/5 pts max)

b. **Transfer of Credit – 4-year institutions**
   - Provide evidence of Articulation/Transfer agreements with 4 year institutions offering a concentration or cybersecurity (or related field) degrees/areas of study/track or certificates
   - Identify specific cyber courses that are accepted at partner institutions and a crosswalk of the accepted courses. Examples include, (but are not limited to): statewide transfer agreements, articulation agreements, college in the high school, dual credit, running start, credit for prior learning, credit for military training or occupation

   (1 pt per agreement/5 max)

c. **Transfer of Credit or Partnerships - High School**
   - Provide evidence (e.g., MOA, dual-credit, college in high school, running start, lecture series, curriculum/faculty sharing, etc.) of agreements with high schools (cyber-related or technical pre-requisite and not just general pathway programs) to <u>facilitate awareness and training</u> for faculty, administration or students

   (1 pt per agreement/5 maximum

d. **Community Outreach** – activities outside of student/campus events (senior centers, K-12, camps, etc.)
   - Provide evidence of faculty/employee sponsorship or oversight of students for Cyber events for the community at large. Events could include Cyber awareness and education for local schools, adult education centers, senior centers, camps, first responders and the surrounding community
   - Examples of events could be, but are not limited to, computer “check-up” days, protecting personal information in cyber space, workshops for senior citizens on Internet safety, or preventing and recovering from a “virus”

   (1 pt per event/5 pts max)

e. **Business/Industry Collaboration** – explain involvement (internships for students, identifying needs of business partners for course content, job fairs, guest speakers, etc.)
    - Provide evidence on how the institution partners with companies and other employers to identify Cyber Defense needs of potential employers and encourage student internships
    - Provide evidence on how the institution works with employers and students to support placement for Cyber related jobs
    - Provide evidence of obtaining input on curriculum to meet industry needs

    (1 pt per collaboration/5 pts max)