

NSA/DHS National Centers of Academic Excellence in Cyber Defense  
Applicant Checklist  
**CAE-2Y Designation**

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>).

- Applicants must identify a specific curriculum path followed by individual students to receive a certificate, minor, degree, concentration or other recognized program completion. Curriculum in this path must map to the eleven core Knowledge Units required for the CAE-2Y designation.
- Applicants must demonstrate compliance with program criteria, including establishment and maintenance of a Cyber Defense (CD) Center, CD program of study, student development, CD faculty, and outreach.

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. Designation as a CAE2Y does not carry a commitment of funding from NSA or DHS. CAE institutions with designations that will expire in 2018 must submit no later than 15 January 2018 and are not required to submit this checklist.

- 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 for possible designation in June or by 15 April 2018 for possible designation at the NICE Annual Conference in November 2018.
- Applicants that are new to the CAE process or those who wish to receive assistance should complete an Applicant Checklist to ascertain readiness to apply. Applicants have the opportunity to receive mentorship. Application Assistance with a mentor is being offered as a benefit to the institution and is designed to help applicants understand the depth of program and designation requirements.
- Applicants that opt to receive support will have their checklists reviewed and will be referred to one of two assistance paths:
  - Program Development: 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 for assistance. In this phase, the applicant will have access to workshops, seminars and an advisor to help in their preparation for designation. Schools in this phase will also be invited to programs and events hosted by the CAE Community ([www.caecommunity.org](http://www.caecommunity.org)) and have access to other resources offered by the Program Office only for the CAE audience.
  - Application Assistance: Institutions assessed to be within 12 – 18 months of meeting curriculum and programmatic criteria will be referred to the Application Assistance path for mentorship. The CAE Program Office requires the endorsement of the mentor to process applicants that have chosen this path. Submissions must be received no later than 15 April 2018 or a subsequent designation cycle.
- Applicants that choose to opt out of Application Assistance must acknowledge the last page of this New Applicant Inventory.

Yes, I opt to receive support via the CAE Application Assistance Program Please complete the inventory and follow submission instructions. (If opt in, then applicant will complete Application checklist and not the “Application Assistance Opt Out” section on the last page)

No, I opt out of the CAE Application Assistance Program (inventory is not required, please proceed to last page) (if opt out, then applicant will only complete the “Application Assistance Opt Out” section on the last page)

Contact the Program Office at [askcaeiae@nsa.gov](mailto:askcaeiae@nsa.gov) for further information.

NSA/DHS National Centers of Academic Excellence in Cyber Defense  
Applicant Checklist  
**CAE-2Y Designation**

\*Institution Name: (Fillable character field)

POC Name: \*First: (Fillable character field)      \*Last: (Fillable character field)      \*Title: (drop down?)

\*POC Phone: (Fillable character field)      Alt. Phone (Fillable character field)

\*POC Email (must be .edu): (Fillable character field)

\*POC Mailing Address: Street: (Fillable character field) State: (2 character drop down)      Zip: (Fillable character field)

\*Curriculum Path (dropdown: certificate, minor, concentration, degree, other) with: Please describe other (fillable character field) Name: (Fillable character field)

\*Department that houses the Path: (Fillable character field)

Dean or Above Name: \*First (Fillable character field) \*Last: (Fillable character field) \*Title: (drop down?) \*Phone: (Fillable character field)

1. \*Regional Accreditation - required for designation: (drop down list of accrediting bodies) – if regionally accredited not selected, then message saying “not eligible for CAE-CD submission” and rest of application is not available to complete
  
2. Provide the course number, name and short description of courses you believe map to the CAE 2Y Core KUs  
EXAMPLE: Course #: ITS222      Course name: Enterprise Security.  
Course Description: The Enterprise Security Seminar is designed so that you understand the critical components of network security. The course covers physical security and devices as well as software and organizational components. This course covers the material recommended as preparation for the ComTIA Security + certification examination. Exercises and assignments are geared toward practical skills needed as a Network Manager.

Multiple Courses containing the following fields:

- \*Course#: (Fillable character field)
- \*Course name: (Fillable character field)
- \*Course Description: (Fillable character field)

3. \*Please indicate ‘Yes or Done’, ‘No or None’, or ‘Unknown/Unsure’ to the questions below and submit the checklist; you will be contacted with information on how to continue.

*\*Denotes required field*

NSA/DHS National Centers of Academic Excellence in Cyber Defense  
 Applicant Checklist  
**CAE-2Y Designation**

| Criteria Name   | Criteria Description   | Yes<br>or<br>Done | No or<br>None | Unknown<br>or<br>Unsure |
|---|--|-------------------|---------------|-------------------------|
| 0. Letter of intent                                   | Please acknowledge this requirement. Once assigned to the application assistance path, applicants will need to obtain a letter containing POC information, institutional support, regional accreditation information, cyber center support, and accomplishments in the field of Cyber Defense.   |                   |               |                         |
| 1. Cyber Defense Curriculum Path                      | Is there a Curriculum Path that meets the all of the mandatory Knowledge Units (KUs)?  |                   |               |                         |
|   | Has the stated curriculum path been in existence for at least 3 years and have 1 year of students that have completed the curriculum path with recognition of completion?  |                   |               |                         |
|   | Are there at least 1 year of students that have received a two-year associate's degree or a certificate for the curriculum path?   |                   |               |                         |
| 2. Student Scholarly Skill Development and Assessment | Do courses in the curriculum path require students to write papers or complete projects or presentations?  |                   |               |                         |
|   | Do courses in the curriculum path require lab assignments for hands-on learning?   |                   |               |                         |
|   | Do students participate in cybersecurity competitions?   |                   |               |                         |
|   | Are students provided with access to cybersecurity practitioners such as guest lecturers working industry or government, internships, etc?   |                   |               |                         |
| 3. "Center" for Cyber Education                       | Does the institution have an officially established entity (either physical or virtual) serving as the focal point for its Cyber educational program? The center shall provide the following services: program guidance and oversight; general cyber defense information; and collaboration and outreach opportunities among students, faculty, and other institutions. Additionally, the center must be supported by a website that is dynamic, current and visible within the institution and the external community at large. |                   |               |                         |
|   | Not required but beneficial - Does the department that houses the Cyber "Center" have an external board of advisors, local industry professionals, to provide programmatic guidance over the activities of the center and the program as a whole?  |                   |               |                         |
| 4. Program Faculty                                    | Is there someone with overall responsibility for the program?  |                   |               |                         |
|   | Does at least one faculty member 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?   |                   |               |                         |
|   | Is there adequate faculty available to teach Cyber related courses in the curriculum path at the institution?  |                   |               |                         |
|   | Are faculty supporting Cyber Student activities? Clubs, Competitions, etc.?  |                   |               |                         |
| 5. Cybersecurity Practice is Multidisciplinary        | Are non-technical/non-CD students introduced to CD through modules in existing non-CD courses, such as information security included in business, health courses incorporating HIPAA regulations, etc?   |                   |               |                         |

NSA/DHS National Centers of Academic Excellence in Cyber Defense  
 Applicant Checklist  
**CAE-2Y Designation**

|                            |  |  |  |  |
|----------------------------|--|--|--|--|
|                            | Are papers or projects or test questions required that demonstrate knowledge of security concepts or awareness in non-CD courses?  |  |  |  |
|                            | Does the institution offer non-credit/credit professional development CD-related courses?  |  |  |  |
| 6. Institution IS Security | Does the institution have an Information System Security Plan? A plan must provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. NOTE: For the final application, evidence of such a plan must be provided. |  |  |  |
|                            | Does the institution have an ISSO to oversee Security throughout?  |  |  |  |
|                            | Does the institution have in place a means to encourage cybersecurity awareness throughout the campus?   |  |  |  |
| 7. Outreach/Collaboration  | Does the institution share cyber related curriculum or faculty beyond the boundaries of the institution, such as materials provided to high schools or technical schools, or faculty serving on another institution's development committee?   |  |  |  |
|                            | Does the institution have transfer of credit agreements with four-year institutions offering a cyber-concentration, degree, area of study, or track?   |  |  |  |
|                            | Does the institution have cyber or technical pathways such as transfer agreements, college in high school, running start, lecture series, etc. with high school faculty, administrators or students?   |  |  |  |
|                            | Does the institution sponsor cybersecurity-related community events such as cybersecurity education workshops, homeland security events, first responder workshops, computer diagnostic check-ups, etc?  |  |  |  |
|                            | Does the institution collaborate with other CAE schools on projects, grants, etc? Business/Industry?   |  |  |  |

Reviewer Name: \*First: (Fillable character field) \*Last: (Fillable character field)

Reviewer Notes: (Fillable character field with date of note associated with it – allow for multiple notes on multiple dates?)

NSA/DHS National Centers of Academic Excellence in Cyber Defense  
Applicant Checklist  
**CAE-2Y Designation**

Application Assistance Opt Out

I, name of POC (fillable field), from name of institution (fillable field), acknowledge that I have been given the opportunity to receive application assistance and work with a mentor to complete my application for possible designation as a NSA/DHS National Center of Academic Excellence in Cyber Defense Education. I understand that this process is an opportunity to receive program development and application assistance prior to submitting an application. I acknowledge that if my application does not meet requirements, the assistance of a mentor is a requirement to submit an application in a future cycle. If at any time I require Application Assistance I may complete the new applicant inventory and request assistance with the understanding that it may move my submission to a subsequent cycle.

By “Submitting agree to the above term” with associated date of submission

Head of the Department that houses the Curriculum path email address: (Fillable character field)

After form is complete and applicant presses “submit” - form will be sent to [askCAEIAE@nsa.gov](mailto:askCAEIAE@nsa.gov)