National Centers of Academic Excellence in Cyber Defense (CAE-CDE) Education Program Criteria for Measurement

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

Goal

The goal of the CAE-CDE program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in Cyber Defense (CD) and to produce a growing number of professionals with expertise in CD disciplines. 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 the graduate and undergraduate levels.
- Provide the Nation with a pipeline of qualified students poised to become CD professionals.
- Continuously improve the quality of CD programs, curriculum, faculty, students and other institutions.
- Emphasize faculty efforts in improving CD scholarship, professional development and instructional capabilities.
- Foster and encourage further development of strong CD focused education and research depth at U.S. institutions.

CAE-CDE Program Eligibility and Summary

The CAE-CDE Program is open to current regionally accredited four-year colleges and graduate-level universities. All institutions must hold current regional accreditation as outlined by the Department of Education (http://ope.ed.gov/accreditation).

Overall CAE-CDE requirements are:

- **KU Mapping** - Mapping of the institution’s curriculum to the four-year core Knowledge Units (KUs) + 5 optionals (22 total) and demonstrate that a student can reasonably complete the necessary course of study to include all KUs identified.
- **Program Requirements** - Demonstration of program outreach and collaboration, center for CD education, a robust and active CD academic program, CD multidisciplinary efforts, practice of CD at the institution level, and student and faculty CD efforts.

Focus Area (Optional)

All CAEs have the option to apply for one or more CAE-CDE Focus Area (FA) 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 FA.
- 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 Program Evaluation

- Applications shall be submitted via the CAE Application website – www.iad.gov/nietp.
- Re-designating CAE institutions that will expire in 2017 must submit **no later than 15 January 2017**.
- Applicants that already have a CAE application account and have been actively gathering information may continue with their submission and submit by 15 January 2017.
- 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 2017 Submission Cycle must complete their application in coordination with a designated mentor. Submissions must be received no later than 1 June 2017. 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 CD 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.

CAE-CDE Designation

Qualifying applicants will be designated as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) for a period of five academic years, after which they must successfully re-apply in order to retain 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 National CAE-CDE does not carry a commitment of funding from NSA or DHS.

National Centers of Academic Excellence in Cyber Defense (CAE-CDE) Education Program Criteria for Measurement

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

CAE-CDE Program Criteria

0. **Letter of Endorsement and Intent** and statement of CAE-CDE mission and purpose.
Provide official notice of institutional endorsement and intent to participate in the CAE-CDE 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-CDE application. Do not mail. **This is a mandatory requirement.**

1. Cyber Defense Academic Program Path
The Cyber Defense (CD) program path <u>must</u> have been in existence for <u>at least</u> 3 years. Evidence must show one (1) year of student granted degrees with program path completion. The CD program path of study is central to a vibrant and mature CAE for Cyber Defense education program. The path is defined as a series of courses that meet all of the mandatory Knowledge Units plus five (5) optional Knowledge Units (KUs). The institution <u>must show</u> its CD curriculum program path and show that students are enrolled and successfully complete the CD program path and receive recognition.
Overall Point Value: 15 mandatory (20 if pursuing a Focus Area)

a. Cyber Defense Program of Study
Describe the CD program path offered by the institution. This description **<u>must</u>** contain the following:

- Provide the entire course path that makes up the program at your institution – clearly highlight the courses that meet all of the mandatory Knowledge Units (KU) and at least five optional KUs required for completion of the Cyber Defense path
- If there is more than one path, then each must be clearly identified and meet all of the mandatory KUs and at least five optional KUs*
- Identify department(s) that oversee the program
  Point Value: 10 points mandatory

***NOTE** – If application is approved, only the CD curriculum program path(s) identified in this criterion are allowed to be marketed as designated CAE-CDE Curriculum Path(s). If additional curriculum path(s) are identified after this application is submitted, the onus is on the institution POC to confirm all core KUs are covered and the POC must identify the additional path(s) in the re-designation application.

b. Student Participation in program path

Evidence provided must include, but is not limited to:

- Student enrollment over the last 3 years
- Number of students that have received a degree and completed the Cyber Defense program path within one (1) year of submission

  NOTE: Beginning in 2019, two (2) years of graduates will be required
- Sample certificate or notation on transcript issued to students completing the CD program path
- Provide at least three (3) redacted student transcripts, dated within the last 3 years and clearly highlight the courses taken that meet the Cyber Defense program path. All courses used to map to the KUs must be present, ***<u>or</u>***
- Provide a memo of record from the Registrar or other Institution official (at a level higher than the department with the program path) detailing that at least three (3) students have completed the Cyber Defense path. The memo 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

  Point Value: 5 points mandatory

c. Student Participation in Focus Area (FA) program path

Evidence provided must include, but is not limited to:

- 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. All courses used to map to the mandatory KUs and FA must be present, ***<u>or</u>***
- A memo of record from the Registrar or other Institution official (at a level higher than the department with the program) detailing that students have completed the Focus Area path. The memo 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

  Point Value: 5 points mandatory (if FA is identified)

2. "Center" for CD Education

The institution must have an officially established entity (either physical or virtual) serving as the focal point for its CD 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.
Overall Point Value: 10 points mandatory/15 maximum

a. Cyber "Center "

- Show formal documentation (e.g., letter of endorsement, charter, mission statement, etc.) of the Cyber "Center." (For the purpose of this document, "Center" is used as a generic term allowing for other terminology to be used because of restrictions at some universities)
- The "Center" must have higher level institutional support with endorsement from a Dean or higher. Must attach endorsement here – may be the letter of intent
  Point Value: 5 points mandatory

b. Cyber "Center" Website

- Cyber "Center" shall provide program guidance and general CD information, and promote collaboration and interaction with students, faculty, and programs
- The Cyber "Center" and its website must be **<u>operational, dynamic, current</u>** and visible within the institution and to the community at large
- Evidence provided must include, but is not limited to:
  - Information about the CD program of study and faculty
  - "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

  Point Value: 5 points mandatory

c. External Board of Advisors

- The department that houses the Cyber "Center" shall 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. This board provides a connection between the program and the local community
  Point Value: 5 points maximum

3. Student-based Cyber Defense Skills Development

The institution must show how it fosters student development 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. Skills development shall relate back to one or more of the mapped KUs.
Overall Point Value: 15 points mandatory/30 maximum

a. Courses Requiring Scholarly Skills Development

- Provide syllabi of CD courses that are mapped to the KUs that require papers, presentations or projects – **highlight requirement** – must relate to papers/projects/presentations submitted in criterion 3b
- Courses requiring papers/projects/presentations must have been taught within the last 3 years
- Courses requiring papers/projects/presentations must be a part of the CD curriculum path as identified in the application

  Point Value: 1 point per course/at least 3 different courses/3 mandatory

b. Scholarly Skills development requirements for Cyber Defense students

Although the depth of the research may vary, both undergraduate and graduate students should be encouraged to analyze Cyber Defense issues and offer solutions or recommendations.

- Provide Cyber Defense scholarly skills requirements for students participating in the CD program path of study
- Provide working **links or attachments** to 3 to 10 of the best CD papers, theses, dissertations, presentations or projects produced by ***students*** within the last 3 years. Clearly highlight cyber content. Course number and date of paper/project must be included
- **Links or attachments to actual papers/projects/presentations are required – not a subscription service**

  Point Value: 1 point per paper, etc /at least 3 different courses/3 mandatory

c. Courses Requiring Lab Exercises

- Provide syllabi of CD courses that require labs – highlight lab requirement – must relate to labs submitted in criterion 3d
- Courses must have been taught within the last 3 years

  Point Value: 1 point per course/at least 3 different courses/3 mandatory

d. Cyber Defense Physical/Virtual Labs

Demonstrate that physical and/or virtual labs and equipment are available and demonstrate how these resources are used by students and faculty to enhance hands-on learning in the Cyber Defense program path of study.

- Provide a description of required lab projects or exercises required for students participating in the CD program path of study. Identify the related course for each of the lab projects and exercises

- Provide working links or attachments to samples of lab projects or exercises completed within the last 3 years
  Point Value: 1 point per lab/at least 3 different courses/3 mandatory

4. Cyber Defense 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. **It must be possible to locate all permanent faculty members by searching the Institution website.**
Overall Point Value: 9 points mandatory/20 maximum

a. Head(s) of the Cyber Defense Program of Study

- Provide an endorsement on University letterhead identifying by name and title the full-time employee or employees with overall responsibility for the CD program of study at the institution. Must verify that faculty is qualified to teach Cyber Defense courses
- Provide biography, CV or related evidence outlining job responsibilities that support requirements of the position
  Point Value: 5 points mandatory

b. Additional permanent employees of the institution teaching Cyber Defense related courses in the department where the cyber defense program path resides

- Identify by name additional full-time, part-time or adjunct faculty members teaching the courses in the CD program path of study, do *not include faculty listed in criterion 4a*
- Provide biography or CV with cyber background clearly identified
- Evidence must include department where the faculty member teaches and courses that they teach in CD program path of study
  Point Value: 2 point each/4 points mandatory/15 maximum

5. Cyber Defense Faculty Expertise and Research

The institution must show that the faculty members are Cyber Defense experts and are active in current CD practice and research. Cyber Defense faculty members must be contributing their CD knowledge to publications, presentations, and professional societies as well as seeking grants for CD resources and mentoring CD students. Faculty members in this section must also be associated with the CD program of study, if they are not listed in section 4, then documentation of how they are connected is required.
Overall Point Value: 20 points mandatory/30 maximum

a. Faculty Authored Cyber Defense Publications

- Provide evidence of current faculty contributions to peer reviewed publications on CD/Cybersecurity topics to include refereed journals and conference proceedings within the last 5 years
- **Provide links or attachments to actual papers not a subscription service**
- More than one (1) faculty member must publish
  Point Value: 1 points per paper/5 maximum

b. Published Books or Chapters of Books on Cyber Defense/Cybersecurity authored by faculty

- Books/chapters must focus on Cyber Defense/Cybersecurity and have been published within the last 5 years
- Provide title, authors and date published
- Identify specific chapters if authoring a chapter of a book
- Papers published in a conference proceedings will be accepted in criterion 5a, not criterion 5b
  Point Value: 5 points per book/1 point per chapter/5 maximum

c. Cyber Defense Presentations

- Provide evidence that faculty members have presented CD content at Local/Regional/National/International conferences and events within the last 3 years (link to program or website with presentation clearly highlighted)
- Provide a synopsis of the involvement. This can include guest lecturer at other institutions or government organizations (provide proof – link to program, website, etc.)
  Point Value: 1 point per presentation/5 maximum

d. Professional Societies

- Provide level of effort evidence that faculty members are CD subject matter experts for accrediting bodies and professional societies. (e.g., ACM, IEEE, regional accreditation, professional accreditation, etc.)
- Provide evidence that faculty members are active members in CD/Cybersecurity organizations (e.g., ISSA, Cyberwatch, Cyberwatch West, Infraguard, CAE Community participation, etc.)
- Provide evidence of active involvement for the last 3 years (meeting roster, CV accomplishment, thank you for reviewing, etc.)
- Provide evidence of performing reviews or acting as a mentor for the CAE CD program

- Provide evidence of presenting a CAE Tech Talk for the CAE Community
  Point Value: 1 points per review or active involvement/5 maximum

e. Support to Cyber Defense Student activities

- 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.
  Point Value: 1 points per program/5 maximum

f. Writing Cyber Defense Grants and External Funding

- Provide evidence that CD faculty members write grants and obtain funding for CD education and/or research or lab equipment
- Provide a synopsis of the grant to include date and approximate monetary value
- Provide links to organization providing the grant or links to a news article
- Provide an explanation if funding or grants were not obtained
  Point Value: 1 points per award or funding/5 maximum

6. Cyber Defense is a Multidisciplinary Practice at the Institution

The institution must demonstrate that CD is not treated as a separate discipline, but integrated into additional degree programs within the institution.
Overall Point Value: 8 points mandatory/12 maximum

a. Cyber Defense Concepts Taught in Other Fields of Study

- Provide evidence that CD topics are integrated in courses outside of the department that contains the CD program path of study. **Provide course name and syllabus with cyber modules <u>clearly highlighted</u>**
- Cannot be any courses in the program path used to map to the Knowledge Units
- Courses taught outside the CD program of study can be technical or non-technical. *For example*: health practitioners learning about privacy and patient data protection; accountants learning about data backup and protection; or non-credit continuing education courses on IT security basics
  Points: 2 point per course/6 maximum

b. Non-Cyber Defense Courses Encourage Papers, Projects or Test Questions in CD topics.

- Provide evidence that courses taught outside the CD program path of study require CD topic papers/projects/posters/test questions/etc. *For example*: health care practitioners write a paper on the importance of safeguarding patient health care records
- Provide links or attachments to 3 to 5 best papers, presentations, projects or test questions on CD with Cyber topics clearly highlighted within 3 years of application. **Link or attachment to actual item required – not a subscription service Paper/projects/presentations/test questions must correspond to courses provided in 6a**
  Points: 1 point per item/6 maximum

7. Institution Information System (IS) Security

The objective of system security planning is to improve protection of information system resources. All systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. 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. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a 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.

Overall Point Value: 15 points mandatory/20 points maximum

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

Points: 5 points mandatory

b. Institutional Cyber Security/Information Security Officer

- Provide the **<u>name, title and job description</u>** for the individual responsible for the institution IS program. If there is a committee to oversee IS security, please explain duties and implementation

Points: 5 points 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.

Points: 5 points mandatory/10 maximum

8. Cyber Defense Outreach Beyond the Institution

The institution must demonstrate how Cyber Defense practices are extended beyond the normal boundaries of the institution. Show how CD principles developed at the University are shared with others.

Overall Point Value: 20 mandatory/30 maximum

a. Shared Curriculum or Advancing Cyber Defense Educational Practice

- Provide evidence of how the institution shares it CD curriculum and/or faculty with other schools, to include K-12 schools, 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
  Point Value: 1 point per event/5 maximum

b. Transfer of Credit

- Provide evidence that the institution awards credit in CD courses and/or technical prerequisite courses from other academic institutions or through alternative means. 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
  Point Value: 1 point per agreement/5 maximum

c. Community Outreach

- Provide evidence of faculty/employee sponsorship or oversight of CD events for the community at large. Events could include CD 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”
  Point Value: 1 point per event/5 maximum

d. Sponsorship or Participation in Cyber Defense Exercises, Capture the Flag and other Cyber Related Competitions

- 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.)
- 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?
  Point Value: 1 point per exercise/5 maximum

e. CAE Collaboration

- Provide evidence on how the institutions partners with other CAE schools on research or shared classes/events
- Evidence can include collaboration on papers, grants, cyber camps, etc.
- Provide evidence of performing reviews or acting as a mentor for the CAE CD program
- Provide evidence of presenting a CAE Tech Talk for the CAE Community
  Point Value: 1 point per collaboration/5 maximum

f. Cyber Defense Business/Industry Collaboration

- 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
  Point Value: 1 point per collaboration/5 maximum

KU Mapping

The KU mapping will require the institution to demonstrate how it meets each Core and Optional (if applicable) KU. An institution has many ways to demonstrate how a program meets/fulfills a KU. Some examples include: course syllabus, course outline, student assignments, lab assignment, modules in a course/collection of courses, and certifications (CCNA, CISSP, etc.). Required information will include: course syllabi, course outlines and justifications showing where and how the KUs are addressed in the curriculum. One course may fulfill the requirements of multiple KUs, and multiple courses may fulfill the requirements of a single KU. A course to KU ratio of 1:1 is not required.

Available Tools

The following tools are available to assist in gathering the information needed to map to the following KU sets:

- CAE IA/CD KUs
- CAE IA/CD Focus Areas
- CAE KU Mapping Matrix
- National Cyberwatch Center's KU Mapping Guide

These tools are useful to identify the topic/objective/week/session/project/lab/etc. numbers (whatever is used in the syllabi/course outline) that covers each of the KU topic and/or outcome elements. The spreadsheets consolidate mapping information which expedites entering it in the CAE application website. Many also find the spreadsheets useful in determining program overlaps and gaps. Links to all tools can be found on the CAE Application website under CAE Requirements and Resources.

Questions? Please direct any questions or concerns to AskCAEIAE@nsa.gov.