...

National Centers of Academic Excellence in
Cyber Defense Education Program (CAE-CDE)
Criteria for Measurement
Bachelor, Master, and Doctoral Level

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 - Bachelor, Master, and Doctoral Level

The CAE-CDE Bachelor, Master and Doctoral Level 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 at the Bachelor, Master, and Doctoral level requirements are:

- **KU Mapping** - Mapping of the institution's curriculum to the requisite Foundational, Core (5 Technical or 5 Non-Technical), and Optional Knowledge Units (KUs) at either the Bachelor, Master, or Doctoral level as outlined on page 4 of this document: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf and demonstrate that a student can reasonably complete the necessary course of study to include all KUs identified.
- **Programmatic Criteria** - Demonstration of program outreach and collaboration, center for CD education, a robust and active CAE-CDE academic program, CD multidisciplinary efforts, practice of CD at the institution level, and student and faculty CD efforts.

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 2019**.
- Applicants that already have a CAE application account and have been actively gathering information may continue with their submission and submit anytime during the 2019 cycle before the closing date of 1 May 2019. Submissions are processed as they are received. Positive adjudication of applications will result in an Institution's immediate designation.
- Applicants that are new to the CAE process may start by completing a New Applicant Checklist to ascertain readiness to apply (https://www.iad.gov/NIETP/CAERequirements.cfm).
- Checklists 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 18 months 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 2019 Submission Cycle must complete their application in coordination with a designated mentor. Submissions must be received no later than 1 May 2019. 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.

CAE Cyber Defense Education 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 Specialty Areas (SAs)) 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

0. Letter of Intent and Endorsement.

Provide official notice of institutional endorsement and intent to participate in the CAE-CDE program. Shows management support of the program(s) at the institution. 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 Director
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.** Designated schools are expected to actively participate in the CAE Community and support the CAE-CD program.

Submission of this letter acknowledges the following minimum participation expectations:

- Submission of an Annual Report with all required information
- Attendance at the CAE Community Symposium each year
- Regular communication with the CAE Program Office, the CAE Community, and the CAE Regional Resource Center. (Responds to email, offers input and suggestions for workshops, programs, program decisions, etc.)
- Maintenance of institution information on https://www.iad.gov/NIETP/index.cfm

1. Cyber Defense Academic Curriculum Path

The Cyber Defense (CD) curriculum path must have been in existence for at least 3 years. Evidence must show one (1) year of student granted degrees with curriculum program path completion identified. The institution must have a mature curriculum program path in place that leads to a degree, minor or a certificate in a related cyber discipline. The path is defined as a series of courses that meet all of the mandatory foundational and core Knowledge Units (KUs) plus additional mandatory KUs of your choosing. The institution must show its curriculum path and show 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 pts mandatory

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. Courses must be mandatory for students completing the program path.
- Identify department(s) where curriculum path resides.
- If application is approved, only the CD curriculum program path identified in this criterion is allowed to be marketed as designated CAE-CDE Curriculum Path(s).

(5 pts – mandatory)

b. Student Participation in Curriculum Path

Evidence provided must include, but is not limited to:

- Student enrollment in curriculum path for the last 3 years (letter from Registrar)
- Number of students that have received a degree and completed the Cyber Defense program path within one (1) year of submission (Registrar letter)
- 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**
- Sample certificate or notation on transcript issued to students completing the CD program path

(5 pts mandatory)

c. Curriculum Program Path Identification

- Identify the **name** of the curriculum path that maps to the KUs. Only the name of the curriculum program path is required; e.g., "BS in Computer Science, Cyber minor". This information will be used to market the CAE program at the applying institution, on nsa.gov and other related websites and for program identification on the designation certificate. All other information about the program should be entered in 1a.

(0 pts awarded, but must provide - mandatory)

d. NICE Framework Crosswalk

- Identify how the mapped curriculum path relates to the NICE Cybersecurity Workforce Framework (NCWF), NIST SP 800-181. Select one or more NCWF Categories that best define the applying institution program: Operate and Maintain; Oversee and Govern; Protect and Defend; Investigate; Collect and Operate; Analyze; and/or Securely Provision. **Only identification** of the NCWF categories is required, no explanation is needed.

(0 pts awarded, but must provide - mandatory)

e. Masters/Doctoral Thesis/Dissertation requirement

- If 22 KUs are mapped to courses in the program at the applying institution then this does not pertain. Provide explanation.
- Provide evidence of your institutional requirement for Master's or Doctoral level students for program completion. Provide details of the actual assignment that is given to students to complete the thesis/dissertation.

- Also, Provide evidence as follows:
  - Masters level - Attach three (3) actual papers from students that are specific to cybersecurity. If a thesis is not required of students, explain your required equivalent and provide student work.
  - Doctoral level - Attach one (1) actual paper from students that are specific to cybersecurity. If a dissertation is not required of students, explain your required equivalent and provide student work

(0 pts if 22 KUs mapped/3 pts mandatory if thesis/dissertation/equivalent required/5 maximum)

2. Student Skill Development and Assessment

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. Courses used in this section must be KU mapped courses.

Overall Point Value: 18 pts mandatory, 25 pts maximum

a. Courses Required for Student Scholarly Skills Development

- Provide syllabi of CD courses that require papers, presentations, projects, test questions – **highlight requirement** – courses must map to the KUs and must relate to papers/projects/etc. submitted in criterion 2b
- Courses requiring papers/projects/presentations/test questions must have been taught within the last 3 years
- Courses requiring papers/projects/presentations/test questions must be a part of the CD curriculum path as identified in the application

(1 pt per course/at least 3 different courses/3 pts mandatory/5 pts maximum)

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.

- Students assessed by one or more methods: Provide actual student work (can be redacted) in the form of papers, projects, test questions, etc. from students in the curriculum path (**must** be courses in the curriculum path identified in 2a). Papers/projects, etc. **must** be clearly identified with course title, course number, and date of submission.
- Links or attachments to actual papers/projects/presentations/test questions are required – not a subscription service or

(1 pt per paper/project/etc./from at least 3 different courses/5 pts mandatory/5 pts maximum)

c. Courses Requiring Lab Exercises

- Provide syllabi of CD courses that require labs – highlight lab requirement – must relate to student labs submitted in criterion 2d, must be courses mapped to KUs

- Courses must have been taught within the last 3 years

(1 pt per course/at least 3 different courses/3 pts mandatory)

d. Students Assessed by Lab Assignments/Hands on Activities

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. Courses must be in the curriculum path.
- Provide examples of actual student lab work (**must** be from courses in the curriculum path identified in 2c) 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)

e. Student participation in cyber competitions

- Provide evidence of participation in Cyber Defense exercises and/or 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.). This can include in-class exercises with explanation.
- 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/1 pt mandatory/5 pts maximum)

f. 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 for students, etc.). Provide fliers, posters, letters, etc.

(1 pt per partnership/1 pt mandatory/4 pts maximum)

3. <u>"Center" for Cyber 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. The center shall provide the following services: program guidance and oversight; general cyber defense information; 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 pts mandatory/13 pts maximum

a. Cyber "Center"

- Cyber "Center" shall provide program guidance and general CD information, and promote collaboration and interaction with other students, faculty, and programs.

- 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 academic institutions
- The Cyber "Center" and its website must be operational, dynamic, current 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
  - 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

(8 pts mandatory)

b. External Board of Advisors

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. This board provides a connection between the program and the local community. Provide names, meeting minutes, etc.

(2 pts mandatory/5 pts maximum)

4. <u>Cyber Faculty Qualifications and Courses Taught</u>

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 **<u>must</u>** be possible to locate all permanent faculty members by searching the Institution website.

Overall Point Value: 15 pts mandatory/20 pts maximum

a. Head of the Cyber Program of Study

- Identify by name faculty member with overall responsibility for the CD curriculum path.
- Provide evidence, i.e., verification letter and/or job description. Provide link or attachment to biography, resume or curriculum vitae (CV) with cyber background clearly identified. Institution affiliation must be clearly identified.
- Highlight or list professional societies and level of effort.

(5 pts mandatory)

b. Designated Alternate and Additional Faculty

- Must identify a permanent faculty as a designated alternate for notices – CV required.
- 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 – highlight or list professional societies for each additional faculty
- Evidence must include department where the faculty member teaches and courses that they teach in CD program path of study.

(1 pt each/2 pts mandatory)

c. 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
- 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
- Faculty publications or research should be produced while employed at the submitting institution. Exceptions can be considered if most faculty work is from permanent employees and some are from new employees brought in to enhance the program

(1 pt per paper or book chapter/3 pts per book/5 pts mandatory)

d. Cyber Defense Presentations

- Provide evidence that faculty members have presented Cyber 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.)

(1 pt per presentation/1 pt mandatory/5 pts maximum)

e. Faculty support to Cyber Student activities, Clubs, Competitions, etc.

- Provide evidence that CD faculty members support enrolled 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. 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 mapped to the Knowledge Units.

Overall Point Value: 6 pts mandatory/10 pts 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. *For example*: health practitioners learning about privacy and patient electronic data protection; criminal justice learning about chain of custody for electronic evidence; or accountants learning about data backup and protection. **Provide course name and syllabus with cyber modules clearly highlighted**
- Cannot be any courses in the department or curriculum path used to map to the Knowledge Units; exception would be a course that all students are required to take on basic cyber hygiene.
- Courses taught outside the CD program of study can be technical or non-technical. For example: health practitioners learning about privacy and patient electronic data protection; accountants learning about data backup and protection; criminal justice learning about chain of custody for electronic evidence; or non-credit continuing education courses on IT security basics.

(1 pt per course/3 pts mandatory/5 pts 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 electronic patient health care records.
- Provide links to three to five best papers, presentations, projects or test questions with Cyber topics clearly highlighted within 3 years of application. **Actual student work is required – not just the assignment required of students.**
- Paper/projects/presentations/test questions must correspond to courses provided in 5a.

(1 pt each/3 pts mandatory/5 pts maximum)

6. Institutional Security Plan

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: 6 pts mandatory/9 pts 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.
(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 the 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.

(1 pt per example/2 pts mandatory/5 pts maximum)

7. **Cyber Outreach/Collaboration *Beyond* the Institution**
The institution must demonstrate how Cyber Defense practices are extended beyond the normal boundaries of the institution. Show how CD concepts developed at the Institution are shared with others or how industry theory and practice are incorporated into curriculum.
Overall Point Value: 15 pts mandatory/25 pts maximum

a. **Faculty Involvement in Sharing Expertise**
- Provide evidence of how the institution shares Cyber related 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.
- Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such

as emails, formal meeting notes, links to material on accepting parties' website, etc. is encouraged.

- Identify shared faculty (e.g., Faculty on Cybersecurity curriculum development committee). The institution should specifically state its contribution to the shared effort, (e.g. If faculty is on a curriculum development committee, what was the institution/faculty specific contribution?).

(1 pt per event/1 pt mandatory/5 pts maximum)

b. Transfer of Credit – Agreements - community college, college in high school, dual credit, etc

- Provide evidence that the institution awards credit in cyber related courses and/or technical prerequisite courses from other academic institutions, community colleges, tech schools, etc. or through alternative means. This is not meant for credit issued for general education courses. Examples include, but are not limited to: statewide transfer agreements with community colleges; articulation agreements; college in the high school; dual credit; running start; credit for prior learning; credit for military training or occupation; etc.

(1 pt per agreement/3 pts for statewide agreement/1 pt mandatory/5 maximum)

c. Support/participation to the CAE Community

- Provide evidence that the applying institution has participated in CAE events such as: CAE Symposium, CRRC workshops for candidate institutions, CAE Tech Talk/Forum used in classroom (1pt = 3 uses), collaboration on grants with CAE institutions. Provide emails, attendance roster, etc.
- Provide evidence of faculty collaborating with current CAE institutions on research, grants, course development, etc. Provide documenting information.
- Reviews/mentor/advisor, etc.

(1 pt per event/1 pt mandatory/5 maximum)

d. Community Outreach – Activities outside of student/campus events

- 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 responder training 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" (senior centers, K-12, camps, etc.) Provide fliers, emails, web announcement, etc.

(1 pt per event/1 pt mandatory/5 pts maximum)

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/1 pt mandatory/5 pts maximum)