Goal

The goal of the CAE IA-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:

- 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.

- KU Mapping - Mapping of the institution’s curriculum to the four-year core Knowledge Units (KUs) = 2 + 4 Year core and 5 optionals.
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 FA.
- 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 should be submitted via the CAE Application website – www.iad.gov/nietp. New applicants can register for an account at the above link under Login/Join. Applications and are due no later than 15 January 2016.

Qualified CD professionals and Subject Matter Experts from NSA, DHS, and other government, academic 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. The last phase of the criteria may be an on-site evaluation focused on course content, course relevance, laboratory facilities, and faculty involvement.

CAE-CDE Designation

Successful institutions 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.
CAE-CDE Program Criteria

0. **Letter of Intent as CAE-CDE and statement of CAE-CDE mission and purpose.**

Provide official notice regarding the institutional intent to participate in the CAE-CDE program. Provide formal documentation showing the establishment of an official “Cyber Center” within the institution. Letter should be on institution letterhead, signed by the Dean or higher, contain information about the Cyber Defense program and name the POC from the institution. Letter should also state accreditation information and any pertinent accomplishments in the cyber defense field. The letter should be addressed to:

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

**Mandatory requirement**

1. **“Center” for CD Education.**

The institution must have an officially established organization serving as the focal point for its CD educational program (physical or virtual). The center should 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 community at large.  

*Overall Point value: 10 points mandatory*

   a. **Cyber Center**  
   Show formal documentation of the designation of Cyber “Center.” This can be included in the letter of intent. (For the purpose of this document, the word “Center” is used in a general sense). The “Center” must have the endorsement from a Dean or higher.  
   *Point Value: 5 points mandatory*

   b. **“Cyber Center” Website**  
   Provide an operational hyperlink to the “Cyber Center” website. This “Cyber Center” should provide program guidance, general CD information and promote collaboration and interaction with other students, faculty, and programs. The “Cyber Center” and its website must be operational, dynamic, current and visible within the institution and to the community at large. Evidence provided should include, but is not limited to:
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)

information about the CD program of study and faculty, “Cyber Center” points of contact, links to student CD activities, institutional security resources and awareness, as well as up-to-date links to key CD resources such as other academic institutions, government sites, conferences, workshops, and CD news.

Point Value: 5 points mandatory

2. Cyber Defense Academic Program
The CD program of study is central to a vibrant and mature CAE for Cyber Defense Education program. The institutional must show its CD academic requirements and explain how students participate and successfully complete the CD curriculum.

Overall Point value: 17 mandatory/20 maximum

a. Cyber Defense Program of Study
Describe the CD program of study offered by the institution. What department(s) oversee the program? What types of CD curriculum paths are offered, i.e., CD major, minor, certificate program? What courses are required for those paths that satisfy the CAE requirements for all the mandatory KU requirements and at least five operational KU requirements? Provide the course path that map to the KUs. Provide a sample of a student transcript, completion letter or certificate. (Please note – Only the CD curriculum program(s)/path(s) identified in this criterion, are allowed to be marketed as CAE-CDE Curriculum Path(s)/Program(s) at an institution, if application is approved. If additional curriculum path(s)/program(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)/program(s) in the re-designation application).

Point Value: 10 points mandatory

b. Availability of Subscription-based, on-line CD publications
Provide evidence that students and faculty have access to subscription-based, on-line CD journals, books and other publications. How are these resources integrated into the curriculum and provided to students? Provide sample course materials showing references to these resources or hyperlinks to instructor webpages offered to students.

Point Value: Up to 5 points/2 mandatory
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)

c. Overview of Student Participation in program
   Provide information on the student enrollment over the last 3 years to include current
   participants and graduates. Provide numbers of students that have
   participated/graduated in the last 3 years.
   
   **Point Value: 5 points mandatory**

3. Student-based Cyber Defense Research
   The institution must show how it fosters student research in CD. This item focuses on STUDENT-
   based research as it contributes to evolution of theory and practice in the field of cyber defense.
   Research should related back to one or more of the KUs.
   
   **Overall Point value: 12 mandatory/25 maximum**

   a. Research requirements for CD program participants
      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. What are the research requirements for students participating in
      the CD program of study? Provide links to 5 to 10 of the best CD theses, dissertations,
      papers or projects produced by these students within the last 3 years. **Link to actual papers required – not a subscription service.**
      
      **Point Value: Up to 10 points/1 point per paper or project/5 points mandatory**

   b. Cyber Defense Physical/Virtual Labs
      Show that physical and/or virtual labs and equipment are available and demonstrate
      how these resources are used by students and faculty to support the Cyber Defense
      program of study. Evidence provided should include either a description or links to
      information about the lab resources available as well as samples of lab projects or
      exercises.
      
      **Point Value: Up to 5 points/2 points mandatory**

   c. List of courses requiring research and/or labs
      Provide a list of CD courses that require research papers or labs and links to the course
      syllabi. Courses need to be either current or taught within the last 3 years.
      
      **Point Value: Up to 10 Points/1 point per course/5 courses mandatory**
4. Cyber Defense Faculty and Course load
The institution must demonstrate that it has someone responsible for the overall CD program of study and sufficient faculty members, either full- or part-time, teaching at least one CD course. The criterion requires a link to the biography or curriculum vitae for each faculty member. It must be possible to locate all faculty members from the University website.

*Overall Point Value: 9 points mandatory/20 points maximum*

   a. **Head of the Cyber Defense Program of Study**
      Identify by name the full-time employee or employees with overall responsibility for the CD program of study at the institution. Evidence must include a job description and biography or CV.
      
      *Point Value: 5 points mandatory*

   b. **Additional full-time Cyber Defense faculty members**
      Identify by name full-time faculty members teaching the courses in the CD program of study. Evidence must include a job description and biography or CV. Also required is the department where they teach and course load.
      
      *Point Value: 2 point each/4 points mandatory/10 points maximum*

   c. **Part-time or Adjunct Cyber Defense Faculty members**
      Identify by name part-time or adjunct faculty members teaching the courses in the CD program of study. Evidence must include a job description and biography or CV. Also required is the department where they teach and course load.
      
      *Point Value: 1 point each/5 points maximum*

5. Cyber Defense Faculty Expertise and Research
The institution must show that the faculty members are CD experts and are active in current CD practice and research. Cyber Defense faculty members should be contributing their CD knowledge to publications, presentations, and professional societies as well as seeking grants for CD resources and mentoring CD students.

*Overall Point Value: 9 points mandatory/41 points maximum*

   a. **Faculty authored Cyber Defense publications**
      Provide evidence of faculty contributions to peer reviewed publications on CD topics to include refereed journals and conference proceedings within the last 3 years. Provide links to actual papers not a subscription service.
      
      *Point Value: 2 points per paper/2 papers mandatory/10 points maximum*
b. Published books or chapters of books on Cyber Defense/Cybersecurity
   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 5A, not 5B.
   
   Point Value: 5 points per book/1 point per chapter/10 points maximum

c. Cyber Defense Presentations
   Provide evidence that faculty members present CD content at major Regional/National/International conferences and events within the last 3 years. Provide a synopsis of the involvement. This can include guest lecturer at other institutions or government organizations.
   
   Point Value: 1 point per conference/2 presentations mandatory/6 points maximum

d. Professional societies
   Provide evidence that faculty members are CD subject matter experts for accrediting bodies and professional societies. (e.g., ACM, IEEE, regional accreditation, professional accreditation, etc.). Faculty members are active members in CD/Cybersecurity organizations (e.g., ISSA, Cyberwatch, Infraguard, etc.). List involvement for the last 3 years.
   
   Point Value: 2 points per review or membership/2 points mandatory/6 points maximum

e. 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 are not obtained.
   
   Point Value: 2 points per award or funding/6 points maximum

f. Support to Cyber Defense Student activities
   Provide evidence that CD faculty members support their student by serving as mentors or advisors to student led activities. Evidence can include links to student clubs, Cyber Defense Exercises, etc.
   
   Point Value: 1 points per program/1 mandatory/3 points 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 related fields.

**Overall Point Value: 7 points mandatory/15 points maximum**

   a. Cyber Defense Concepts taught in other fields of study
   Provide evidence that CD topics are taught in courses outside the CD program of study department and its courses. Courses taught outside the CD program of study could 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. Provide course name and syllabus with cyber modules highlighted.
   
   **Points: 2 point per course/2 courses mandatory/up to 10 points.**

   b. Non-Cyber Defense courses encourage papers or projects in CD topics.
   Courses taught outside the CD program require papers/projects/posters/etc. For example: health care practitioners write a paper on the importance of safeguarding patient health care records. Provide links to 5 to 10 best papers or projects on CD within 3 years of application. **Link to actual papers required – not a subscription service. Paper/projects should correspond to courses provided in 6a.**
   
   **Points: 1 point per item (3 mandatory)/only 2 items per course/up to 5 points.**

7. Institution Information System (IS) Security Plan

**Overall Point Value: 16 points minimum/20 points maximum**

   a. Security plans or polices
   Provide links to the CD/IS Security Plan(s) or policies for the institution to show how it practices institutional security.
   
   **Points: 5 points mandatory**

   b. Institutional Cyber Security/Information Security Officer
   Provide the name, title and job description for the individual responsible for the information IS program at the institution.
   
   **Points: 5 points mandatory**
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)

---

c. Implementation of Cyber Security Practices
   Provide evidence of how the institutional implements its CD 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.)

   **Points: 6 points mandatory/10 points maximum**

8. Cyber Defense Outreach Beyond the Institution
   The institution must demonstrate how CD is extended beyond the normal boundaries of the institution.

   **Overall Point Value: 15 mandatory/30 maximum**

      Show how the institution shares its CD curriculum or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities within the last 3 years. Provide 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: Up to 5 points/3 points mandatory**

   b. Reciprocity of Credit
      Provide evidence of written agreements showing that the institution accepts credit in CD courses and/or prerequisite courses from other academic institutions. (e.g., Accepting academic credit in CD courses from minority institutions, two-year community colleges, or technical schools). Must show the course designator and how it translates to the accepting school.

      **Point Value: Up to 5 points/3 points mandatory**

   c. Sponsorship or participation in Cyber Defense Exercises and Competitions
      Provide evidence of participation in or sponsorship of CD exercises and competitions within the last 3 years.

      **Point Value: Up to 5 points**
d. **CAE Collaboration**
   Show how the institutions partners in CD research or shared classes/events with other CAE institutions.
   
   *Point Value: Up to 5 points*

---

e. **Cyber Defense Business/Industry Collaboration**
   Show how the institution partners with companies and other employers to identify CD needs of potential employers and encourage student internships. Show how the institution works with employers and students to support job placement.
   
   *Point Value: Up to 5 points*

---

f. **Community Outreach**
   Show how the institution sponsors CD events for the community at large. Events could include CD awareness and education for local schools, adult education centers, and senior centers. Examples of events could be computer “check-up” days, protecting personal information in cyber space, or preventing and recovering from a “virus”.
   
   *Point Value: Up to 5 points/2 mandatory*