

**National Centers of Academic Excellence in  
Information Assurance/Cyber Defense (IA/CD) 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 IA/CD program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in Information Assurance/Cyber Defense (IA/CD) and to produce a growing number of professionals with expertise in IA/CD disciplines. This program will contribute significantly to the advancement of state-of-the-art IA/CD knowledge and practice.

**Vision**

The vision of the CAE IA/CD Program is to:

1. Provide programs that commit to excellence in the field of Information Assurance and Cyber Defense education at the graduate and undergraduate levels.
2. Provide the Nation with a pipeline of qualified students poised to become IA/CD professionals.
3. Continuously improve the quality of IA/CD programs, curriculum, faculty, students and other institutions.
4. Emphasize faculty efforts in improving IA/CD scholarship, professional development and instructional capabilities.
5. Foster and encourage further development of strong IA/CD focused education and research depth at U.S. institutions.

**CAE IA/CD Program Eligibility and Summary**

The CAE IA/CD 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 IA/CD requirements are:

- Program Requirements - Demonstration of program outreach and collaboration, center for IA/CD education, a robust and active IA/CD academic program, IA/CD multidisciplinary efforts, practice of IA/CD at the institution level, and student and faculty IA/CD efforts; (*Criteria below*);
- Courseware requirements - A core (mandatory) set of IA/CD Knowledge Units (KUs) that all institutions must address in their curriculum; and choose five KUs from a set of additional KUs, to which institutions must map

Completion of these requirements will designate the institution as a NSA/DHS National Center of Academic Excellence for Information Assurance/Cyber Defense (CAE IA/CD) Education. Institutions shall demonstrate that students can successfully complete the CAE IA/CD course of study and receive recognition on a transcript, diploma, etc.

# 2014 NSA/DHS National CAE IA/CD Criteria

---

## Focus Area (Optional)

All CAEs have the option to apply for one or more CAE IA/CD Focus Area (FA) designations.

The criteria include:

- 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.

## Knowledge Units:

The KU section will require the institution to address how it meets each Core and chosen Optional 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.

## Program Evaluation:

Institutions will be evaluated by CAE Program staff with assistance from Subject Matter Experts. The last phase of the criteria may be an on-site evaluation focused on course content, course relevance, laboratory facilities, and faculty involvement.

## CAE IA/CD Designation:

Successful institutions will be designated as a National Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD). Due to the requirement to have all current institutions designated by 2014, designation periods granted during this designation cycle will range from three to six years from the institution's application. This will allow a more distributed range of re-applications in the future. Subsequent cycles will revert to a five year cycle. The initial designation period will be dependent upon timing of the application, with allowances for changes by the program office. Future criteria (including KUs and FAs) will continue to be reviewed annually and strengthened as appropriate to keep pace with the evolving nature of IA/CD. Designation as a National CAE IA/CD does not carry a commitment of funding from NSA or DHS.

## 2014 NSA/DHS National CAE IA/CD Criteria

---

### CAE IA/CD Program requirements:

1. *Outreach/Collaboration.* The institution must demonstrate how IA/CD is extended beyond the normal boundaries of the Institution.

**Overall Point Value: 15 points minimum/25 points maximum**

- a. Shared curriculum (e.g., IA/CD teaching materials provided to minority colleges/universities, two-year community colleges, technical schools, or K-12 schools) or shared faculty (e.g., Faculty on IA/CD curriculum development committee and/or teaching IA/CD at minority colleges and universities, two-year community colleges, technical schools, or K-12 schools.)

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

- b. Reciprocity of credits (e.g., Accepting academic credit in IA/CD courses from minority institutions, two-year community colleges, or technical schools.). Evidence in the form of written agreements must demonstrate that IA/CD-related courses from the above types of schools are accepted for credit at the applying institution.

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

- c. Sponsorship of or participation in Cyber Defense or Forensics Exercises and competitions within 3 years of submission. Sponsorship of state, regional, or national IA/CD curriculum workshops, colloquia, etc. (e.g., sponsorship of workshops for K-12, community colleges, technical schools, state homeland security, industry, etc.).

**Point Value: Up to 5 points**

- d. CAE Collaboration. Partner in research/shared classes or shared events with other institutions. Institutions are encouraged to partner with other CAEs on cyber or IA/CD research/instruction.

**Point Value: Up to 5 points**

- e. Community Outreach. Sponsorship of community events such as cybersecurity education for local schools, adult education centers, senior centers, etc. (e.g., schools in a target region are encouraged to participate in cybersecurity education events, like community computer diagnostic “check-ups” and IA/CD awareness days.)

**Point Value: Up to 5 points**

## 2014 NSA/DHS National CAE IA/CD Criteria

---

2. *Center for IA/CD Education.* The institution must have a formal organization for use as a resource for faculty and students. The Center should provide program guidance, general IA/CD information and promote collaboration and interaction with other students, faculty, and programs. (For the purpose of this document, the word “Center” is used in a general sense). **The Center and the website must be operational, dynamic and current.**

**Overall Point Value: 14 points minimum/20 points maximum**

- a. Show formal documentation of the designation of the IA/CD/Cybersecurity “Center” and provide a hyperlink to the “Center.”

**Point Value: 5 points required**

- b. Demonstrate the “Center” website is operational, dynamic and current: contains up-to-date links to key IA/CD resources such as other academic institutions, government sites, conferences, workshops, IA/CD news, center POCs, IA/CD courses, etc. The website must be easy to find and easily accessible. Demonstrate how students know about the website.

**Point Value: 5 points required**

- c. Provide evidence that subscription-based, on-line IA/CD journals are available for student and faculty use. . Demonstrate that hyperlinks to key IA/CD .on-line resources are provided in course syllabus and/or professors’ webpage or provided to students during class instruction.

**Point Value: Up to 5 points/2 required**

- d. Demonstrate that physical and/or virtual IA/CD labs and equipment are available and used for hands-on learning (provide examples of student lab projects/exercises/case studies – syllabus, links to assignments, etc.).

**Point Value: Up to 5 points/2 required**

3. *A robust and active IA/CD academic program.* Demonstrate how students successfully participate in the academic program requirements to meet the IA/CD curriculum.

**Overall Point Value: 5 points minimum/ 20 points maximum**

- a. Provide evidence that students who participate sufficiently in the IA/CD curriculum (i.e., take and pass courses that satisfy all of the mandatory KU requirements and at least five of the optional KU requirements) will receive a certificate, or a reference to completing the CAE IA/CD course of study on their transcript and/or degree. Provide evidence in the form of a letter, transcript notation, and/or degree (student information may be redacted)

**Point Value: 10 points/Students are taking the IA/CD curriculum path**

**5 points/Students have an opportunity to take the IA/CD path**

- b. Provide evidence that students who participate sufficiently in the IA/CD curriculum for a Focus Area (i.e., take and pass courses that satisfy all of the mandatory KU requirements for that Focus Area) will receive certificate, or a reference to a focus area on their transcript and/or degree (student information may be redacted).

**Point Value: 10 points/Students are taking the IA/CD curriculum path**

**5 points/Students have the opportunity to take the IA/CD path**

## 2014 NSA/DHS National CAE IA/CD Criteria

---

4. *IA/CD is multidisciplinary within the institution.* The institution must demonstrate that IA/CD is not treated as a separate discipline, but as a multidisciplinary science with the body of IA/CD knowledge incorporated into various disciplines.

**Overall Point Value: 7 points minimum/ 10 points maximum**

- a. Evidence that IA/CD is taught as modules in existing non-IA/CD courses and that non-technical/non-IA/CD students are being introduced to IA/CD. For example: IA topics such as security countermeasures are covered in courses for managers/leaders/non-technical students.

**Points: 1 point per course/2 courses required/up to 5 points.**

- b. Non-IA courses encourage papers in IA topics or projects. Provide **links** to 5 to 10 best thesis, dissertation, or projects in IA within 3 years of application. **Link to actual papers required – not a subscription service.**

**Points: 1 point per paper/only 2 papers per course/up to 5 points.**

5. *Practice of IA encouraged throughout the Institution.* The academic program must demonstrate how it encourages the practice of IA, not merely that it teaches IA.

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

- a. Provide a **link** to the Institution IA security plan. **(required)**

**Points: 5 points required**

- b. Provide name, position and job description for person or persons responsible for information security at the institution.

**Points: 5 points required**

- c. Provide evidence of the implementation of the Institution's IA security plan that encourages IA awareness throughout the campus (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. - 2pts awarded per item).

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

6. *Student-based IA/CD/Cybersecurity research.* The institution must demonstrate how it encourages research in IA/CD. This criterion focuses on **STUDENT**-based research and is important because research fuels the relevancy and currency of IA curricula. Research should relate back to one or more KUs.

**Overall Point Value: 10 points minimum/30 points maximum**

- a. Program with IA/CD focus has thesis, dissertation, student papers, or independent research project requirements. Focus areas include declared majors, declared minors, established certificates of study within a major that produce research papers/projects. Provide links to 5 to 10 best actual thesis, dissertation, student papers, or projects in IA within 3 years of application (student information may be redacted).

**Point Value: 1 point per paper or project/5 points required/10 points maximum**

- b. List IA/CD courses that require research paper(s) or virtual/physical lab project(s). Provide IA course titles that require these papers/lab projects within 3 years of application. Provide link to course syllabus.

**Point Value: 1 point per course/3 points required/20 points maximum**

## 2014 NSA/DHS National CAE IA/CD Criteria

---

7. *Number of IA/CD/Cybersecurity faculty and course load.* The institution must demonstrate that IA/CD faculty consists of a sufficient number of full time IA/CD faculty members and additional faculty members (may be part-time, adjunct, visiting professor, etc.) teaching at least one IA/CD course. This criterion **requires a link** to a biography or curriculum vitae for each faculty member.  
**Overall Point Value: 8 points minimum/16 points maximum**

- a. Identify by name full-time employee or employees, as defined above, either faculty or member of the administration working in IA with overall responsibility for the IA Instructional Program. **Provide evidence, i.e., letter of testimony or job description. Provide link to biography or CV.**  
**Point Value: 5 points required**
- b. Identify by name additional full-time IA faculty members (not listed in 7.a.), teaching IA/CD courses within the department that sponsors IA/CD programs. **Provide link to biography or CV.**  
**Point Value: 2 point each/6 points maximum**
- c. Identify by name part-time, shared (inter departmental, other institution, etc.), adjunct (industry expert, etc.) teaching IA/CD courses within the department that sponsors IA/CD programs. **Provide link to biography or CV.**  
**Point Value: 1 point each/5 points maximum**

## 2014 NSA/DHS National CAE IA/CD Criteria

---

8. *Faculty active in current IA/CD/Cybersecurity practice and research.* The institution must clearly demonstrate that the faculty is active in current IA/Cyber practice and research, contributes to IA literature, and are members of IA professional societies are subject matter experts or attend/present at professional IA conferences.

**Overall Point Value: 15 points minimum/37 points maximum**

- a. Peer reviewed publications – papers (electronic or traditional) on IA/CD/Cybersecurity as evidenced in refereed journals or conference proceedings within the past 3 years. **Provide links to actual papers not subscription service.**  
**Point Value: 2 points per paper/8 points maximum**
- b. Published books or chapters of books on IA/CD/Cybersecurity. Books/chapters must focus on IA and have been published within the last 5 years. **Provide title, authors and date published. ID specific chapters if authoring a chapter of a book.**  
**Point Value: 5 points per book/1 point per chapter/10 points maximum**
- c. Faculty is involved in writing grants and obtaining funding for IA education and/or research development or lab equipment. Provide synopsis of IA related grants, funding, equipment donations, or other funding to include date and approximate monetary value for the past 3 years.  
**Point Value: 2 points per award/6 points maximum**
- d. Faculty members are subject matter experts (IA/CD/Cybersecurity) for accrediting bodies and professional societies for IA/CD/Cybersecurity, (e.g., ACM, IEEE, regional accreditation, professional accreditation, etc.). Faculty members are active members in IA/CD/Cybersecurity organizations (e.g., ISSA, Cyberwatch, Infraguard, etc.) **List involvement for the last 3 years.**  
**Point Value: 2 points per review/membership/6 points maximum**
- e. Faculty members are engaged in and/or initiate student IA programs.  
**Point Value: 1 points per program/3 points maximum**
- f. Faculty presents IA/CD/Cybersecurity content at major Regional/National/International conferences and events. Provide synopsis of involvement for the last 3 years.  
**Point Value: 1 point per conference/4 points maximum**

### **CAE IA/CD Knowledge Unit requirements:**

In addition to the above Program Requirements, institutions must also map their curriculum to the Knowledge Units.