2021 National Centers of Academic Excellence in Cyber Research (CAE-R) Criteria

Goal

Proactively increase our understanding of robust cyber technology, policy, and practices that will enable our Nation to effectively prevent and respond to a catastrophic cyber event.

Vision

Establish a process that will:

- Recognize schools with programs that integrate cyber research activities into the curriculum and into the classroom setting.
- Provide NSA, its partner agencies and the larger federal community with insight into academic cyber programs (with their reach into industry) that can support advanced academic, research, and development capabilities.
- Serve as potential source and facilitator for government-academia researcher exchanges.
- Present opportunities for cyber research centers to drill deeper into much needed solutions for securing critical information systems and networks.

CAE-R Program Eligibility and Summary

All CAE-R applicants must be:

- A DoD school, a PhD producing military academy, or a regionally accredited PhD degree granting college or university.
- Rated as either a Doctoral University – Highest Research Activity (R1), Doctoral University – Higher Research Activity (R2), or Doctoral University – Moderate Research Activity (R3) as determined by the Carnegie Foundation Basic Classification system (and/or other independent body to measure CD) or provide a written justification as to significant CD research.

The CAE-R criteria include:

- Demonstration of cyber research initiatives (faculty and student)
- Core cyber publications and their impact
- Graduate-level cyber student production (Masters and PhD)
- Funding for core cyber research
- Adequate student cyber subject matter preparation

The burden is on the college/university to provide clear and concise evidence within the CAE application for each of the criteria. Designated schools are expected to actively participate in the CAE Community and support the National Centers of Academic Excellence (NCAE) program.

CAE-R Program Requirements

0. Letter of Intent

Provide a document, on University letterhead, stating the Institution's intent to apply for CAE in Cyber Research (CAE-R). The letter should be signed by a Provost or higher stating University backing of the program, accreditation status and Carnegie Foundation ranking or similar. The letter should be addressed to:

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

The Letter of Intent is uploaded in the CAE application – do not mail.

Submission of this letter acknowledges the following minimum participation expectations:

- Submission of an annual update with all required information. Be available to discuss responses should the CAE Program Office have questions about any submitted information.

- Attendance at the CAE Community Symposium or CAE Principals Meeting each year. If attendance isn't feasible in a particular year, contact the CAE Program Management Office (caepmo@nsa.gov) for a suitable alternative.

- Represent institution by participating in CAE Program activities and projects and maintaining regular communication with the CAE Program Management Office and the CAE Community. This includes, but is not limited to:
  - Acting as a Mentor, Advisor, or Reviewer
  - Participating in a Working Group
  - Provide timely input on questions and projects managed by the CAE PMO
  - Contribute curriculum, time, and resources in support of the CAE Community as a whole
  - Share expertise via a CAE Forum or Tech Talk.
  - Maintain institution information in the application tool. Update the appropriate Point of
  - Contact and President information is regularly to ensure PMO correspondence is received by the intended recipients.
  - Submission of an Annual Report with all required information

- Virtually attend at least one CAE Tech Talk or CAE Forum calendar year.

- Answer annual call for CAE Program Book updates. (View current version here: www.caecommunity.org/content/cae-marketing-materials).

1. Cyber Foundation

Applicants applying for CAE-R must be actively linked to research being conducted and show an adequate Cyber Security foundation. Criteria for pathway to get to PhD (showing foundational education).

a. Cyber Research Initiatives
Evidence of significant engagement in cyber research initiatives, community service, outreach, and collaboration regarding cyber. Examples include the following: conducting

research, serving on technical program committees of conferences, editing journals, hosting conferences and workshops, and assisting/collaborating with the government (federal, state, local), academia, industry, and the local community. Evidence must be less than five years old and show a variety of engagement activities.

b. Cyber Area of Study
The academic program, within a regionally accredited four-year college or graduate-level university, has a sufficient area of study in cyber (Major, Minor, Certificate, or Concentration). Provide syllabi of the cyber-related courses needed for each indicated area of study. Provide the documented process for accepting students into the Doctoral cyber program at your institution.

c. Declared Cyber Center
The university has a declared, operational, and active center for cyber education or a center for cyber research. Provide a link to the center's website.

2. Research Rating

The institution must be rated as either a Doctoral University – Highest Research Activity (R1), Doctoral University – Higher Research Activity (R2), or Doctoral University – Moderate Research Activity (R3) as determined by the Carnegie Foundation Basic Classification system **http://carnegieclassifications.iu.edu/**, and/or other independent body to measure cyber; or a DoD school/or PhD producing military academy. If a university does not have a research rating or designation, a written justification of the university's significant cyber research credentials may be submitted for consideration.

3. Faculty CV

Clearly demonstrate that the faculty is active in current cybersecurity practice and research and contributes to cyber literature. Substantiate breadth and depth of faculty expertise through submission of biographies and bibliographies with link to CV. Highlight the main areas of cyber research/expertise **and** the CD courses taught in the documents. The University faculty must include at least 3 full-time instructors who teach courses that contain cyber related material **and** who conduct research in the cyber area. All material must have been completed/conducted within the last five years.

4. Publication and Research

Evidence of a strong peer-reviewed cyber publication record by faculty and students, research papers and their impact. Evidence should demonstrate the breadth and depth of cyber expertise at the institution.

a. Peer-reviewed CD publication

The baseline that distinguishes research from technical writing is peer evaluation. Those aspiring to CAE-R status must provide evidence of a strong peer-reviewed cyber publication record by faculty and students. pdfs and links are appropriate; CAE-R faculty should be highlighted. Organize and list the publications by major cyber core areas: 1. Principles, 2. Security Mechanisms/Functionality, 3. Architectures, 4. Assurance, 5. Operations, 6. Analysis, and 7. Non-technical IA Issues; or CAE CD Specialization Areas.*****

(Examples of publications: books or chapters of books, peer reviewed journals, peer reviewed conference reports/presentations, peer reviewed electronic publications, technical/trade magazines, invited presentations, and graduate-level thesis/dissertation.)

b. CD Research Expertise/Impact

What are your school's areas of expertise?

Include impact of research in at least two of the cyber core areas**.** Include the number of published papers with a narrative on how they influence the cyber community (number of citations, etc.). Published papers must have been published in the last five years. Narrative should be between 3 and 6 sentences and should clearly define how that particular core area has impacted the cyber community.

c. Relevant Papers

Provide links to 10 to 20 cyber-related papers published within the last five years. The focus of the papers must clearly be cybersecurity related, not EE or IT. Organize the papers by the core areas to support the areas of expertise identified in 4.b. The links should provide access to complete papers with contributions highlighted. Do NOT provide links to a subscription service.

***Cybersecurity Core Area List**

Includes, but is not limited to the following:

1. Principles

- Domains and domain separation
- Resources and resource isolation
- Privileges and least privilege
- Layering
- Application of principles to function, component and system levels
- Composition

2. **Security Mechanisms / Functionality**
   - Cryptography
   - Identification and Authentication
   - Authorization and Access Controls
   - OS/DBMS/Network mechanisms

   Security Mechanisms / Functionality (cont'd)
   - Trusted processes (what are they, when are they needed)
   - Virtualization
   - Biometrics
   - Audit, monitoring, anomaly detection, DLP
   - Wireless, link, and signal security
3. **Architectures**
   - Network models
   - OS/DBMS/Network architectures
   - OS/DBMS/Network subjects and objects (active entities and data containers)
   - Cloud, Grid, distributed computing
   - Custom/specialized architectures (e.g., Ad-hoc networks, SCADA, DLT)
   - Interconnectivity and routing
   - Privilege and separation issues
   - Components vs. Solutions vs. Systems
   - Critical infrastructure security
4. **Assurance**
   - Software
   - Hardware
   - Testing (functional, penetration, black box, white box, measurement, etc.)
   - Modeling and Formal methods (must focus on feasibility, applicability, strengths/weaknesses)
5. **Operations**
   - Configuration
   - Security automation/orchestration
   - Intrusion detection/analysis/remediation
   - Asset Discovery
6. **Analysis**
   - Cryptanalysis
   - Malware analysis
   - Forensics
   - Data mining
   - Process
   - Audit
   - Certification and accreditation
7. **Non-technical CD Issues**
   - Legal issues
   - Policy issues
   - Privacy
   - Business Case / Economics
   - Awareness
   - Supply Chain

Please note:
Additional research products considered in this section include other cyber related publications and software or hardware artifacts.

5. Graduate-level Production

The CAE-R applicant must provide evidence that the school is producing graduate level (PhD and Masters) students in cybersecurity.

a. Current Student Enrollment/Graduation
The CAE-R candidate school should have an average of three PhD students enrolled in any given year conducting research in cybersecurity. In addition, three PhD students currently studying cyber should be expected to graduate within a future five-year period. Provide student name, faculty advisor, research area/title, status, number of CD publications, and expected date of graduation. Upon re-designation, institutions should be able to prove that these students graduated or provide an explanation to account otherwise.

b. Relevant Student Papers
Provide links to a minimum of five papers/works by current PhD and Masters Students conducting research in cybersecurity. The focus of the papers/works must clearly be cybersecurity. The links should access complete papers or links to available papers. Contributions must be highlighted. Do NOT provide links to a subscription service. Do not include graduate papers listed in 4a.

a. Recent Graduates
Provide information regarding the number of PhD and Masters Graduates who completed a cybersecurity-focused thesis/dissertation (complete with name, date, research area, and thesis title and ***link to paper***), regardless of department (such as CS, EE, MIS, or Math) in the last five years. The focus of the theses/dissertations must clearly be cybersecurity. Transcripts should be provided.

6. Research Funding

The CAE-R applicant must provide a history of cybersecurity research funding for the past five years and, wherever possible, from national sources such as DARPA, NSF, and IARPA. Include highlights of the cyber aspect of at least 10 of the institution's best research projects, in addition to a brief description of other cyber-related research projects. Wherever possible, documentation from the funding source (government, industry, etc.) verifying that funded research in core cybersecurity and with cybersecurity implications of a significant level and impact is occurring, and/or provide evidence of patents awarded, or applied for if applicable. Documentation from the funding source can be a link to the specific award on the funding source website, such as those found for NSF awards at https://www.nsf.gov/awardsearch/ . If documentation from the funding source is not available, a letter of verification from the Dean will suffice. The program should produce evidence of conducting cyber research/study of potential benefit to national/homeland security.

7. Subject Matter Preparation

Graduate/research programs must demonstrate that students have received adequate cybersecurity subject matter preparation either at the university or as a transfer from another university. Explain how you determine your graduate level research students have a sufficient cyber background (a good

grounding in Cyber fundamentals) to prepare them for advancing scientific study in support of cybersecurity. What specific Cyber coursework and/or activities are required? The requisite subject matter must encompass the Cybersecurity field or demonstrate relevance to the field. Submit three transcripts with student name and identifying information removed to show formal course of study.

Evaluation Criteria

1. Either a current CAE in Education or must meet:
    a. Cyber research initiatives Yes ___ No ___
    b. Cyber area of study Yes ___ No ___
    c. Declared Cyber Center Yes ___ No ___

2. Carnegie Foundation Classification level Yes ___ No ___

3. Faculty CV
    3 faculty who teach/conduct research Yes ___ No __

4. Publications:
    a. Peer reviewed publications Yes ___ No ___
    b. Cyber Expertise/Impact Yes ___ No ___
    If no impact – explanation? Yes ___ No ___
    c. Ten Papers by core area Yes ___ No ___

5. Graduate-level Production
    a. Enrollment (avg 3/yr + 3 grads in 5yr) Yes ___ No ___
    b. Student papers (at least 5) Yes ___ No ___
    c. Recent graduates (name/date/link) Yes ___ No ___

6. Research Funding/Grants
    New and sustained research funding Yes ___ No ___
    Quality – Evidence of significant impact Yes ___ No ___

7. Adequate Subject Matter Preparation Yes ___ No ___

Review Process

Members of the cybersecurity research community will conduct reviews. Two reviewers will review each application, independently. If the two reviews are not in agreement, a third reviewer will be assigned. The program office will make a final determination based on all three assessments.

CAE-R Program Terms

- The burden is on the university to clearly demonstrate their qualifications for the CAE-R Program.
- Evaluation results will be provided to each applicant regarding their own application. Reviewer comments will be provided upon request.
- CAE-R status is good for a period of five academic years.
- If an application is not approved, the University may reapply during the next annual cycle.