

**National Centers of Academic Excellence in
Information Assurance/Cyber Defense (IA/CD) Research (CAE-R)
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-R program is to proactively increase our understanding of robust IA/CD technology, policy, and practices that will enable our Nation to effectively prevent and respond to a catastrophic cyber event. This program will contribute significantly to the advancement of state-of-the-art IA/CD knowledge and practice.

Vision

The vision of the CAE-R Program is to recognize institutions that:

1. Recognize schools with programs that integrate research activities into the curriculum and into the classroom setting.
2. Provide NSA, DHS, and other federal, state and local agencies with insight into academic IA/CD programs (with their reach into industry) that can support advanced academic, research, and development capabilities.
3. Serve as potential source and facilitator for government-academia researcher exchanges.
4. Present opportunities for IA/CD research centers to drill deeper into much needed solutions for securing critical information systems and networks throughout the Nation.
5. Ensure the future strength of IA/CD education and research in our nation by encouraging the development of future faculty and research leaders.

2014 NSA/DHS National CAE IA/CD Criteria

Re-designating CAE-R Program Requirements

There are six foundational criteria for establishing CAE-R: Please review the following criteria for compliance then provide the information requested for existing CAE-R institutions after criteria 6:

1. Applicants must either be an existing Center of Academic Excellence in Information Assurance/Cyber Defense Education or meet the revised CAE criteria outlined here:
 - a. Provide evidence of significant engagement in IA/CD research initiatives, community service, and outreach with regard to IA/CD research initiatives, such as serving on technical program committees of IA/CD conferences, editing IA/CD journals, hosting conferences and workshops, and collaborating with or assisting local government, business, universities and industry.
 - b. The academic program encourages research in IA/CD. This criterion focuses on STUDENT-based research. Provide titles and links to theses, dissertations, or projects within the last five years. Provide links to actual papers, not a subscription service.
 - c. The academic program, within a regionally accredited four-year college or graduate-level university, has an area of study in IA/CD that link to the attached Focus Area document. Provide syllabus for courses as evidence.
 - d. The university has a declared center for IA/CD education or a center for IA/CD research.
2. The institution must be either a DoD school/or Ph.D. producing military academy or be rated as either Research University - Very High Research Activity (RU-VH), a Research University – High Research Activity (RU-H), or a Doctoral/Research University (DRU) as determined by the Carnegie Foundation Basic Classification system (and/or other independent body to measure IA/CD or written justification as to significant IA/CD research).
http://classifications.carnegiefoundation.org/lookup_listings/institution.php
3. It is clearly demonstrated that the faculty is active in current IA/CD practice and research and contributes to IA/CD literature. Substantiate depth and length of faculty expertise through submission of biographies and bibliographies with link to CV including main areas of IA/CD research/expertise. The university faculty must consist of more than one full-time instructor who teaches courses that contain IA/CD related material and who conducts research in the IA/CD area.
4. Publication. The baseline that distinguishes research from technical writing is peer evaluation. Those aspiring to CAE-R designation must provide evidence of a strong peer-reviewed publication record by IA/CD faculty and students. (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 theses/dissertations). Include impact of research – number of papers and how they impact the IA/CD community. Use the attached Focus Area Document and core area list (below) as a reference to highlight your institution's area of expertise. Your research should be in at least one of the core areas listed below or in a Focus Areas (FA). Research conducted in an area that is not encompassed by a FA or the core list must show relevance to the IA/CD discipline for inclusion in the future. Provide links to 10 to 20 actual papers (not a subscription service) that highlight your area of expertise in IA/CD research – it is strongly encouraged that research be conducted in more than one core area. Other research products considered in this section include other IA publications and software or hardware artifacts.

2014 NSA/DHS National CAE IA/CD Criteria

Core area list – includes, but is not limited to the following:

- Principles
 - Domains and domain separation
 - Resources and resource isolation
 - Privileges and least privilege
 - Layering
 - Application of principles to function, component and system levels
 - Composition
- Security Mechanisms / Functionality
 - Cryptography
 - Identification and Authentication
 - Authorization and Access Controls
 - OS/DBMS/Network mechanisms
 - Trusted processes (what are they, when are they needed)
 - Virtualization
 - Biometrics
 - Audit, monitoring, anomaly detection, DLP
 - Wireless, link, and signal security
 - Policy (expression, composition, enforcement)
- 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)
 - Connectivity, switching, routing, dynamic networks
 - Privilege and separation issues
 - Components vs. Solutions vs. Systems
 - Critical infrastructure security
- Assurance
 - Software
 - Hardware
 - Testing (functional, penetration, black box, white box, measurement, etc.)
 - Modeling and Formal methods (need focus on feasibility, applicability, strengths/weaknesses)
- Operations
 - Configuration
 - Security automation
 - Intrusion detection/analysis/remediation
 - Resilience, recovery, reconstitution
- Analysis
 - Cryptanalysis
 - Malware analysis
 - Forensics
 - Data mining and anomaly detection
 - Process
 - Audit
 - Certification and accreditation
 - Tradecraft analysis
- Non-technical IA Issues
 - Legal issues
 - Policy issues

2014 NSA/DHS National CAE IA/CD Criteria

- Privacy
 - Business Case / Economics
 - Awareness
 - Supply Chain
5. Graduate-level Production. The CAE-R applicant must provide evidence that they are producing graduate level (Ph.D. and Masters) students in IA/CD. Provide information regarding the number of M.S. or Ph.D. students who completed an IA/CD focused thesis (complete with name, date, and thesis title and link), regardless of department (such as CS, EE, MIS, Math, etc.). The thesis or dissertation must have a clear IA/CD focus. The CAE-R candidate school should have an average of three Ph.D. students enrolled with an IA/CD emphasis in a one-year period. In addition, three Ph.D. students should graduate within a five-year period. Provide links to the best works of Ph.D. or Masters students in the area of IA/CD (at least 3).
6. Research Funding. The CAE-R applicant must provide a history of research funding for the past five years and, wherever possible, from sources such as DARPA, NSF, HSARPA, and IARPA. Include highlights of the IA/CD aspect of at least 10 best research projects, in addition to a brief description of other IA/CD related research projects. Wherever possible, documentation from the funding source (government, industry, etc.) verifying that funded research in core IA/CD and with IA/CD implications of a significant level and impact is occurring, and/or provide evidence of patents awarded, or applied for if applicable. 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 research/study of particular interest to NSA and DHS.
-

For existing CAE-R institutions:

- I. I certify that all information entered in the CAE-R submission is truthful and accurate. I verify that (name of University) still meets all of the existing criteria, including 1a. – 1.d (include IA/Cyber Defense Center link) and that grant levels are equal to or greater than when we originally applied.
- _____ (signature)
- II. Provide links to 5 faculty papers and 5 graduate-level papers since last designation, up to 5 years. The research papers shall follow the guidelines of criteria 4 (in blue).
- III. Provide a list of 5 Ph.D. graduates in IA/CD in the last 5 years, with their dissertation title and abstract or a link to the dissertation.
- IV. Provide links to at least 3 faculty members whose area of expertise is Information Assurance/Cyber Defense. Provide CV or biography.
- V. Provide a narrative listing of any improvements or changes to the program since last designation, up to 5 years. Include information on expanded partnering, the number of Ph.D. students enrolled, major new grants for IA/CD research, and any impacts on IA/CD within your university.

2014 NSA/DHS National CAE IA/CD Criteria

- VI. Graduate/research programs must demonstrate that students have received adequate subject matter preparation. Explain how your graduate level research students have met this requirement either at your university or as a transfer from another university. The requisite subject matter must encompass the Information Assurance/Cyber Defense field or demonstrate relevance to the field (see criteria 4). Evidence can include verification of transcripts (actual transcripts not required for PII reasons – or if submitted, remove names and PI information), topics and numbers of students conducting IA/CD research, written verification from a department leader attesting to how the students received the knowledge, etc.