CAE-R Designation Criteria

Executive Summary

In 2008, the National Security Agency (NSA) established the Center of Academic Excellence in Cybersecurity-Research (CAE-R) program. The purpose of the program is to support and further build the cadre of experts to address new challenges resulting from the onslaught of ever-evolving cyberattacks, as well as to allow the government to engage CAE-R experts to solve the most challenging cybersecurity problems confronting our nation. From an initial 23 institutions, the program has grown to more than eighty CAE-R designated institutions today.

Given the everchanging nature of cybersecurity, it is important to conduct periodic self-evaluations to maintain and improve the excellence of the CAE-R program. This is necessary to further its recognition and respect from the general public, especially from the cybersecurity research community in government, industry and academia. To this end, the CAE-R designation criteria have been reviewed and updated to emphasize high standards and rigor, as well as to support a straightforward and well-defined review process based on objective measures. It is expected that high standards will encourage new and existing CAE-R institutions to respond with programmatic growth and improvements.

The primary objectives of the CAE-R program are:

- Recognize institutions with programs that integrate cybersecurity research activities into their doctoral curricula.
- Provide NSA, its partner agencies and the larger federal community with insight into academic doctoral cybersecurity programs (with their reach into industry) that can support advanced research and development capabilities.
- Serve as potential source and facilitator for government-academia exchanges of cybersecurity research personnel.
- Present opportunities to institutions to pursue much needed solutions for securing the country's critical information systems and networks.

Using longstanding attributes for assessing academic excellence in research scholarship, the necessary requirements to achieve distinction as a CAE-R institution are identified as follows:

- Nationally recognized rating as a research institution. (Carnegie Classification of Institutions of Higher Education or justification.)
- One or more doctoral programs which allow a research focus in cybersecurity.
- Faculty engaged in cybersecurity research.
- Peer-reviewed cybersecurity-focused publications and patents by faculty and students.
- Competitive external research funding in cybersecurity.
- Students engaged in cybersecurity research.
- Institutional support of cybersecurity research.

- Faculty involvement in service to the cybersecurity research community.
- For re-designation, involvement in the CAE-R community.

These requirements are further detailed below. All must be met for an institution to achieve the CAE-R designation from the NSA. The burden is on the institution to provide clear and concise evidence for each requirement as part of the application.

CAE-R Program Requirements

0. Letter of Intent

Provide a letter of intent and endorsement to participate in the CAE-R program (in PDF, do not mail), written on official institution letterhead, signed by the Provost or higher and addressed to:

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

This letter should:

a) Identify regional accreditation information.
b) State the institution's classification according to the Carnegie Classification of Institutions of Higher Education.
c) Identify the CAE-R Point of Contact (POC) from the institution.
d) List the doctoral programs supporting the requested designation.
e) Pledge of commitment to the minimum participation expectations of a CAE-R as listed below:
    i. Excellence in research in cybersecurity.
    ii. Submission of an annual report with all required information.
    iii. Attendance at either (or both) the CAE Principal's Meeting and CAE Community Symposium.
    iv. Regular communication with the CAE Program Management Office (PMO), including responding to email.
    v. Participation in the CAE-R community.
    vi. Ethical behavior of all faculty, students and staff in their cybersecurity research and activities. Provide evidence that measures are in place to adjudicate any ethical issues as they arise.

1. Research Classification

The Carnegie Classification of Institutions of Higher Education provides a neutral assessment of research institutions. (For definitions, see https://carnegieclassifications.iu.edu/classification_descriptions/basic.php.)

a) Applicants are expected to have R1 or R2 status.
b) Doctoral and Professional (D/P) institutions may be considered.
c) Weighted values will be assigned to R1, R2 and D/P institutions.
d) Institutions without Carnegie Classification may provide reasons and evidence to indicate the strength of their doctoral cybersecurity programs.

2. Academic Programs

A CAE-R institution must offer doctoral degree programs which allow a research focus in cybersecurity. Multiple programs from multiple departments may be included. These doctoral programs will be the main focus of the evaluation. All questions must be answered separately for each program. Provide the following:

a) Degree Name. For example, Ph.D./Doctorate in Computer Science, Cybersecurity, Electrical Engineering, Political Science, Management, Juris Doctor, etc.
b) Program Requirements. Describe the major milestones towards graduation, such as
   i. Qualifying Exam or equivalent. Describe how it is conducted. For example, the exam could be a written or oral exam; or equivalently, might involve passing a set of required courses. If the latter, include course names and syllabi.
   ii. Dissertation Committee. Describe the required minimum composition.
   iii. Comprehensive Exam or equivalent. Describe the purpose of the exam, how it may be related to the dissertation proposal, and how it is conducted.
   iv. Dissertation Defense. Describe how it is conducted.
   v. Impartiality. Describe how impartiality is ensured throughout the doctoral program. For example, the qualifying exam is written by a departmental doctoral committee (not the candidate's dissertation committee).
   vi. Other program requirements if any, describe in detail. For example, an annual departmental review of all doctoral students is conducted, the presence of an observer external to the candidate's academic unit for the dissertation defense, etc.
   vii. Provide links to or upload PDFs of the material documenting and supporting these requirements.
c) Broad Knowledge in Cybersecurity. Describe how the program requires comprehensive opportunities throughout a student's doctoral studies, to ensure that each student is exposed to a broad range of cybersecurity concepts. A program must satisfy at least 4 from the following items.
   i. Cybersecurity courses. (Include syllabi.)
   ii. A cybersecurity reading list. (Provide a copy of the reading list and a description of how completion of the readings is evaluated.)
   iii. Practical experience in cybersecurity, for example experiential learning, internships, externships, etc. (Provide examples and evidence.)
   iv. Teaching or serving as a teaching assistant in a general cybersecurity course (include syllabus).
   v. Regular attendance in seminars; conference attendance; workshops; etc. (All these items must refer to cybersecurity focused topics. Provide evidence.)
   vi. Other (provide details and justification, at most one description will be accepted)
d) Assessment. Describe the process(es) used to assess the doctoral program internally or externally.

Note: The subsequent requirements are to be met, in combination, by all doctoral programs included above.

3. Faculty

Faculty are the backbone of any strong doctoral program working on state-of-the-art research. Each applicant must provide the following information.

a) Faculty Capacity.
   i. A list of all full time tenured or tenured track (T/TT) faculty (indicating their tenure status and rank as full, associate or assistant professor) who are teaching courses and conducting research in cybersecurity (a minimum of 3 members is required). For institutions where tenure is not granted, describe how equivalence to the T/TT system is achieved.
   ii. A list of all full time research or adjunct faculty members (or equivalent) who are conducting cybersecurity research at the institution.
   iii. A total of at least 5 personnel, including a minimum of 3 T/TT faculty, conducting cybersecurity research is required.

b) Faculty Expertise.
   i. For each person named above in 3.a), a biographical sketch must be included. Every biographical sketch should be no more than 4 pages long. A template for the biographical sketch is included in Appendix A.
   ii. For each person named above in 3.a), specify his/her subject expertise from the list below.
      A. System security
         - Operating system
         - Web security
         - Mobile systems security
         - Distributed systems security
         - Cloud computing security
      B. Network security
         - Intrusion and anomaly detection and prevention
         - Network infrastructure security
         - Denial-of-service attacks and countermeasures
         - Wireless security
         - Authentication, access control and authorization
      C. Security Analysis
         - Cybersecurity threats and threat models
         - Malware analysis
         - Analysis of network and security protocols
         - Attacks with novel insight, techniques or results
         - Forensics and diagnosis for security
         - Covert and side channel analysis
         - Security analysis of source code and binaries
         - Program analysis
         - Formal methods and verification
      D. Hardware security
         - Secure computer architectures
         - Security analysis of hardware designs and implementation

- Methods for detection of malicious or counterfeit hardware
- Embedded system security

E. Cryptography
- New cryptographic approaches
- Analysis of deployed cryptography and cryptographic protocols
- Cryptographic implementation analysis
- New cryptographic protocols with real-world applications

F. Privacy and Anonymity
- Privacy-enhancing technologies and anonymity
- Usable security and privacy

G. Machine learning security and privacy

H. Data driven security and measurement studies
- Measurements of fraud, malware, spam
- Measurements of human behavior and security
- Metrics
- Policies

I. Social issues and security
- Research on computer security law and policy
- Ethics of computer security research
- Human factors in cybersecurity
- User perceptions and understanding of cybersecurity
- Research on security education
- Information manipulation, misinformation and disinformation
- Protecting and understanding at-risk users
- Emerging threats, harassment, extremism and online abuse
- Economics of security and privacy

J. Cybersecurity Management
- Organizational cybersecurity
- Cybersecurity governance, strategy and policy
- Managing cybersecurity
- Cybersecurity regulations, standards and compliance
- Cybersecurity in business process assurance, continuity, and resilience
- Risk management
- Organizational protection and security assurance

K. Other (describe)

4. Publications

Peer reviewed publications and patents reflect relevance of faculty research accomplishments. Only such products related to cybersecurity published within the last 5 years will be considered. Accepted or pending products can be included if proper documentation can be provided. PDFs or links to the publications should be provided where possible.

a) For at least 5 personnel in 3.a) including a minimum of 3 T/TT faculty members, list at least 3 products each. Highlight faculty and student authors from the institution.
b) Products listed in 4.a) should be arranged according to the subject expertise areas as defined in 3.b).

5. Funding

To enable research, sufficient financial resources are necessary to cover faculty time, support of (doctoral) students, and purchase supplies or equipment. Unlike internal support, competitive externally funded research grants by national funding agencies such as NSF, DARPA, IARPA, DoD, DHS, or DOE and/or prestigious industrial research awards from Microsoft, Intel, Google, IBM, etc. are indicators of research excellence. Applicants should provide the following:

For each faculty in 3.a), provide a history of funding as described above for the past 5 years, together with all the pending research funding at the time of this submission.

a) Funding Portfolio. Within the last 5 years, the portfolio should show a diversity of competitive external research grants. The minimum requirements are as follows:
    i. At least 3 active grants per year for the last 5 years involving faculty in 3.a),
    ii. At least 3 grants within the last 5 years corresponding to 3 different projects, and
    iii. At least 3 different faculty in 3.a) with active grants within the last 5 years.
b) Future Funding. For the year following the date of this application, demonstrate that there is at least one active grant involving some faculty in 3.a).
c) Grant Details. For each grant, provide the project title, funding source, and years covered.
d) Supporting Documentations. Links to the specific award on the funding source website (for example, such as those found on the NSF website) should be provided when possible. If links are not available, the list in c). should be signed by the dean of the college and/or director or the dean of the institution's research management office.

6. Students

Graduating doctoral students on a regular and continuing basis and the successful publication of student research results is another indicator of research excellence.

a) Doctoral Students in the Last 5 Years. Only report on students who worked or are working on research in topic areas such as those listed in 3.b).
    i. Provide doctoral enrollment number across all cybersecurity-related programs named in 2.a) for the past five years. On average, there should be at least 4 doctoral students per year conducting cybersecurity research throughout the five years.
    ii. For each current student, list the name, faculty advisor, research area, status, number of publications, expected date of graduation, and funding source (for example, grants, industry support, funding by the institution, teaching assistantships, self).
    iii. It is expected that at least 3 of the current doctoral students will graduate within the next 5 years.

iv. Provide evidence that funding for all current doctoral students is in place through the coming year via research grants, teaching assistantships, industrial support, institution and/or other resources.

b) Relevant Student Products.
Provide PDFs or links to a minimum of five distinct cybersecurity research products such as papers/software/datasets and other research artifacts produced within the last five years as a result of work by doctoral and/or master-level students. The links should allow access to the referenced products. Do not duplicate products already appearing in 4.a).

c) Recent Graduates.
   i. Show that at least 3 students graduated with a doctoral degree within the last five years with a dissertation topic focused on cybersecurity.
   ii. Provide information regarding the number of doctoral and master-level graduates who have completed a cybersecurity-focused thesis/dissertation (including thesis/dissertation title, author name, date, research area and link to thesis/dissertation documents or PDFs) in the past 5 years.
   iii. If possible, provide information on the first job placement for recent doctoral graduates.

7. Institutional Support

Cybersecurity research is strengthened when the institution supports its pursuit. The institution must provide evidence that it supports research excellence in cybersecurity. Describe how it is implemented at the institution. Of the items below, an institution must satisfy a) and at least one of b), c) and d).

a) Identify operational, and active entities (for example laboratories/centers) that focus on research in cybersecurity. (Provide links to these entities.)
b) List research seminars and/or colloquium talks by cybersecurity professionals, both from within and outside of the institution. (Provide evidence.)
c) Describe activities such as hosting of research conferences, workshops and/or other similar events at the institution. (Provide evidence.)
d) Describe other institutional support.

8. External Professional Service in Cybersecurity

Across the institution, faculty are actively involved in external professional activities in cybersecurity. Specifically, an institution must demonstrate that

a) at least two of the three T/TT faculty members listed in 3.a) are actively involved in at least one professional external service in cybersecurity per year, and
b) a total of at least 6 cybersecurity service activities across the institution within the past 5 years. Examples of activities include:
   i. Serving on technical program committees of cybersecurity related research conferences.
   ii. Serving on proposal review panels for funding agencies.
   iii. Reviewing cybersecurity papers for peer reviewed publications.

iv. Serving on the editorial boards of professional cyber security related publications.
v. Giving cybersecurity related invited colloquium talks and/or keynote speeches.

Documentation for these activities must be provided wherever possible.

9. CAE-R Community Involvement

This criterion applies only to re-designating institutions.

Across the institution, its personnel listed in 3.a) should be actively involved in the activities of the CAE-R community.

An institution applying for re-designation must have completed within the last 5 years at least 4 activities in at least 2 different categories a) – f) given below.

a) Reviewing CAE-R applications.
b) Giving and/or participating in CAE Forum and/or Tech talks.
c) Reviewing CAE-R grant applications.
d) Serving in an advisory capacity as a research/subject matter expert resource for the government in matters of cybersecurity.
e) Providing guidance and advice to (NCAE) institutions that aspire to become CAE-R institutions.
f) Other (provide details)

Documentation for these activities must be provided.

Appendix A

CAE-R Faculty Resume Template
(no more than 4 pages)

Current Position
Address
Contact Information

Professional Preparation

Appointment History (minimum last 8-10 years)

Cybersecurity Research Interests

Five Recent Publications in Cybersecurity (use standard publication reference format such as that of IEEE or ACM)

Five Other Significant Publications (use standard publication reference format)

Synergistic Activities (give priority to cybersecurity, see examples below)
- Chair, Member of Technical Program Committee
- Invited Colloquium/Workshop Talks, Panel Discussions, Keynote Speaker, etc.
- Reviewer (for journals, grants, and others.)
- Editorial Board, Board of Directors, etc.
- Other Activities, both Educational and Research

Grants and Awards (last 5 years)

Doctoral Students (last 5 years)

Other Relevant Information (for example, mentoring postdoc fellows, masters students, etc.)

Appendix B

CAE-R Evaluation Criteria

An institution will achieve the CAE-R designation if all criteria are met and the sum of 1. and 2.b) is at least 4.

0. **Letter of Intent**

a) Accreditation Met _____Not Met _____
b) Carnegie Classification Met _____Not Met _____
c) POC from the institution Met _____Not Met _____
d) List of doctoral programs supporting the designation Met _____Not Met _____
e) Pledge of commitment to Met _____Not Met _____
   i. Excellence in research Met ____Not Met _____
   ii. Annual Report Submission Met ____Not Met _____
   iii. Attendance at Community Symposium and/or CAE-R Principals meeting Met ____Not Met _____
   iv. Regular communication with the CAE program office Met ____Not Met _____
   v. Participation in CAE-R community Met ____Not Met _____
   vi. Ongoing ethical behavior by all faculty, staff and students and existence of adjudication measures for violations Met ____Not Met _____

Items a), b), c), d) and e) Met_____Not Met _____

Comments _____

1. **Research Classification** (This criterion is met if it is above 0.)
   a) R1 (score=3)
   b) R2 (score=2)
   c) D/P (score=1)

Score _____

Comments_____

_____

2. **Academic Program** (This criterion is met if items a), c) and d) are met and Item b) is above 0.)
   a) Degree Names Met _____Not Met _____
   b) Program Requirements for each program
      score =0; >=2 items from (i)-(v) are not met.
      score =1; one item from (i)-(v) is not met.
      score =2; all of items from (i)-(v) are met.
      score =3; other elements that add rigor and/or oversight to the doctoral program outside of items in (i)-(v). For example, external PhD evaluator on dissertation committee.
      Final score = average of scores of all programs (rounded to integer value).
      Score _____
   c) Broad Knowledge in Cybersecurity Met _____Not Met _____
   d) Assessment Met _____Not Met _____

Items a), c) and d) **Met _____Not Met _____**
Score _____

Comments_____

_____

3. **Faculty** (This criterion is met if all its sub-elements are met.)
   a) Faculty capacity
      T/TT or equivalent (>=3) Met _____Not Met _____
      Total (>=5) Met _____Not Met _____
   b) Faculty expertise
      Biographical Sketch Met _____Not Met _____
      Listed according to subject areas Met _____Not Met _____

Items a) and b) **Met _____Not Met_____**

Comments_____

_____

4. **Publications** (This criterion is met if all its sub-elements are met.)
   a) At least 3 products each for at least 5 personnel in 3.a) including a minimum of 3 T/TT faculty Met _____Not Met _____
   b) Arranged according to subject areas Met _____Not Met _____

Items a) and b) **Met _____Not Met_____**

Comments_____

_____

5. **Funding** (This criterion is met if all its sub-elements are met.)
   a) Funding Portfolio Met _____Not Met _____
      i. At least 3 active grants per year involving faculty in 3.a) Met _____Not Met _____
      ii. At least 3 different funded projects within the last 5 years
      Met _____Not Met _____
      iii. At least 3 different people in 3.a) have active grants within the last 5 years
      Met _____Not Met _____
   b) For the year following the date of submission, there is at least one active grant involving faculty in 3.a) Met _____Not Met _____
   c) Grant details provided Met _____Not Met _____
   d) Links and/or signed document from institution authority are included
      Met _____Not Met _____

Items a), b), c) and d) **Met _____Not Met_____**

Comments_____

_____

6. **Students** (This criterion is met if all its sub-elements are met.)
   a) Doctoral Students in the Last 5 Years Met _____Not Met _____
      i. Average of at least 4 students per year Met _____Not Met _____
      ii. Student details provided Met _____Not Met _____
      iii. At least 3 current students graduating in next 5 years Met _____Not Met _____

iv. Funding for all current doctoral students is in place through the coming year
Met _____Not Met _____

b) Show relevant student products such as papers/software/datasets and other artifacts
Met _____Not Met _____

c) Recent Graduates Met _____Not Met _____

i. Within the last five year, at least 3 students graduated with a doctoral degree with dissertation topic focused on cybersecurity Met _____Not Met _____

ii. Information on recent graduates Met _____Not Met _____

Items a), b) and c) Met _____Not Met_____

Comments_____

_____

7. **Institutional Support** (This criterion is met if items a) and at least one of b), c), and d) are met.)

a) Cybersecurity entities Met _____Not Met _____

b) Seminars, other support Met _____Not Met _____

c) Hosting research conferences/workshops Met _____Not Met _____

d) Other institutional support Met _____Not Met _____

Items a) and at least one of b), c) and d) Met _____Not Met_____

Comments_____

_____

8. **External Professional Service in Cybersecurity** (This criterion is met if all its sub-elements are met.)

a) >=2 T/TT faculty with >=1 service activity per year Met _____Not Met _____

b) >=6 activities across the institution during the past 5 years
Met _____Not Met _____

Items a) and b) Met _____Not Met_____

Comments_____

_____

9. **Re-designation only**

CAE-R Community Involvement (This criterion is met if all its sub-elements are met.)

At least 4 activities in at least 2 different categories within last 5 years
Met _____Not Met _____

Comments_____

_____

SUMMARY

Criteria 0, 2 a), 2.c), 2.d), 3, 4, 5, 6, 7, 8, 9 Met _____Not Met_____

Score Sum of Criteria 1 and 2.b) Score_____