



2022 CAE Symposium

Proposed Revised NCAE-R (Re-)Designation Criteria

Agnes Chan

Northeastern University

Cynthia Irvine

Naval Postgraduate School

Susanne Wetzel

Stevens Institute of Technology

9 June 2022



- ▶ 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 sources and facilitators 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.

Revision emphasizes

- ▶ High standards and rigor.
- ▶ Support a straightforward and well-defined review process that is based on objective measures.



- ▶ Nationally recognized rating as a research institution (Carnegie Classification of Institutions of Higher Education or justification).
- ▶ One or more doctoral programs that allow a research focus in cybersecurity.
- ▶ Faculty engaged in cybersecurity research.
- ▶ Peer-reviewed cybersecurity-focused publications, patents, and other significant research products 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 Community of Practice in Research (CoP-R).



Section I Requirements



Institutions without Carnegie Classification may provide reasons and evidence for equivalence.

- ▶ R1: Doctoral Universities – **score = 2**
- ▶ R2: Doctoral Universities – **score = 2**
- ▶ D/PU: Doctoral/Professional Universities – **score = 1**
- ▶ No Carnegie Classification (Justification required) – **score range = 0 to 2**

C2. Academic Program(s) - Overview



- ▶ Must offer doctoral program(s) that allow research focus in cybersecurity
- ▶ Multiple programs from multiple departments may be included
- ▶ In aggregate, doctoral programs submitted in C2 must meet Section II requirements.
- ▶ All requirements for criterion C2 must be submitted per program.

C2. Academic Program(s) - Requirements



For each program, supply

- a) Degree name (link to catalog or website)
- b) Doctoral Program Elements
 1. Describe the milestones towards graduation
 2. Provide PDF of or link to the graduate handbook describing
 - i. Qualifying Exam or equivalent
 - ii. Dissertation Committee - minimum composition
 - iii. Comprehensive Exam or equivalent
 - iv. Dissertation Defense - how conducted
 - v. How impartiality is ensured
 - vi. Other program requirements



c) Broad Knowledge in Cybersecurity

- ▶ Describe how the program provides comprehensive opportunities throughout a student's doctoral studies, so that each student is exposed to a broad range of cybersecurity concepts.
- ▶ This requirement can be satisfied by providing a list of cybersecurity courses that students must complete (include syllabi), or by providing a description of how the program affords opportunities to students. Examples include
 - (a) Cybersecurity reading list
 - (b) Practical experience in cybersecurity
 - (c) Teaching or serving as a teaching assistant in a cybersecurity course
 - (d) Regular attendance in seminars; conference attendance; workshops; etc.

c) Assessment

- ▶ Describe the process(es) used to assess the doctoral program internally or externally.

C2. Academic Program(s) - Scoring



Institutions are scored on milestones, processes and procedures 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.

Overall score for C2 determined as average of all program scores.



Section I is met if

- ▶ C2.a, C2.c, and C2.d are met for each submitted program and
- ▶ the sum of the C1 score and the C2 score is at least 4.



Section II Requirements

C3. Institutional Commitment: a) Commitment Letter



Letter of intent signed by Provost or higher and the letter should

1. Identify regional accreditation information. Include the name of the accrediting body, date of the most recent accreditation, and date of the next re-accreditation.
2. State institution's classification according to the Carnegie Classification of Institutions of Higher Education.
3. Identify CAE-R Point of Contact from the institution
4. List doctoral program(s) supporting supporting the requested designation.
5. Pledge of commitment to the minimum participation expectations of a CAE-R
 - i. Excellence in research in cybersecurity.
 - ii. Submission of a CAE-R annual report with all required information.
 - iii. Attendance at CAE Principal's Meeting and/or CAE Community Symposium.
 - iv. Regular communication with NCAE-C Program Management Office, including responding to email.
 - v. Participation in CAE Community of Practice in Cyber Research (CoP-R).
 - vi. Ethical behavior of all faculty members, students, and staff in their cybersecurity research and activities.

C4. Faculty Members: a) Faculty Capacity



- a) Faculty Capacity: A total of at least five personnel, including a minimum of three T/TT faculty, conducting cybersecurity research is required.
1. A list of all full-time tenured or tenured track (T/TT) faculty members (indicating their tenure status and rank as full, associate or assistant professor) who are teaching courses and conducting research in cybersecurity (a minimum of three faculty members is required). For institutions where tenure is not granted, describe how equivalence to the T/TT system is achieved.
 2. A list of all other full-time faculty (or equivalent) not listed in C4.a.i above, who are currently conducting cybersecurity research at the institution (indicating their position and title).



b) Faculty Expertise

1. For at most 15 faculty members named above in C4.a, including a minimum three T/TT faculty members, a biographical sketch must be included. Every biographical sketch should be no more than our pages long.
 - ▶ Guidelines are provided
2. Provide the summary table of Research Subject Areas for all faculty members
 - ▶ A list of expertise areas is provided in the criteria



Peer reviewed publications, patents and other research products reflect the relevance of faculty members' research accomplishments.

- a) Provide the summary table of Research Products for Faculty Members.
 - ▶ For at least five personnel in C4.a, including a minimum of three T/TT faculty members, list at least three products each.
 - ▶ This list must include at least 15 distinct products.
 - ▶ Highlight faculty members and student authors from the institution.
 - ▶ For significant products, such as major software components, datasets, and test beds, a justification must be included.
 - ▶ For each person, at least two products must be peer-reviewed.
- * Product citations should be provided using standard publication reference format.
- * The criteria describe how to provide evidence using templates and examples

C5. Cybersecurity-Related Research Products - Example



| C5 - Summary Table of CAE-R Research Products for Faculty Members | | | | | | | | | | | | | | | | | | | | | |
|---|---|--|---|------------------------------|---------------------|----------------------|----------------------|-----------------|--------------------------|-----------------------------|-------------------------------|-----------------------------|----------------------------------|----------|--|--|--|--|--|--|---|
| Product No. | Faculty member (Duplicate names for multiple products): | Product citation (use standard publication reference format such as that of IEEE, ACM, or APA) | Digital Object Identifier (DOI) (if available) | CAE-R Research Subject Areas | | | | | | | | | | | | | | | | | |
| | | | | A. SYSTEM SECURITY | B. NETWORK SECURITY | C. SECURITY ANALYSIS | D. HARDWARE SECURITY | E. CRYPTOGRAPHY | F. PRIVACY AND ANONYMITY | G. DATA DRIVEN SECURITY AND | H. SOCIAL ISSUES AND SECURITY | I. CYBERSECURITY MANAGEMENT | J. MACHINE LEARNING SECURITY AND | K. OTHER | | | | | | | |
| 1 | Jane Doe, Ph.D. | Russ, M., Doe, J., & Chen, A. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | X | | | | | | | | | | | | | | X |
| 2 | Jane Doe, Ph.D. | Doe, J., & Butler, W. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | X | | | | X | | | | | | | | | | | | | |
| 3 | Jane Doe, Ph.D. | Tejay, G., Goel, S., & Doe, J. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | X | X | | | | | | | | | | | | | |
| 4 | Alice McCumber, Ph.D. | McCumber, A. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | X | | | X | | | | | | | | | | | | | |
| 5 | Alice McCumber, Ph.D. | Xu, H., & McCumber, A. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | X | | | | | X | | | | | | | | | | |
| 6 | John Abbot, Ph.D. | Abbot, J. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | | | | | | | | | | | | | | | |
| 7 | Wei Li, Ph.D. | Li, W., & Zeichick, D. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | | | | | | | | | | | | | | | |
| 8 | Wei Li, Ph.D. | Robertson, T., Lee, B., & Li, W. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | X | | | | | | | | | | | | | | | | X |
| 9 | Sandra Blanke, Ph.D. | Blanke, S., & Bliss, G. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | X | | | | | | | | | | | | | | X |
| 10 | Sandra Blanke, Ph.D. | Konkey, A., Kepner, J., & Blanke, S. (year). Title. <i>Journal, Vol (Iss)</i> , pp-pp. | https://doi.org/... | | | | | | | X | | | | | | | | | | | X |
| ... | ... | ... | ... | | | | | | | X | | | | | | | | | | | |



a) Funding Portfolio: For each faculty member in C4.a, provide a history of cybersecurity-related research funding as described above for the past five years, together with all the pending research funding at the time of this submission. Within the last five years, the portfolio should show a diversity of competitive external research grants. The minimum requirements are as follows:

1. At least three active grants per year for the last five years involving faculty members in C4.a;
2. At least three grants within the last five years corresponding to three different projects; and
3. At least three different faculty in C4.a. with active grants within the last five years.

For each grant, provide the project title, funding source, and years covered. The criteria describe how to provide evidence.



b) Future Funding: For the year following the date of this application, demonstrate that there is already, or a documented firm commitment for, at least one active grant involving some faculty members listed in C4.a.



a) Doctoral Students in the Last Five Years:

1. Provide doctoral enrollment number (unduplicated headcount) across all cybersecurity-related programs submitted in C2.a for the past five years. On average, there should be at least four doctoral students per year conducting cybersecurity research throughout the five years
2. 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).
3. Describe the progress of at least three current doctoral students and show how they can be expected to graduate within the next five years
4. Provide evidence that funding opportunities are available for all current doctoral students through the coming year via research grants, teaching assistantships, industrial support, institution and/or other resources.



b) Published Student Products

- ▶ Provide PDFs or links to a minimum of five distinct cybersecurity peer-reviewed papers or patents.
- ▶ For significant products, such as major software components, datasets, and test beds, a justification must be included.
- ▶ Only include products published within the last five years that resulted from work by doctoral and/or master-level students.
- ▶ Links should allow access to the referenced products.
- ▶ Do not duplicate products already appearing in C5.a.



c) Recent Graduates

1. Provide a list of at least three students graduated with a doctoral degree within the last five years with a dissertation topic focused on cybersecurity.
2. Provide information regarding the number of doctoral and master-level graduates who have completed a cybersecurity-focused thesis/dissertation in the past five years.
 - ▶ If possible, provide information on first job placement for recent doctoral graduates.



- a) Active entities: Identify operational, and active entities (for example laboratories/centers) that focus on research in cybersecurity.
- b) Support: At least one of the following three:
 1. Event Support: List research seminars and/or colloquium talks by cybersecurity professionals, both from within and outside of the institution.
 2. Event Housing: Describe activities such as hosting research conferences, workshops and/or other events at the institution.
 3. Other Support: Describe other institutional support.



a) Faculty Members' External Professional Service

- ▶ At least two of the three T/TT faculty members listed in C4.a are actively involved in at least one professional external service in cybersecurity per year.

b) Faculty Members' Cybersecurity Scholarly Service

- ▶ Serving as a cybersecurity subject matter expert on the technical program committees of conferences where cybersecurity-related research papers are presented.
- ▶ Serving on review panels of cybersecurity-related proposals for funding agencies.
- ▶ Reviewing cybersecurity papers for peer reviewed publications.
- ▶ Serving on the editorial boards of professional cybersecurity-related publications.
- ▶ Giving cybersecurity-related invited colloquium talks and/or keynote speeches.



Requirement for Redesignating Institutions only:

- a) A CAE-R institution must have participated in at least three different CAE-R Community of Practice in Cyber Research activities in at least two different categories within the last 5 years.

Categories of activities are:

1. Attendance at CAE-R Symposium and CAE-R meetings.
2. Participation in any working groups in the CAE CoP-R, including giving feedback and attending small group discussions.
3. Reviewing CAE-R redesignation applications
4. Giving and/or participating in CAE Tech talks
5. Reviewing CAE-R grant applications
6. Provide guidance and advice to NCAE institutions that aspire to become a CAE-R
7. Other CAE-R activities.

Documentation must be provided whenever possible.



Section II is met if all criteria C3 through C10 are met.



An institution will achieve the (re-)designation if

1. Section I and
2. Section II are met.



Community Involvement in Developing Revised Criteria



- ▶ August 2021: Soliciting feedback from a few PoCs on an initial draft.
- ▶ December 2021: Soliciting first round of feedback from all PoCs of current CAE-Rs in December through Google survey.
- ▶ February 2022: Focus group meetings.

Acknowledgements



Mike Burmester,
Florida State University

Ram Dantu,
University of North Texas

Jack Davidson,
University of Virginia

William Enck,
North Carolina State University

Hanan Hibshi,
Carnegie Mellon University

Paul Kealey,
University of Arizona

Karen Leuschner,
National Security Agency

Nasir Memon,
New York University

Guevara Noubir,
Northeastern University

Roberto Perdisci,
University of Georgia

Lori Pfannenstien,
National Security Agency

Craig Shue,
Worcester Polytechnic Institute

Michael Stiber,
University of Washington

Daniel Takabi,
Georgia State University

Patrick Tague,
Carnegie Mellon University

George Trawick,
Mississippi State University

Shambhu Upadhyaya,
SUNY Buffalo

Ping Yang,
Binghamton University (SUNY)

Birol Yesilada,
Portland State University

Yuliang Zheng,
University of Alabama at Birmingham



Submission/Review Process

(SUBJECT TO DISCUSSION & CHANGE)



- ▶ One application step — Program of study and criteria are integrated.
- ▶ Mentors - From institutions which currently hold NCAE-R designation.
- ▶ Pre-submission review - Recommendation by CoP-R to be merged with mentoring.
- ▶ Group of reviewers - From institutions which currently hold NCAE-R designation and government representatives chosen by PMO.
- ▶ Panel review with PoC for NCAE-R application.
- ▶ Panel recommendation to PMO - Final decision rests with PMO (as in case of other designations).



The End