National Centers of Academic Excellence in Cybersecurity

NCAE-C 2023

Proposed Designation Requirements and Application Process

For

CAE-Cyber Research (CAE-R)

January 2023

This publication was partially supported by the NCyTE Center at Whatcom Community College,
under NSA award number H98230-20-1-0294

OVERVIEW

The following is an overview of the requirements for designation in the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program for **Cyber Research (CAE-R)** Designation administered by the National Security Agency (NSA). Details on each requirement and application processes are provided in the body of this document. The goal of the NCAE-C program is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

NCAE-C Core Values and Guiding Principles Overview

- *The Ethical Behavior Core Value:* The academic institution must encourage and support ethical behavior by students, faculty, administrators, and professional staff.
- *The Share Core Value:* The institution enables an environment in which students, faculty, administrators, professional staff, and practitioners can share, interact, and collaborate with others in the cybersecurity field.
- *The Lead by Example Core Value:* The institution demonstrates a commitment to address, engage, and respond to current and emerging cybersecurity issues in the classroom, the institution itself, and outside the institution.

NCAE-C Program Objectives

The objectives of the NCAE-C Program include:

- Shared governance
- Maintain/improve NCAE-C Program standards
- Focus on output (workforce) in cybersecurity
- Rely on existing proven methods of regional accreditation
- Align with the NCAE-C Strategic Vision

The United States Government must support the development of cybersecurity skills and encourage ever-greater excellence so that America can maintain its competitive edge in cybersecurity. "Prepare, grow, and sustain a national cybersecurity workforce that safeguards and promotes America's national security and economic prosperity" (NIST, 2018, para. 5).

TABLE OF CONTENTS

CAE-R DESIGNATION ELIGIBILITY AND SUMMARY

In 2008, the National Security Agency (NSA) established the National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Cyber Research (CAE-R) program. The purpose of the CAE-R Designation 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 United States (U.S.) 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 80 CAE-R designated institutions today. Only U.S. academic institutions are eligible to apply to the NCAE-C program. Given the everchanging nature of cybersecurity, it is important to conduct periodic self-evaluations to maintain and improve the excellence of the CAE-R Designation. 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 Designation are:

- Recognize United States (U.S.) 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.
- Sustain and strengthen the research and education posture of the nation in cybersecurity.

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:

C1. **Research Classification:** Nationally recognized rating as a U.S. research institution (Carnegie Classification of Institutions of Higher Education or justification).

C2. **Institutional Commitment:** A commitment letter signed by the leadership of the academic institution documenting awareness of the expectations and responsibilities associated with the CAE-R Designation

C3. **Academic Program(s):** One or more doctoral programs that support a research focus in cybersecurity.

C4. **Faculty Members Capacity and Expertise:** Faculty engaged in cybersecurity research.

C5. **Cybersecurity-Related Research Products:** Peer-reviewed cybersecurity-focused research products by faculty members and students.

C6. **Cybersecurity-Related Research Funding:** External research funding in cybersecurity.

C7. **Students:** Students engaged in cybersecurity research.

C8. **Institutional Support for Cybersecurity-Related Research:** Institutional support of cybersecurity research.

C9. **External Professional and Scholarly Service in Cybersecurity-Related Research:** Faculty involvement in service to the cybersecurity research community.

C10. **NCAE-C Activities, CAE Community, and CAE Community of Practice in Cyber Research (CAE CoP-R):** For Re-Designation, involvement in the NCAE-C Activities, CAE Community, and CAE CoP-R.

There are 10 criteria, C1 through C10. These requirements are further detailed below. The requirements are divided into Section I and Section II, where C1 to C9 are in Section I, and C10 are in Section II (For re-designation only). All requirements in criteria C1 to C9 must be met for an institution to achieve the CAE-R Designation. For Re-Designating CAE-R institutions, criterion C10 must also be met. The burden is on the institution to provide clear and concise evidence for each requirement as part of the application. It is expected that, as the program matures, many of the materials required in the application will be accumulated and found in the institutional CAE-R annual reports.

Definitions

An ***institution*** is a U.S. legal entity authorized to award associate degrees or higher. All institutions applying to the NCAE-C program must be a U.S. institution of higher education and hold current regional accreditation as outlined by the U.S. Department of Education (https://www.ed.gov/accreditation).

An ***academic unit*** operates within an institution offering associate degrees or higher, and depends on the institution for authority to grant degrees and for financial, human, and physical resources.

An ***active entity*** refers to a center, laboratory, or an institute at the applying institution.

A ***requirement*** is a specific mandatory information needed for the application submission.

CAE-R DESIGNATION CRITERIA

Overview

A U.S. institution of higher education will achieve the CAE-R Designation if all requirements in criteria C1 to C9 (Section I) are met. For Re-Designating CAE-R institutions, criterion C10 must also be met. The table below provides an overview of the required criteria needed for CAE-R Designation. All data for CAE-R Designation will be stored in an online Application Tool provided by the NCAE-C PMO to improve accountability, where the history and purity of the data is documented.

Table 1. Summary of CAE-R Designation Required Criteria

Section I
C1. Research Classification: The institution must be a U.S. institution of higher education and is expected to have Carnegie Classification to hold a CAE-R designation.
C2. Institutional Commitment: A letter of intent and endorsement, signed by the Provost or higher, documenting that the institution is aware of the expectations and responsibilities associated with the CAE-R Designation including active entity (for example laboratory/center/institute) of cybersecurity research, identified CAE-R Point of Contact (POC), as well as acknowledging minimum participation expectations, including annual update of required metrics, attendance at annual events, and active participation in the NCAE-C Activities, CAE Community, and CAE Community of Practice in Cyber Research (CoP-R).
C3. Academic Program(s): The institution must offer one or more doctoral degree programs which allow a research focus in cybersecurity to hold a CAE-R designation.
C4. Faculty Members Capacity and Expertise: Faculty members are the backbone of any strong doctoral program working on state-of-the-art research. Each applicant institution shall demonstrate its strength through: (a) Faculty Capacity; and (b) Faculty Expertise in cybersecurity research.
C5. Cybersecurity-Related Research Products: Research products, such as peer-reviewed publications, patents, etc. reflect the relevance of faculty members' research accomplishments. Only such research products related to cybersecurity within the past five (5) years will be considered. Accepted or pending products can be included if proper documentation can be provided.
C6. Cybersecurity-Related Research Funding: The institution must provide evidence of faculty members engagement in externally funded research portfolio from agencies, industrial research, and/or foundation awards for the past five (5) years.
C7. Students: Applicant institutions shall demonstrate that it is graduating doctoral students on a regular and continuing basis. Applicant institutions shall also demonstrate the successful publication of students' research results as another indicator of research excellence.
C8. Institutional Support for Cybersecurity-Related Research: The institution must provide evidence of support to research excellence in cybersecurity.
C9. External Professional and Scholarly Service in Cybersecurity-Related Research: Applicant institutions must demonstrate how its faculty members are actively involved in external professional and scholarly activities in cybersecurity-related research.
Section II (For Re-Designating Institutions Only)
C10. Involvement in NCAE-C Activities, CAE Community, and CAE Community of Practice in Cyber Research (CAE CoP-R): Institutions applying for CAE-R Re-Designating must provide evidence that its faculty members are actively involved in the activities of the NCAE-C Activities, CAE Community, and CAE Community of Practice in Cyber Research (CoP-R).

Section I Criteria

This section pertains to the research status of the U.S. institution of higher education in accordance with the Carnegie Classification, considers academic programs of the institution that produces doctoral students with a focus in cybersecurity, as well as the quality of the faculty members engaged in the doctoral programs, and their cybersecurity related research. All criteria in Section I are evaluated based on the aggregate of all the doctoral programs applying for in Section C3.

C1. Research Classification

The Carnegie Classification of U.S. Institutions of Higher Education provides a neutral assessment of research institutions (For definitions, see https://carnegieclassifications.iu.edu/classification_descriptions/basic.php). Applicants must be a U.S. institution of higher education and are expected to have a Carnegie Classification. Institutions without Carnegie Classification must provide NSA's prior approval in the justification (in PDF).

Requirement:

a) **Carnegie Classification:** Indicate the Carnegie Classification level of the institution:

- R1: Doctoral Universities – Very high research activity
- R2: Doctoral Universities – High research activity
- D/PU: Doctoral/Professional Universities
- Other (NSA's prior approval to submit required in the justification)

Discussions and Rationale. Carnegie Classification is an indicator of the level of the research carried out across the institution.

C2. Institutional Commitment

The letter of intent and endorsement, signed by the Provost or Higher, demonstrating that the institution is aware of the expectations and responsibilities associated with the CAE-R Designation.

Requirements:

a) **Commitment Letter:** Provide a letter of intent and endorsement to participate in the NCAE-C program for CAE-R Designation (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 shall:

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 the institution's classification according to the Carnegie Classification of Institutions of Higher Education.
3. Identify the CAE-R Point of Contact (POC) from the institution.
4. List the doctoral program(s) supporting the requested designation.
5. Pledge of commitment to the minimum participation expectations of a CAE-R as listed below:
   i. Excellence in research in cybersecurity.
   ii. Submission of a CAE-R 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 NCAE-C Program Management Office (PMO), including responding to email.
   v. Participation in the 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.

Discussions and Rationale. The commitment letter reflects the appreciation of the applying institution on the obligations involved to be a CAE-R designated institution.

C3. Academic Program(s)

Each applicant institution must be offering a doctoral degree program that allows a research focus in cybersecurity and meets the requirements in Section I. Only graduates of the doctoral program(s) evaluated under C3 are recognized as CAE-R graduates of the institution. Multiple programs from multiple departments may be included. For more than one program, all requirements for this criterion must be submitted per program.

Requirements (All required for each program submitted):

a) **Degree Name:** State the official Degree Name as it appears in the institutional documentations (e.g. catalog and website). For example, Ph.D./Doctorate in Computer Science, Cybersecurity, Information Systems, Computer Engineering, Electrical Engineering, Management, Business Administration, Political Science, etc.

b) **Doctoral Program(s) Elements:**

1. Provide the graduate handbook (in PDF) for each program submitted to be evaluated and highlight the sections describing the following three (3) elements:

   i. A process for establishing the student's readiness to pursue the doctoral program (i.e. Qualifying Exam or equivalent),

   ii. A process for establishing the student's readiness to conduct research in cybersecurity (i.e. Comprehensive Exam or equivalent), and

   iii. A process for evaluating the student's research results (i.e. Dissertation Defense or equivalent).

2. The program must demonstrate how its processes achieve academic rigor and objectivity. Describe:

   i. How the faculty of the academic unit or a subcommittee thereof oversees the Qualifying Exam (or equivalent)?

   ii. How the program forms a Comprehensive Exam Committee (or equivalent) that includes at least three (3) full time faculty members holding doctoral degrees?

   iii. How the program forms a Dissertation Committee (or equivalent) that includes at least three (3) full time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program?

   iv. Any other requirements pertaining to rigor and objectivity, e.g., that the program conducts an annual program review of all doctoral students.

c) **Broad Knowledge in Cybersecurity:** Describe how the program provides ample opportunities throughout a student's doctoral studies so that each student is exposed to a broad range of current cybersecurity concepts. This requirement can be satisfied by providing evidence of doctoral program admissions requirements that the incoming doctoral students have broad knowledge in cybersecurity via prior degrees and/or work experience in cybersecurity. This requirement also 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 may include (but are not limited to): (a) A cybersecurity reading list (Provide a copy of the reading list and a description of how completion of the readings is evaluated); (b) Practical experience in cybersecurity, for example experiential learning, internships, externships, etc. (Provide examples); (c) Teaching or serving as a teaching assistant for a cybersecurity course (Provide evidence); (d) Attendance at seminars, conferences, workshops, etc. (Provide examples). All these items must refer to cybersecurity-focused topics per Table 2.

d) **Assessment:** Describe the process(es) used to assess the doctoral program internally or externally.

Discussion and Rationale.

Criterion C3 allows applicants to submit multiple doctoral programs for evaluation. It recognizes the fact that there are institutions where faculty who are actively engaged in cybersecurity research may be spread across multiple academic units producing doctoral students in the respective discipline. This criterion supports and encourages such multi-disciplinary approaches. Applicants should submit all doctoral programs for evaluation that are necessary to meet all criteria C4-C10 (i.e., on faculty and students anchored in these programs) in totality across all these programs.

With C3.a, the criterion ensures that all doctoral programs meet the minimum requirement of implementing the three main elements of a doctoral program. Ultimately, the individually scored C3.b in all programs listed in C3 are aggregated and assessed, thus allowing the high-quality processes of one program to balance evolving processes of another program. Applicants are asked to provide sufficient evidence to facilitate an objective assessment of the overall academic rigor of each doctoral program submitted.

It is important to note that C3.c does not mandate a particular approach to providing doctoral students with opportunities to establish a broad knowledge in cybersecurity. Instead, it only requires that the program offers one or more such options.

C4. Faculty Members Capacity and Expertise

Faculty members are the backbone of any strong doctoral program working on state-of-the-art research. For the CAE-R designation, an applicant institution must have a minimum of four (4) full-time faculty members conducting cybersecurity research and directly affiliated with the academic doctoral program (listed in C3). At least three (3) of those must be T/TT, or equivalent, faculty members, and at least two (2) of them must have cybersecurity related research as their primary research area.

Requirements: Only include faculty members who have produced at least one (1) research product in cybersecurity in the past five years. There shall be a total of at least four (4) full-time faculty members from C4.a and C4.b.

a) Provide a list of all full-time tenured (T), tenured track (TT), or equivalent, faculty members. For each faculty member in this list, provide the name, phone number, email address, highest degree earned, field and year, academic rank (e.g. Assistant Professor, Associate Professor, or Full Professor), tenure status (e.g. Tenure Track (TT), Tenured (T), or TT/T equivalent), Research Subject Areas (See Table 2), and years of academic experience. Provide a biographical sketch and a link to the faculty member's websites (wherever available). Every biographical sketch shall be no more than four (4) pages long. Guidelines for the biographical sketch are included in Appendix A. At least three (3) faculty members shall be in this list. For institutions where tenure is not granted, describe how equivalence to the T/TT system is achieved.

b) Provide a list of all other full-time faculty members not listed in C4.a above, who are currently conducting cybersecurity research at the institution. For each faculty member in this list, indicate: name, phone number, email address, highest degree earned, field and year, academic rank (Research Associate, Research Professor, Lecturer, Instructor, Teaching Assistant Professor, Professor of the Practice, etc.), Research Subject Areas (See Table 2), years of academic experience, and at least one (1) research product in cybersecurity in the past five years as defined in Criterion C5 below. For each faculty member, provide a biographical sketch and a link to the faculty member's websites (wherever available). Every biographical sketch shall be no more than four (4) pages long. Guidelines for the biographical sketch are included in Appendix A.

Example 1. Data on Faculty Members in C4

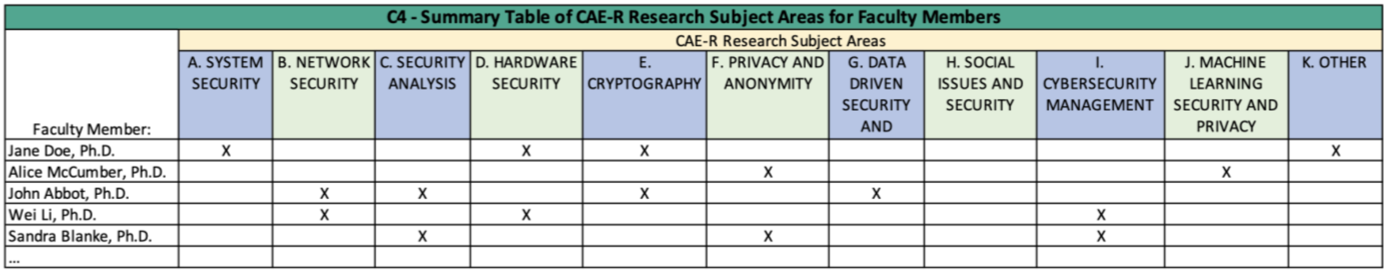
Name	Phone	Email	Highest Degree	Filed	Year	Academic Rank	Tenure Status (T, TT, NTT)	Years of academic experience	Research Subject Area	One research product
John Smith	Xxx	jsmith@xxx.edu	Ph.D.	Computer Science	1980	Full Professor	T	20	System Security	Russ,M, Smith,J, title,journal,vol(iss), pp

c) Provide the summary table of Research Subject Areas for all faculty members indicated in C4.a and C4.b (in PDF) (See the 'CAE-R C4 and C5 Summary Table Templates' spreadsheet provided, and Example 2). For each faculty member, specify their top-level subject expertise from the list found in Table 2 (viz., A-K). A list of example subtopics is included (See Table 2).

Table 2. Summary of CAE-R Research Subject Areas and Example List of Subtopics

A. SYSTEM SECURITY	**B. NETWORK SECURITY**	**C. SECURITY ANALYSIS**
• Operating system • Web security • Mobile systems security • Distributed systems security • Cloud computing security	• Intrusion and anomaly detection and prevention • Network infrastructure security • Denial-of-service attacks and countermeasures • Wireless security • Authentication, access control and authorization	• 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	**E. CRYPTOGRAPHY**	**F. PRIVACY AND ANONYMITY**
• Secure computer architectures • Security analysis of hardware designs and implementation • Methods for detection of malicious or counterfeit hardware • Embedded system security	• New cryptographic approaches • Analysis of deployed cryptography and cryptographic protocols • Cryptographic implementation analysis • New cryptographic protocols with real-world applications	• Privacy-enhancing technologies and anonymity • Usable security and privacy
G. DATA DRIVEN SECURITY AND MEASUREMENT STUDIES	**H. SOCIAL ISSUES AND SECURITY**	**I. CYBERSECURITY MANAGEMENT**
• Measurements of fraud, malware, spam • Measurements of human behavior and security • Metrics • Policies	• 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	• 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
J. MACHINE LEARNING SECURITY AND PRIVACY	**K. OTHER**	
	• Describe	

Example 2. An Example of a C4.d - Summary Table of CAE-R Research Subject Areas for All Faculty Members



C4 - Summary Table of CAE-R Research Subject Areas for Faculty Members

	CAE-R Research Subject Areas										
Faculty Member:	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 PRIVACY	K. OTHER
Jane Doe, Ph.D.	X			X	X						X
Alice McCumber, Ph.D.						X				X	
John Abbot, Ph.D.		X	X		X		X				
Wei Li, Ph.D.		X		X					X		
Sandra Blanke, Ph.D.			X			X			X		
...											

Discussion and Rationale. The requirement for at least three (3) T/TT faculty members conducting cybersecurity research ensures a critical mass for strong research activities. In the event that one of the three has left the institution, there will still be two T/TT faculty members conducting cybersecurity research and they constitute a sufficient strong basis upon which the institution may recruit a replacement for the lost faculty member.

Many teaching professors, lecturers and/or instructors conduct research although this may not be their primary responsibility. Such a faculty member can be included if s/he has at least one cybersecurity-related research product within the last five years.

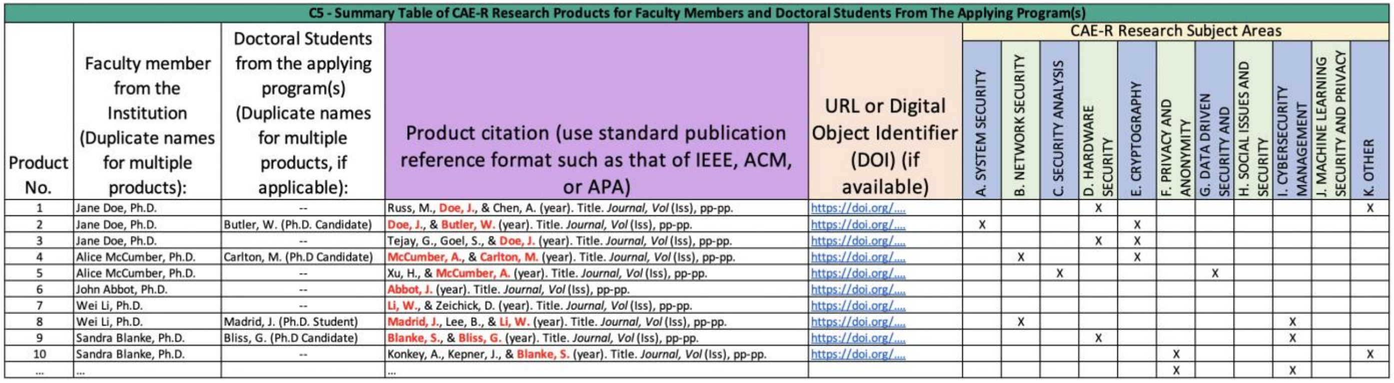
C5. Cybersecurity-Related Research Products

Research products such as peer-reviewed publications and patents are examples of faculty members' and doctoral students' research accomplishments. For the purpose of this CAE-R designation, applicant institutions who wish to claim cybersecurity-related research products such as major software components, datasets, and test beds, must provide a justification. Products related to cybersecurity published only within the past five (5) years will be applicable. Accepted or pending research products can be included if proper documentation can be provided. PDFs or links to the cybersecurity-related research products should be provided where possible. Note, the cybersecurity-related research product(s) are associated with the faculty members not institutions. Example: a cybersecurity-related peer-reviewed paper published by a faculty member two (2) years ago while they were at a different institution is applicable for this criterion.

Requirements

a) **Cybersecurity-Related Research Products:** Provide the summary table of at least twelve (12) distinct cybersecurity-related research products that involve at least three (3) T/TT faculty members noted in C4.a. Research Products submitted shall follow the template provided (See the *'CAE-R C4 and C5 Summary Table Template'* spreadsheet provided, and Example 3). Highlight faculty members and student authors from the institution. For the last five (5) years, at least four (4) faculty members listed in C4 (at least three (3) of them are T/TT faculty members) must have at least three (3) distinct research products each. At least two (2) of the three (3) distinct research products must be peer-reviewed. Products listed shall be arranged according to the top-level (viz., A-K) subject expertise areas as defined in Table 2. Citations of the products shall be provided following standard publication reference format such as that of IEEE, ACM, or APA and include a link (Uniform Resource Locator (URL)), or if available, a Digital Object Identifier (DOI) (https://doi.org/) should be included.

Example 3. An Example of a C5.a. - Summary Table of Cybersecurity-Related Research Products for Faculty Members and Doctoral Students of the Applying Program(s)



C5 - Summary Table of CAE-R Research Products for Faculty Members and Doctoral Students From The Applying Program(s)

Product No.	Faculty member from the Institution (Duplicate names for multiple products):	Doctoral Students from the applying program(s) (Duplicate names for multiple products, if applicable):	Product citation (use standard publication reference format such as that of IEEE, ACM, or APA)	URL or 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 PRIVACY	K. OTHER
1	Jane Doe, Ph.D.	--	Russ, M., **Doe, J.**, & Chen, A. (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....				X							X
2	Jane Doe, Ph.D.	Butler, W. (Ph.D. Candidate)	**Doe, J.**, & **Butler, W.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....	X				X						
3	Jane Doe, Ph.D.	--	Tejay, G., Goel, S., & **Doe, J.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....				X	X						
4	Alice McCumber, Ph.D.	Carlton, M. (Ph.D Candidate)	**McCumber, A.**, & **Carlton, M.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....		X			X						
5	Alice McCumber, Ph.D.	--	Xu, H., & **McCumber, A.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....			X				X				
6	John Abbot, Ph.D.	--	**Abbot, J.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....											
7	Wei Li, Ph.D.	--	**Li, W.**, & Zeichick, D. (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....											
8	Wei Li, Ph.D.	Madrid, J. (Ph.D. Student)	**Madrid, J.**, Lee, B., & **Li, W.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....		X							X		
9	Sandra Blanke, Ph.D.	Bliss, G. (Ph.D Candidate)	**Blanke, S.**, & **Bliss, G.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....				X					X		
10	Sandra Blanke, Ph.D.	--	Konkey, A., Kepner, J., & **Blanke, S.** (year). Title. *Journal, Vol* (Iss), pp-pp.	https://doi.org/....						X					X
...	...		...							X			X		

Discussion and Rationale. Peer reviewed products provide an objective evaluation on programmatic research expertise and impact. With at least four (4) full time faculty members conducting research in cybersecurity, it is expected that on the average each faculty member produces at least three (3) research products over the span of five (5) years.

C6. Cybersecurity-Related Research Funding

To enable research, sufficient financial resources are necessary to cover faculty members' time, support of (doctoral) students, and purchase supplies and/or equipment. Unlike internal support, competitive, externally funded research grants and awards by funding agencies (e.g., NSA, NSF, DARPA, IARPA, DoD, DHS, DOE, etc.), industrial research awards (e.g., Microsoft, Intel, Google, IBM, etc.), and/or other foundation awards are indicators of research excellence. Note, the cybersecurity-related research funding(s) are associated with the faculty members not institutions. Example: a cybersecurity-related grant received by a faculty member four (4) years ago while they were at a different institution is applicable for this criterion.

Requirements:

Provide a history of cybersecurity-related research funding as described above within the past five (5) years, together with all the pending research funding at the time of this submission.

a) **Funding Portfolio:** Provide a history of cybersecurity-related research funding as described above for the past five (5) years together with all the pending research funding at the time of this submission. At least three (3) cybersecurity-related research grants within the past five (5) years that involve at least two (2) of the T/TT faculty members indicated in C4.a. are required. For each grant, provide the project title, funding source, and years covered. Links (URLs) to the specific award on the funding source website (for example, such as those found on the NSF) should be provided when possible. If links are not available, the list should be signed by the Dean of the college and/or director or the Dean of the institution's research management office.

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

Discussion and Rationale. Research requires support for those conducting it. Grants demonstrate that the research has been reviewed and judged to be relevant and timely.

C7. Doctoral Students

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

Requirements:

a) **Doctoral Students in the Past Five (5) Years:** Only report on students who worked or are working on research in topic areas such as those listed in Table 2.

1. Provide a letter on official leatherhead signed by the relevant Department Chair(s) or Dean attesting for the doctoral enrollment number (a student can be counted for only one academic program) across all cybersecurity-related programs submitted in C3 for the past five (5) years. On average, there should be at least four (4) new or continuing doctoral students per year conducting cybersecurity research throughout the past five (5) years.
2. For each doctoral student, list the name, faculty advisor, research area, number of publications, graduation year or expected date of graduation, and funding source (for example, grants, industry support, funding by the institution, teaching assistantships, self). Student name(s) may be redacted if needed; however, a justification for redaction should be provided. If possible, provide information on the first job placement for the doctoral graduates.
3. Describe the progress of at least three (3) current doctoral students and show how they can be expected to graduate within the next five (5) 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 Research Products:** Provide PDFs or links to a minimum of five (5) distinct cybersecurity-related research products (peer-reviewed papers, patents, etc.) that have been authored or co-authored by graduate students. For other research products, such as major software components, datasets, and test beds, a justification must be included. Only include research products published within the past five (5) years that resulted from work by doctoral and/or master-level students. The links shall allow access to the referenced products.

c) **Recent Graduates:**

1. Provide a list of at least three (3) students graduated from the doctoral degree program(s) listed in C3 within the past five (5) years, with a dissertation topic focused on solving a research problem in cybersecurity. For each dissertation, provide a link to the dissertation or PDF.
2. Provide information regarding the number of doctoral and master-level graduates who have completed a cybersecurity-focused dissertation/thesis (including dissertation/thesis title, author name, date, research area and link to thesis/dissertation documents or PDFs) in the past five (5) years. If possible, provide information on the first job placement for recent doctoral graduates.

Discussion and Rationale. Doctoral students form an integral part of a strong, active research environment. The presence of at least four students will stimulate interactions among themselves both professionally and socially, producing a strong and invigorating environment for research.

Sustained financial support is always a main concern for doctoral students. A loss of financial support often results in the loss of students from the program. It is thus of utmost importance to ensure that all doctoral students are financially supported without interruption.

C8. Institutional Support for Cybersecurity-Related Research

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 requirements below, an institution must satisfy C8.a, and at least one of: C8.b.1, C8.b.2 and/or C8.b.3.

Requirements:

a) **Active Entities:** Identify operational, and active entities (for example laboratories/centers) that focus on research in cybersecurity (Provide links to these entities).

b) **Support:** At least one (1) of the following three (3) (provide evidence such as flyers, digital announcements, etc.):

1. **Event Support:** List research seminars and/or colloquium talks by cybersecurity professionals, both from within and outside of the institution (Provide evidence).
2. **Event Hosting:** Describe activities such as hosting of research conferences, workshops and/or other similar events at the institution (Provide evidence).
3. **Other Support:** Describe other institutional support.

Discussion and Rationale. To ensure sustainability, it is necessary for the institution to commit its support to efforts in cybersecurity research. Furthermore, knowing about active entities involved at the institution will provide the NCAE Program Office and the community at large about the research foci of the NCAE-R designated institutions.

C9. External Professional and Scholarly Service in Cybersecurity-Related Research

Faculty members are expected to be actively involved in external professional and scholarly activities in cybersecurity research. Do not duplicate activities appearing in C10. Documentation for these activities must be provided wherever possible. Examples of activities include (but not limited to):

- Serving as a cybersecurity subject matter expert on the technical program or organizing 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, keynote, and/or other speeches.
- Serving as an external reviewer for tenure and/or promotion for faculty members at other institutions.

Requirements:

a) **External Professional Service Related to Cybersecurity Research by T/TT Faculty Members Listed in C4.a:** Provide evidence that at least two (2) T/TT faculty members listed in C4.a. are actively involved in at least one (1) professional external service in cybersecurity per year, each; and

b) **Cybersecurity Research Related Scholarly Service by Additional Full-Time Faculty Members Listed in C4:** Provide evidence for involvement of additional full-time faculty members with at least six (6) cybersecurity service activities as listed above within the past five (5) years.

Discussion and Rationale. These services provide a platform for researchers to exchange ideas and to broaden their knowledge.

Section II Criteria (For Re-Designating Institutions Only)

This section includes one criterion (C10) that is required for Re-Designating CAE-R institutions only.

C10. Involvement in NCAE-C Activities, CAE Community, and CAE Community of Practice in Cyber Research (CAE CoP-R)

A CAE-R institution shall be actively involved in the activities of the NCAE-C, CAE Community, and the CAE Community of Practice in Cyber Research (CoP-R), both working within the CAE-R and helping to grow the CoP-R.

Requirement (For Re-Designating Institutions only):

a) **CAE-R Community Involvement:** Provide evidence that the institution was involved with the CAE-R within the past five (5) years. Involvement in a minimum of three (3) different CAE-R activities from at least two (2) different categories are required. Do not duplicate activities appearing in C9. Documentation for these activities must be provided wherever possible. Categories of activities are given below.

1. Attendance at CAE Symposium and CAE-R meetings. Provide evidence such as registration confirmation, a snapshot of a symposium badge, etc.
2. Participation in any working groups in the CAE Community of Practice in Cyber Research (CoP-R), including giving feedback and attending small group discussions. Provide evidence such as an email acceptance of an invitation to participate in a CoP-R working group, feedback confirmation from CoP-R working group, etc.
3. Reviewing CAE-R designation applications. Provide evidence such as an email acceptance of an invitation to review.
4. Giving and/or participating in CAE Tech Talks. Provide evidence such as a Tech Talk announcement.
5. Reviewing CAE-R grant applications.
6. Serve as a mentor for institutions that aspire to become CAE-R institutions.
7. Contribute curriculum, time, and resources in support of the CAE Community as a whole.
8. Other CAE-R activities.

Discussion and Rationale. This requirement reflects the institution’s commitment to the CAE-R program.

CAE-C POST-DESIGNATION REPORTING REQUIREMENTS

Academic institutions holding any NCAE-C designations (CAE-CD, CAE-CO, & CAE-R) must update their relevant qualifying designation criteria information yearly by an annual report or in the reporting tool.

Institutional Metrics

There is a continual need for specific metric elements associated with institution performance to demonstrate the veracity and efficacy of the NCAE-C program. Items such as number of students, number of graduates, and other "metric" elements are used by the NCAE-C PMO to document program effectiveness with a wide constituency. The needed elements are defined by the PMO and collected at application time and annually.

Expectations of All Designated Institutions

- Newly designated institutions will send a Program Representative to an orientation meeting in conjunction with their designation ceremony or within eight (8) months of designation date.
- The appointed Point of Contact (POC) is expected to represent the academic institutions by participating in program activities and projects. Participation may include, but is not limited to, acting as an Advisor, Mentor, or Reviewer; participation in program management Working Groups; providing input on questions and projects sponsored by the PMO; contribute curriculum/resources for the use of NCAE-C designated institutions.
- Submit annual report on or before the due date established by the NSA PMO.
- Send a Program Representative to an annual CAE Community Symposium and/or the annual POC Meeting and/or regional CAE Community Meetings
- Maintain designated program

1. Annual Report of Institutional Metrics

The most important requirement of post-designation is the annual report of institutional metrics. **All NCAE-C designation *MUST* submit their annual report of institutional metrics on or before the due date established by the NSA PMO (normally in the January / February timeframe).** There is a continual need for specific metric elements associated with institution performance. Items such as number of students, number of graduates, and other "metric" elements are used by the PMO to document program effectiveness with a wide constituency. The needed elements will be defined by the PMO and collected at application time and annually. These elements will be delivered via entry into a web-based data collection system and are the responsibility of the institution to keep current. If the required annual report of institutional metrics is not submitted on time each year, a message is automatically sent to the POC's supervisor or the appropriate Dean (See Table 3 for time-dependent additional consequences).

Table 3. Consequences of Failure to Submit the Annual Report of Institutional Metrics

Requirements	Consequence
1. Submit Annual Report on or before the due date	If the required information is not submitted on time, a message is automatically sent to the POC's supervisor or the appropriate Dean
• After 30 days	If the information is not submitted within 30 days of the deadline, a message is sent to the President, cc to Dean; the institution is considered on probation, and faculty/POC/staff are ineligible for travel assistance to NCAE-C sponsored events. The institution's designation returns to good standing upon submission of the report.
• After 90 days	If the information is not submitted within 90 days of the deadline, the institution is ineligible for Grants or Scholarships issued by the PMO for the remainder of the calendar year, and the Institution is removed from the Designated list online; the President is notified of this action. The institution's designation returns to good standing upon submission of the report.

• After 120 days	If the information is not submitted within 120 days of the deadline, beyond the consequences noted in the 90 days mark, an ad hoc committee will be assigned to review the status of the program and report back to the PMO within 30 days. The committee will be authorized, at its discretion, to request documentation and to contact the POC(s), institutional administrators, or take other steps to review the current state of PoS Validation and/or NCAE-C Designation compliance in order to ascertain facts relevant to the status of the program/center remaining in accordance with its most recent PoS Validation and/or NCAE-C Designation application. The PMO will receive a report from the ad hoc committee within 30 days of convening it with comprehensive documentation providing details about their assessment and may take any action deemed appropriate up to declaring the program to be in non-compliance. Upon finding a program in non-compliance the PMO will instruct an institution to remove all references to NCAE-C (including logos and other NCAE-C or CAE indicators) from all printed and electronic materials and to remove all references to NCAE-C status. The institution's designation returns to good standing upon valid reply to the ad hoc committee and submission of the report.
• Over 180 days	Failure to submit the report within 180 days, and or failure to acquire an extension from the PMO, will result in suspension from the program. Upon completion of the 30-day suspension, and if the institution is still non-responsive, the PMO will instruct an institution to remove all references to NCAE-C (including logos and other NCAE-C or CAE indicators) from all printed and electronic materials and to remove all references to CNAE-C status. The institution will be required to reapply for PoS Validation and/or NCAE-C re-designation for return to good standing.
2. Maintain correct contact information	Important events, changes to the program, deadlines, and funding opportunities for POC, Dean and Institution President are distributed by email to the POC. Failure to keep information up to date results in missing out on recognition, speaking and publication opportunities, grant solicitations and other program benefits.
3. Major changes to the doctoral program(s) milestones	Can result in reconsideration of the designation, may include visiting committee visit. NSA reserves the right to rescind designation(s) under circumstances where critical doctoral program(s) milestone requirements are not met any time during the designation period.

2. Maintain Correct Contact Information

Important events, changes to the program, deadlines, and funding opportunities for POC, Dean, and Institution President are distributed by email to the POC. Failure to keep contact information up to date results in missing out on recognition, speaking and publication opportunities, grant solicitations and other program benefits. It is the role of the POC and/or other institutional staff overseeing the NCAE-C designation to ensure that the information about the institution, the POC, Dean, and President, along with all other relevant designation information is updated on a regular basis.

RECURRING REVIEW OF CAE-R DESIGNATION CRITERIA

Academic institutions holding any CAE-R designations must formally renew their CAE-R Designation every five years.

A 5-Year Report of Institutional Metrics

An aggregated document of the past five (5) Annual Reports of Institutional Metrics (See Expectations of All Designated Institutions, Section 1 above).

APPENDIX A – CAE-R FACULTY MEMBER’S BIOGRAPHICAL SKETCH

CAE-R faculty member biographical sketch shall be no more than four (4) pages.

Current Position
Address
Contact Information

Professional Preparation

Appointment History (minimum last 8-10 years)

Cybersecurity Research Interests

Five (5) Recent Publications in Cybersecurity-Related Research (use standard publication reference format such as that of IEEE, ACM, or APA)

Five (5) Other 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 (past five (5) years)
Doctoral Students (past five (5) years)
Other Relevant Information (for example, mentoring postdoc fellows, masters students, etc.)

APPENDIX B – CAE-R APPLICATION EVALUATION FORM

Evaluation of Section I Criteria

Evaluation methodology is developed with two basic principles, (1) the evaluation is objective and does not attempt to rank any program, (2) allowing institutions that are weak in one academic program while strong in another to balance out the total evaluation. Section I is met if the criteria C1 through C9 are met.

C1-E. Research Classification		
a) U.S. institution with Carnegie Classification or with NSA's approval to submit	Met _____	Not Met _____
C1-E	**Met _____**	**Not Met _____**
Comments: ____		
C2-E. INSTITUTIONAL COMMITMENT (This criterion is met if all its sub-elements are met)		
a) Commitment Letter:		
1. Accreditation	Met _____	Not Met _____
2. Carnegie Classification	Met _____	Not Met _____
3. POC from the institution	Met _____	Not Met _____
4. List of doctoral programs supporting the designation	Met _____	Not Met _____
5. 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 NCAE-C PMO	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 _____
C2-E	**Met _____**	**Not Met _____**
Comments: ____		
C3-E. Academic Program(s) (This criterion is met if all sub-items are met AND the average of scores on all submitted doctoral programs is at least three (3))		
Doctoral Program 1		
a) Degree Name	Met _____	Not Met _____
b) Doctoral Program Elements		
1. Graduate handbook (in PDF) for each program)	Met _____	Not Met _____
i. Process for readiness to pursue a doctoral program in cybersecurity	Met _____	Not Met _____
ii. Process for readiness to conduct research in cybersecurity	Met _____	Not Met _____
iii. Process for evaluating student's research result	Met _____	Not Met _____
2. Demonstrate academic rigor		
i. Faculty Committee process to oversee the Qualifying Exam (or equivalent) Score = 0 if no process exists Score = 1 if an oversight committee process is evidenced in programmatic documentation	Score ______	
ii. Any Comprehensive Exam Committee (or equivalent) is required to have >=3 full time faculty members holding doctoral degrees Score = 0 if any Comprehensive Exam Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees. Score = 1 if all Comprehensive Exam Committees (or equivalent) include >= 3 full time faculty members holding doctoral degrees. Score = 2 if all Comprehensive Exam Committees (or equivalent) include five (5) or more full-time faculty members holding doctoral degrees.	Score ______	
iii. Any Dissertation Committee (or equivalent) is required to have >= 3 full time faculty members holding doctoral degrees, one (1) of whom is		

outside the academic unit of the program
Score = 0 if any Dissertation Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees, or no external member is required
Score = 1 if all Dissertation Committees (or equivalent) include >= 3 full time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program
Score = 2 if all Dissertation Committees (or equivalent) are required to include >= 5 full-time faculty members of whom at least three (3) hold doctoral degrees, or if the committee includes at least three (3) full time faculty members holding doctoral degrees and an additional member external to the institution. Score ______

iv. Any other requirements pertaining to academic rigor and objectivity, e.g., that the program conducts an annual program review of all doctoral students.
Score = 0 if no evidence for any other requirement is provided
Score = 1 if evidence for other requirement(s) is provided Score ______

Academic Rigor for Program 1 **Score ______**

c) Broad Knowledge in Cybersecurity Met _____ Not Met _____
d) Assessment Met _____ Not Met _____

Items a, b, c, and d **Met _____** **Not Met _____**

Comments: ____
____

Doctoral Program 2 (if submitted)

a) Degree Name Not Met _____
b) Doctoral Program Elements
3. Graduate handbook (in PDF) for each program) Met _____ Not Met _____
iv. Process for readiness to pursue a doctoral program in cybersecurity Met _____ Not Met _____
v. Process for readiness to conduct research in cybersecurity Met _____ Not Met _____
vi. Process for evaluating student's research result Met _____ Not Met _____

4. Demonstrate academic rigor
v. Faculty Committee process to oversee the Qualifying Exam (or equivalent)
Score = 0 if no process exists
Score = 1 if an oversight committee process is evidenced in programmatic documentation Score ______

vi. Any Comprehensive Exam Committee (or equivalent) is required to have >=3 full time faculty members holding doctoral degrees
Score = 0 if any Comprehensive Exam Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees.
Score = 1 if all Comprehensive Exam Committees (or equivalent) include >= 3 full time faculty members holding doctoral degrees.
Score = 2 if all Comprehensive Exam Committees (or equivalent) include five (5) or more full-time faculty members holding doctoral degrees. Score ______

vii. Any Dissertation Committee (or equivalent) is required to have >= 3 full time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program
Score = 0 if any Dissertation Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees, or no external member is required
Score = 1 if all Dissertation Committees (or equivalent) include >= 3 full

time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program
Score = 2 if all Dissertation Committees (or equivalent) are required to include >= 5 full-time faculty members of whom at least three (3) hold doctoral degrees, or if the committee includes at least three (3) full time faculty members holding doctoral degrees and an additional member external to the institution. Score ______

viii. Any other requirements pertaining to academic rigor and objectivity, e.g., that the program conducts an annual program review of all doctoral students.
Score = 0 if no evidence for any other requirement is provided
Score = 1 if evidence for other requirement(s) is provided Score ______

Academic Rigor for Program 2 **Score ______**

c) Broad Knowledge in Cybersecurity Met _____ Not Met _____
d) Assessment Met _____ Not Met _____

Items a, b, c, and d **Met _____** **Not Met _____**

Comments: ____
____

. . .

Doctoral Program n (if submitted)
a) Degree Name Met _____ Not Met _____
b) Doctoral Program Elements
1. Graduate handbook (in PDF) for each program) Met _____ Not Met _____
i. Process for readiness to pursue a doctoral program in cybersecurity Met _____
ii. Process for readiness to conduct research in cybersecurity Met _____
iii. Process for evaluating student's research result Met _____

2. Demonstrate academic rigor
i. Faculty Committee process to oversee the Qualifying Exam (or equivalent)
Score = 0 if no process exists
Score = 1 if an oversight committee process is evidenced in programmatic documentation
ii. Any Comprehensive Exam Committee (or equivalent) is required to have >=3 full time faculty members holding doctoral degrees Score ______
Score = 0 if any Comprehensive Exam Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees.
Score = 1 if all Comprehensive Exam Committees (or equivalent) include >= 3 full time faculty members holding doctoral degrees.
Score = 2 if all Comprehensive Exam Committees (or equivalent) include five (5) or more full-time faculty members holding doctoral degrees.
iii. Any Dissertation Committee (or equivalent) is required to have >= 3 full time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program Score ______
Score = 0 if any Dissertation Committee (or equivalent) has < 3 full time faculty members holding doctoral degrees, or no external member is required
Score = 1 if all Dissertation Committees (or equivalent) include >= 3 full time faculty members holding doctoral degrees, one (1) of whom is outside the academic unit of the program
Score = 2 if all Dissertation Committees (or equivalent) are required to include >= 5 full-time faculty members of whom at least three (3) hold

doctoral degrees, or if the committee includes at least three (3) full time faculty members holding doctoral degrees and an additional member external to the institution.

iv. Any other requirements pertaining to academic rigor and objectivity, e.g., that the program conducts an annual program review of all doctoral students. Score ______

Score = 0 if no evidence for any other requirement is provided
Score = 1 if evidence for other requirement(s) is provided

Score ______

Academic Rigor for Program n Score ______

c) Broad Knowledge in Cybersecurity Met _____ Not Met _____
d) Assessment Met _____ Not Met _____

Items a, b, c, and d **Met _____** **Not Met _____**

Comments: ____
____

All Programs Items **Met ______** **Not Met _____**
Average Program Score = ____________ (met if >=3) **Met ______** **Not Met _____**

C3-E **Met _____** **Not Met _____**

C4-E. FACULTY MEMBERS CAPACITY AND EXPERTISE (This criterion is met if all its sub-elements are met)

a) T/TT or eq. faculty members whose primary research is in cybersecurity (>=2) Met _____ Not Met _____
b) At least one (1) other T/TT or equivalent faculty members Met _____ Not Met _____
c) Total full-time faculty members (>=4) Met _____ Not Met _____
d) Biographical sketch for each faculty member Met _____ Not Met _____
e) C4 Faculty Summary Table provided Met _____ Not Met _____

C4-E **Met _____** **Not Met _____**

Comments: ____
____

C5-E. CYBERSECURITY-RELATED RESEARCH PRUDUCTS (This criterion is met if all its sub-elements are met)

a) Research Products: Product Summary Table provided with at least twelve (12) distinct products that involve at least two (2) T/TT faculty members noted in C4.a. Met _____ Not Met _____

b) For the last five (5) years, at least four (4) faculty members listed in C4 (at least three (3) of them are T/TT faculty members) must have at least three (3) distinct research products each. At least two (2) of the three (3) distinct research products must be peer-reviewed. Met _____ Not Met _____
Products provided in the C5 Summary Table follow all requirements and use standard publication reference format such as that of IEEE, ACM, or APA

C5-E **Met _____** **Not Met _____**

Comments: ____
____

C6-E. CYBERSECURITY-RELATED RESEARCH FUNDING (This criterion is met if all its sub-elements are met)

a) Cybersecurity-Related Funding Portfolio (Details provided per C6.a):
At least three (3) cybersecurity-related research grants within the past five (5) years that involve at least two (2) faculty members listed in C4 are required. Met _____ Not Met _____

Met _____ Not Met _____

b) Future Funding: For the year following the date of submission, there is at least one (1) grant active or a documented commitment for a grant involving faculty in C4, and details provided per C6.a.	**Met _____**	**Not Met _____**
C6-E		
Comments: ____		
C7-E. STUDENTS (This criterion is met if all its sub-elements are met)		
a) Doctoral Students in the past five (5) years:		
1. Average of at least four (4) students per year with an official affirming letter	Met _____	Not Met _____
2. Student details provided	Met _____	Not Met _____
3. At least three (3) current doctoral students are in path for graduating in next five (5) years	Met _____	Not Met _____
4. Funding opportunities are provided to all current doctoral students is in place through the coming year	Met _____	Not Met _____
b) At least five (5) relevant student products such as papers/software/datasets and other artifacts (no duplication of those listed in C5)	Met _____	Not Met _____
c) Recent Graduates: Within the past five (5) years, at least three (3) students graduated with a doctoral degree with dissertation topic focused on cybersecurity.	Met _____	Not Met _____
C7-E	**Met _____**	**Not Met _____**
Comments: ____		
C8-E. INSTITUTIONAL SUPPORT FOR CYBERSECURITY-RELATED RESEARCH (This criterion is met if items a and b are met)		
a) Active Entities	Met _____	Not Met _____
b) Support (At least one (1) of the three (3) below) 1. Event Support 2. Event Hosting 3. Other Support	Met _____	Not Met _____
C8-E	**Met _____**	**Not Met _____**
Comments: ____		
C9-E. EXTERNAL PROFESSIONAL AND SCHOLARLEY SERVICE IN CYBERSECURITY-RELATED RESEARCH (This criterion is met if all its sub-elements are met)		
a) At least two (2) T/TT faculty members listed in C4.a are each actively involved in at least one (1) professional external service in cybersecurity research per year.	Met _____	Not Met _____
b) At least a total of six (6) cybersecurity services across all faculty members noted in C4 within the past five (5) years.	Met _____	Not Met _____
C9-E	**Met _____**	**Not Met _____**
Comments: ____		
SUMMARY		
SECTION I	**Met _____**	**Not Met _____**

Evaluation of Section II Criterion (This Criterion is for Re-Designating Institutions Only)

Section II is met if C10 criterion is met.

C10-E. INVOLVEMENT IN NCAE-C ACTIVITIES, CAE COMMUNITY, AND CAE COMMUNITY OF PRACTICE IN CYBER RESEARCH (CAE COP-R)		
a) CAE-R Community Involvement activities (>=3 from at least 2 different categories, with no duplications from C9)	Met ______	Not Met ______
C10-E	**Met ______**	**Not Met ______**
Comments: ____ ____		
SUMMARY		
Section II	**Met ______**	**Not Met ______**

ACKNOWLEDGEMENTS

The NSA would like to thank **Agnes Chan** of Northeastern University, **Cynthia Irvine** of Naval Postgraduate School and **Susanne Wetzel** of Stevens Institute of Technology for leading the effort in revising the CAE-R (Re-) Designation Criteria.

In addition, the NSA would like to thank the following individuals for their feedback and contributions to this document:

Mike Burmester, Florida State University

Lynne Clark, National Security Agency

Ram Dantu, University of North Texas

Jack Davidson, University of Virginia

William Enck, North Carolina State University

Lance Fiondella, University of Massachusetts, Dartmouth

Hanan Hibshi, Carnegie Mellon University

Ahmed Ibrahim, University of Pittsburgh

Paul Kealey, University of Arizona

Karen Leuschner, National Security Agency

Yair Levy, Nova Southeastern University

Nasir Memon, New York University

Guevara Noubir, Northeastern University

Roberto Perdisci, University of Georgia

Lori Pfannenstein, 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

Edward V. Zieglar, National Security Agency

Neal Ziring, National Security Agency