National Centers of Academic Excellence in Cybersecurity NCAE-C 2023 Re-designation Requirements Process

Contents

Part One. NCAE-C Re-designation Overview

1.1 Introduction to the NCAE-C Process for Re-designation

The **National Centers of Academic Excellence in Cybersecurity (NCAE-C)** designation is valid for a period of five years; designated institutions apply for re-designation every five years. Academic institutions desiring a NCAE-C designation join the program through the Candidates Program, proceed to **Program of Study (PoS) Validation**, and may then apply for Designation after demonstrating specific institutional commitment, policies, and processes requirements. Figure 1 is a representation of the process where each step builds upon the previous.

Institutions may opt to receive only PoS Validation. Validation also requires re-validation through the Candidates Program every five years to maintain that relationship with the NCAE-C program. These institutions may use the NCAE-C Validation logo (but not the NSA or partner logos) on their website and may attend events. Institutions that only obtain PoS Validation are not eligible for travel reimbursement, grants and scholarship programs, or other opportunities provided NCAE-C designated institutions. The process from intake to designation is managed by the Candidates and Peer Review National Center, with the NCAE-C Program Management Office (PMO) making final designation decisions. Figure 1 represents the process from induction into the Candidates program through the first 10 years of designation.

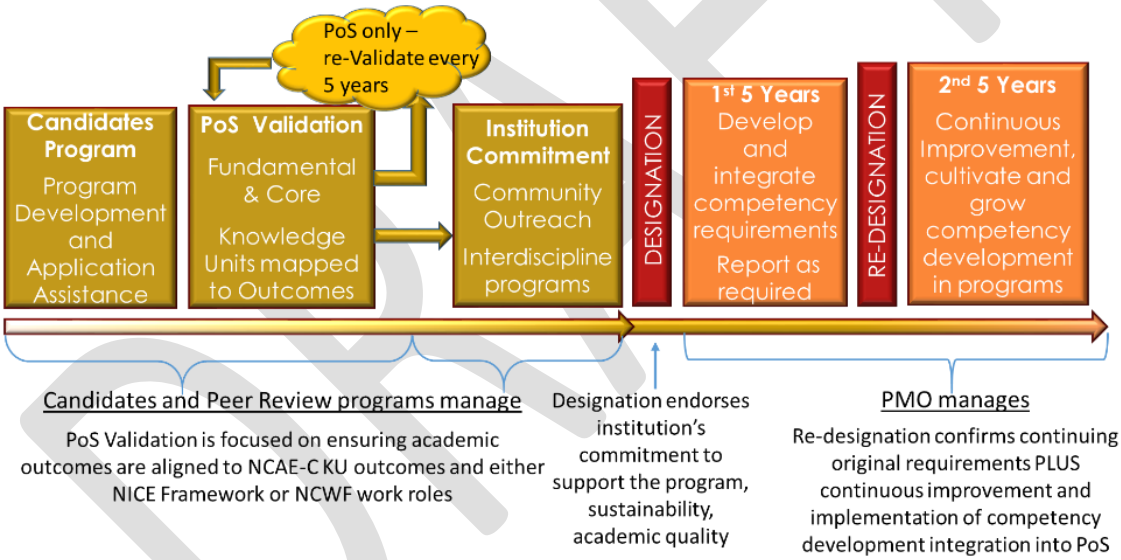

Figure 1: Program Progression from Candidate to Re-designation

Once an institution is designated, the NCAE-C PMO provides oversight. This document outlines the process from designation to re-designation. Re-designation will continue to include monitoring institutions' ongoing development of qualifying courses and the commitment to continuous improvement. Designation Points of Contact (POCs) and alternate POCs are expected to actively contribute to the program, such as joining working groups or committees, or acting as mentors or peer reviewers. POCs and alternate POCs are also expected to participate in program activities, such as attending the annual PMO Meeting and the annual CAE Symposium. In addition, there is an increased emphasis on mechanisms to build the competency of students, to increase the efficacy of faculty members both in pedagogy and technical expertise, and to prepare students for a career.

1.2. Re-designation Process Objectives

The NCAE-C Re-designation process is designed to provide guidelines, requirements, and expectations for the institutions to obtain re-designation with the same PoS(s) at the end of the five-year designation period. The process is designed so that the NCAE-C PMO can track each institution's progress, provide feedback and assistance when needed, and so that the institution is preparing for re-designation incrementally. The institution does not repeat the original PoS validation and designation process; the PoS is re-validated as part of the re-designation process. Information provided by the institution in Annual Reports is compiled over the five-year period and provides the core of information necessary to successfully achieve re-designation.

The original PoS validation and designation requirements are available at https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/. Figure 2 shows the summarized requirements for re-designation; more details are available through the corresponding reference number.

Figure 2. Compiled Re-Designation Requirements	Reference
Attend a designation orientation meeting within three (3) months of the designation/re-designation date.	Part 3
Maintain current contact information in the program management tool database for the designation POC, alternate POC, POCs' supervisor(s), Dean and President to ensure the PMO will be able to contact an institution representative. ***The PMO cannot change this information***.	Part 2.1.
Participate in the NCAE-C program and CAE Community by participating in NCAE-C events, representing NCAE-C at another cybersecurity event, or participating in activities sponsored by other institutions.	Part 2.1.
Contribute time and expertise to programs and initiatives, and other possible contributions listed in Part Two.	Part 2.1.
Pursue continuous improvement according to the institution's accreditation requirements, including maintenance of a continuous improvement plan.	Part 3.1.
Implement student competency development incrementally so that all NCAE-C requirements are fully met by the fifth year of designation.	Part 3.2.
Ensure students have received resources, counseling, and awareness experiences to prepare them for a career in cybersecurity.	Part 3.3.
Ensure faculty members have access to faculty development opportunities, particularly to develop pedagogical expertise necessary to implement these requirements.	Part 3.4.
Submit Annual Status Reports (4.1.) and Biennial Progress Reports (4.2.). Maintain documentation associated with requirements and annual reporting in the Program Development Tool. Use PMO feedback from reports to correct deficiencies.	Part 4
Compile all documentation required for re-designation in Year 5 to prepare for re-designation in the last quarter of the fifth year.	Part 5

Part Two: Maintenance of Participation and Contribution Requirements and Original Designation

2.1. Participation and Contribution Requirements

Once Candidate institutions receive designation, POCs and alternate POCs must meet all participation and contribution requirements, including attendance at the annual CAE Symposium/PMO meeting. Some of these participation options contribute directly to the efficacy of the NCAE-C programs. Others offer the POC and alternate POC the opportunity to network, collaborate with other institutions and learn about growth of the NCAE-C program and subsequent evolution of requirements or program opportunities. These are in addition to the CAE Symposium/PMO meeting. The re-designation package must include evidence that the designation POC and/or alternate POC have participated in and contributed to CAE events, activities, projects and programs **over <u>each</u> of the FIVE years** between designation and re-designation.

2.1.1. Participation in the NCAE-C program includes actively attending and participating in events and activities, and actively maintaining administrative requirements to ensure good communication. Examples include, but aren't limited to:

- Maintaining correct contact information for all institution representatives required by the database (POC, Alt POC, Supervisor, Dean, President). Important events, changes to the program, deadlines, and funding opportunities for POC, Deans, and the 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 to ensure the information about the institution, the POC, Dean, and President, along with all other relevant designation information is updated on a regular basis.
- Presenting, moderating a panel, chairing a session, lightning talk, or workshop at the annual CAE Community Symposium, Executive Leadership Form (ELF), National Cybersecurity Education Colloquium (NCEC), or other CAE Community events including the CAE Communities of Practice (CoPs) events

2.1.2. Contribution to the NCAE-C program should involve active giving of time or expertise to advance cybersecurity education and/or the NCAE-C program. Examples include, but aren't limited to:

- Serving as PoS Validation and/or NCAE-C Designation mentor, reviewer (Pre-Submission Reviewer (PSR) and/or peer-reviewer)
- <u>Actively</u> contributing to a CAE Community of Practice (CoP), such as serving as a Steering Committee member, initiative co-chair or member of committees or Working Groups
- Developing and submitting a challenge, module, game, curriculum, piloting, and/or providing feedback of student cyber competitions such as the NCAE-C Cyber Games, NICE Challenge Project, or CLARK.
- Participating as an active member of a CAE Working Group, active member of a CAE Community Initiative, Community of Practice (CoP) leader or working group, or other significant role in the CAE Community (Please provide additional detailed description of the significant role in the CAE Community in the justifications file. Indicating "other significant role in the CAE Community" without providing valid justification will not be counted.)
- Collaborating with current NCAE-C institutions on research, grants, course development etc

2.2. Maintenance of original designation requirements.

This is essential to retaining the Designation. Some of these original requirements are considered pass/fail and should any of these change during the five-year period of designation they must be reported immediately to the PMO.

- Requirements for the PoS Validation remain current and the PoS remains aligned to the originally chosen KUs and KU learning objectives.
- The institution's regional accreditation remains current.
- The institution's cybersecurity posture and plan is adequate and current
- The institution maintains and supports the established Center per original designation.
- Outreach to the community and partners meets NCAE-C requirements for sharing with others to improve the practice of cybersecurity in the community. This may include but is not limited to:
    - Developing, leading or hosting outreach activities, competitions, and/or other activities
    - Working with industry partners to develop curriculum, internship or apprenticeship that meets their employee needs.
    - Sponsorship or oversight of students for cyber events for the community at large. Events could include: cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community.
    - Attending outreach activities, competitions, and/or other activities led by other NCAE-C institutions or other partners.
    - Hosting a GenCyber program or other cybersecurity education and awareness program for middle and high school students and/or teachers
- Articulation and/or Transfer agreements with institutions offering a concentration of cybersecurity are maintained and/or expanded.
- The NCAE-C Designation POC is a full-time faculty member with influence over maintenance of the PoS.
- The alternate POC is a full-time employee of the institution associated with the Designation and PoS, such as a Dean, a Center Director, Faculty member or other management position with a working knowledge of the CAE program and the institution's curriculum. The POC may not be an employee in an administrative position with no influence over content and management of the designation or PoS.

Part Three: NCAE-C Requirements for Continuous Improvement, Competency Development, Student Professional Development and Faculty Development

Recent work by faculty committees and grants initiatives has provided focus on four critical elements that will further distinguish NCAE-C designated institutions from most others in the academic community. These critical elements include: an institutional commitment to continuous improvement, a commitment to developing competency, a focus on developing professionalism in students completing or graduating from NCAE-C programs of study, and opportunities afforded to faculty members for technical, professional and faculty development. This section explains the NCAE-C objective and process for implementing these critical elements and provides detailed requirements for re-designation.

To ensure all designated institutions are fully cognizant of these requirements and expectations and any subsequent updates, all newly designated and re-designated institutions will send the POC or alternate POC to a

program representative to an orientation meeting, which may be in person or virtual, **within three months** of the designation/re-designation date. The PMO will host webinars to answer questions and help facilitate integration of new designees on a quarterly basis, and the schedule will be communicated to all new designees.

The vision is that students leave the institution with a keen awareness of their place as a cybersecurity professional, with an understanding of the range of career options available to them, and with a documented portfolio of competencies and experiences. In this vision of the NCAE-C program, designated institutions have a reputation for quality academics, quality faculty, and a commitment to continuous improvement of programs and institutional growth.

3.1. Continuous Improvement

The concept of continuous improvement has always been the bedrock of NCAE-C re-designation and remains the core requirement for success in the program. In this context continuous improvement refers to both the academic program and the institution and is intended to be in concert with the institution's continuous improvement actions to maintain accreditation(s).

3.1.1. Continuous Improvement Plan and Process. A key element to ensure vitality and functionality over time is a strong continuous improvement plan and process. A continuous improvement process with a regular evaluation schedule directed at the validated PoS's Program-Level Learning Outcomes is an essential element of the program. All NCAE-C designations are required to show a continuous improvement plan and process, during the re-designation process every fifth year.

3.1.2. Institutional Continuous Improvement. Institutions must have a commitment to the continued growth of designated programs and Programs of Study, must continue to integrate cybersecurity across disciplines in the institution, must offer students who are not in cybersecurity programs of study the opportunity to explore and understand how cybersecurity applies to their chosen field of study, and must continue to expand the practice of cybersecurity in their communities.

3.2. Competency Development

A focus on competency provides an effective bridge between the students' educational experiences and the workplace. The definition of competency adopted by the CAE community is:

"Competency is the ability for the individual to complete a task or tasks within the context of a work role."

Developing opportunities for students to build their competencies is a proven means to augment existing educational offerings through furthering connections with the workplace and aligning learning with existing and future work roles.

To better assist both graduates of NCAE-C validated PoS(s) and hiring managers from government and industry, it is important that the designated institution identifies the cybersecurity work roles that are most relevant to their validated PoS(s). This will promote graduating students' understanding of the cyber workforce and enable them to make connections between their education and employment. Increasing the connections between the PoS and the workforce will build the competencies of PoS graduates in alignment with government and industry needs.

The NICE Workforce Framework for Cybersecurity (NIST Special Publication 800-181 (https://niccs.cisa.gov/workforce-development/nice-framework) lists 50 work roles within 6 work role categories. Pursuant to EO 13870, the NICE Workforce Framework is the standard for federal workforce work role definition, education and training. The DoD Cyber Workforce Framework **(**DCWF) describes the work

performed by the full spectrum of the cyber workforce (71 work roles) as defined in DoD Directive (DoDD) 8140.01 (https://dodcio.defense.gov/Cyber-Workforce/DCWF). Both frameworks provide a relevant organizing principle for relating students' learning outcomes to the workforce. Institutions may use either framework or both for aligning the PoS to work roles depending on the relevancy to the PoS, where the institution envisions students building their careers and the types of work roles appropriate to the PoS.

The Evidencing Competency working group, with feedback and collaboration with the NCAE-C PMO, has developed a mechanism for identifying those competencies associated with a PoS. The Careers Preparation National Center (CPNC) is now leading this effort. Explanation of the ABCDE Essential Elements framework is at Appendix 3.

Year One: In the first year after designation, at least three relevant work roles will be identified for each validated PoS; these will be aligned to either the DCWF or NICE Framework. By identifying these work roles, the designated institution is indicating their graduating students will have the opportunity to acquire the knowledge, skills, and competencies associated with these work roles. The work role alignment should be evidenced through course content (curricular experiences) and co-curricular and extra-curricular activities that students can access through the PoS. By providing students with information about and alignment with work roles, institutions are informing students about a range of work roles, promoting career choices, and increasing their graduating students' competitiveness in the marketplace.

The CPNC offers training sessions throughout the CAE Community at geographically convenient locations and through virtual resources to assist NCAE-C POCs and staff become familiar with and proficient in the use of the ABCDE Essential Elements framework (see Appendix 3) for documentation of PoS work roles and competencies.

Year Two: In the second year after designation, 10 competency statements will be identified for each PoS. These will be aligned to activities and listed in the biennial report. These should be associated with the (at least) three work roles identified in year one's annual report. Competency statements can relate to curricular experiences (e.g. classroom activities, labs, games, assigned hands-on exercises), co-curricular experiences (e.g. cyber-clubs, internships, cyber range time), and/or extracurricular activities (e.g. cyber competitions, conferences, professional association events). At least five of these should be related to classroom activities.

Competency statements are organized through the ABCDE Essential Elements framework tool (see Appendix 3). This provides a rigorous means for connecting activities to tasks associated with work roles within either the DCWF or the NICE framework. Opportunities for students to develop competencies will be developed within the PoS and evidenced through the writing of competency statements. Developing competency statements should not be difficult for educators considering that cybersecurity has long been a field of applied curricular, co-curricular, and extracurricular activities that offer hands-on experiences for students. Opportunities will be provided for faculty members to develop their understanding of this approach to competency through the provision of an e-handbook, training, and ongoing mentorship.

Year Three: In the third year after designation, the 10 competency statements identified in year two will be implemented within each PoS. An additional template will be provided to guide and document evaluation and reflection upon this implementation process. Student feedback will be consistently collected across the year using the STAR method tool.

Year Four: Competency statements will continue to be developed, described, and delivered throughout this period. The biennial report for year 4 will focus on student evaluation and reflection. The data collection for

these evaluations will be in a pilot stage for the first few years of the roll-out of these new re-designation requirements (2024 – 2028).

Year Five: By year five, it is assumed that the faculty will have gained expertise in developing competency statements as well as having engaged in critical reflections. This expertise might be shared with the CAE community through at least three of the following:

- Contributing competency statements to the e-library (see Table 2 in Appendix 3)
- Presenting at NCAE-C events
- Mentoring new institutions
- Reviewing competency statements that have been uploaded into the e-library
- Reviewing use of tools relating to competency
- Engaging with employers to evaluate new competency statements

If changes are made to the competency experiences available to students, these must be documented and explained.

If work roles have changed, an explanation should be given and competency statements should be modified to ensure competency experiences map onto identified work roles.

3.3. Student Professionalism

The NCAE-C is fundamentally designed to produce students ready to pursue a career in cybersecurity. It is essential students understand their career options, how to pursue employment in the field, and are prepared to advocate for themselves and present their competencies and qualifications in a professional manner. While designated institutions are not required to include student professional development in the PoS, re-designating institutions are required to demonstrate a commitment to student professional development. For the purposes of re-designation, the institution must provide metrics on how students are introduced to cybersecurity ethics, cyber work roles/job positions/career pathways, teamwork, communication, and leadership. This could include collaboration with a campus career development center, cyber workforce mentors, assignments or independent study, internship preparation and participation, and cyber competitions.

Appendix 4 offers an overview of NCAE-C resources to assist in ethics education, professional skills, career awareness, and career pathways.

3.4. Faculty Development

Shortage of qualified faculty in cybersecurity is at crisis levels in the United States. This not only makes it difficult for designated institutions to maintain sufficient faculty to sustain the designated program, but faculty become a limiting factor in growing successful programs.

Faculty are the heartbeat of the NCAE-C program. They contribute in two important ways: they are providing quality education to the nation's future workforce, and they are contributing to the efficacy and growth of the NCAE-C program itself. It is a priority for the NCAE-C program to provide faculty members development opportunities, but it is even more important that the designated institution is proactive in opportunities for professional development for their own faculty members in cybersecurity.

While many of the requirements for re-designation are dependent on the faculty and supporting activities, clubs and other institution resources, development of faculty is an institutional requirement.

3.4.1. Institutions must provide documentation and evidence of opportunities afforded faculty members, especially those associated with the validated PoS. In this case, the term "faculty development" refers specifically to providing the faculty associated with the designated PoS additional development with a focus on pedagogy and resources they need to implement the competency and student development requirements to maintain the NCAE-C designation. This requirement could be met by providing release time, providing travel and tuition costs for specific courses, hosting a small event and bringing in guest speakers, supporting certifications, or other opportunities that faculty member are encouraged to attend.

3.4.2. At the minimum, the institution will ensure faculty members associated with the NCAE-C PoS are able to participate in events and training for faculty offered by the NCAE-C PMO and/or the CAE Community, which may include travel funding if other sources cannot provide support.

Part Four: Reporting

Designated institutions are required to submit an annual report every year, due on 15 January, and a biennial report due at the end of the 10th month in Year 2 and Year 4.

The annual status report will address PoS metrics (numbers of graduates/completers and enrolled by PoS). It will also entail a checklist of critical designation requirements to endorse to the PMO that none of these elements have changed since designation, the three (3) work roles associated with the validated PoS, and/or document changes to the choice of work roles.

The biennial reporting will provide incremental feedback on the institution's progress toward meeting the overall five-year requirements.

Figure 3. Reporting Requirements by Year	Year
Annual Status Report NLT 15 Jan (institutions designated after 15 Jan will provide metrics based on date of designation)	1
Annual Status Report NLT 15 Jan	2
Biennial Progress Report based on designation date	2
Annual Status Report NLT 15 Jan	3
Annual Status Report NLT 15 Jan	4
Biennial Progress Report based on designation date	4
Re-designation Panel Report	5

4.1. Annual Status Reporting

Beginning in 2024, the PMO will require newly designated institutions to file an annual report with data from their previous academic year on the schedule in Figure 4 below. Since the designation is awarded based on a mature program having graduated at least one class, and since that institution is being included as a designated institution in the program, status on the previous graduating/completing class will correctly reflect status for all designated institutions in the NCAE-C program.

Figure 4. Annual Report Due Dates		
Designation Period	Annual Report Due	Data Period
Designated before 31 Oct 2023	15 Jan 2024	Academic Year 2022/2023
1 Nov 23 to 28 Feb 24	15 Apr 2024	
1 Mar to 30 Jun 24	15 Jul 2024	

Designated institutions will provide an annual report on numbers of students enrolled and graduated, and status of critical designation elements. The Annual Status Report will be online year-round to allow institutions the opportunity to enter information as is convenient. The Annual Report will also document the currency of the original designation critical elements.

4.2. Biennial Reporting.

As previously stated, designated institutions will provide a biennial progress report to keep both designation POCs and other staff and the PMO aware of the institution's progress toward meeting final re-designation requirements. This progress report is in the form of a checklist, requiring additional information for items that are not fully compliant. It is divided into three sections, which address participation requirements, original designation requirements, and the four critical elements: continuous improvement, competency development, student professionalism, and faculty development.

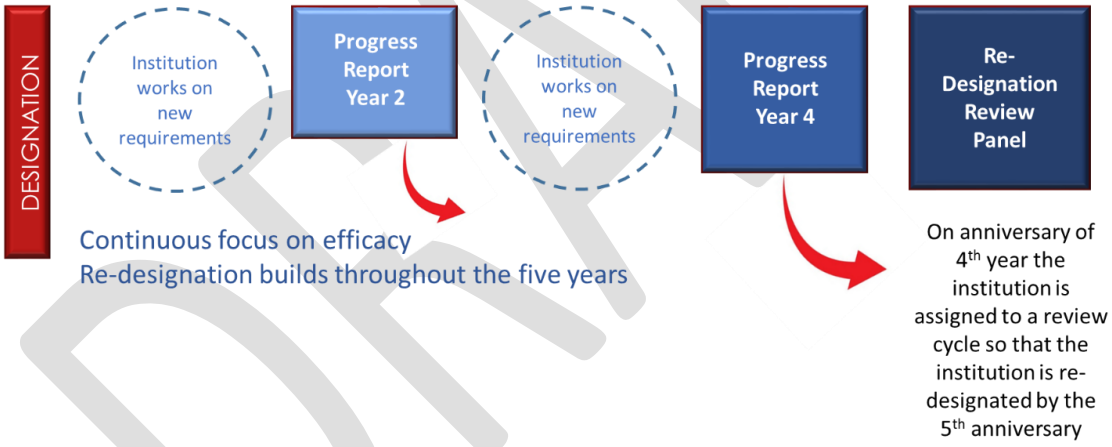

Figure 5: Biennial Progress Report

Each section has the option to answer Yes, Partially, and No.

- Yes answers do not require any additional documentation at the time of submission, but institutions are advised to keep a file of evidence and documents that support the answer. These will be required for the final re-designation.
- Selecting Partially requires a comment to explain why the item is not compliant and the institution's plan to meet the requirement within six (6) months.
- Selecting No requires an explanation and a plan for how the institution will reach compliance in the next six months. The institution will be required to provide an update report six months after the submission date confirming the No has been improved.

The Biennial Re-Designation Progress Report template is available at Appendix 8. Items included in the report are:

4.2.1. Participation Requirements. Have the Designation POC and alternate POC met participation requirements as listed in Part Two, paragraph 2.1? If none of the listed suggestions apply, the report should include explanation of alternate participation.

4.2.2. Original designation requirements. This section includes both PoS Validation and Designation requirements. It is intended to provide the institution and the PMO confirmation that nothing has significantly changed during the reporting period, or that changes are appropriate for the purposes of continuous improvement. Institutions are expected to record appropriate documentation in the program management tool each year so that all evidence is readily available at the fifth year review. This will be especially important should the POC change at some time over the five years of the designation and supports the idea of building up to re-designation annually. Requirements are listed in detail in Part Two, paragraph 2.2.

4.2.3. Continuous Improvement, Competency Development, Student Professional Development, and Faculty Development. These are requirements to be accumulated over the first four years of the designation period. Biennial reports in Years 2 and 4 of the designation must reflect growth towards the final requirement each year. Content for years 2 and 4 is based on requirements in Part Three.

Part Five: NCAE-C Re-designation Requirements

The PMO's objective is to simplify re-designation and preclude any need to start from scratch every five years by repeating Program of Study Validation and the original Designation requirements. The Annual Status Report and the Biennial Progress Reviews will be evaluated by the PMO and feedback will be provided. The intent is to give the PMO an overview of any issues that may need attention before they create a designation problem.

5.1 Overview of Re-designation Process

Designated institutions that remain in compliance throughout the first four years of the Designation should have no problem preparing for re-designation in the fifth year. The biennial Re-designation Progress Report will provide a guideline for institutions so that materials and evidence can be compiled in the fifth year in preparation to meet the Re-designation Review Panel. This will occur in the same quarter the institution was originally designated.

The Re-designation Review Panel will be made up of NCAE-C PMO staff, government partners, and one Peer Reviewer. The Peer Reviewer will be selected from academic institutions in the NCAE-C program that have been through at least one re-designation (more than five years experience) and may not be selected from an institution scheduled for the same cycle. The Peer Reviewer role will be advisory and will not have a vote on adjudication of the re-designation. All members of the Peer Review Panel will receive training on requirements, processes and policies associated with designation and re-designation.

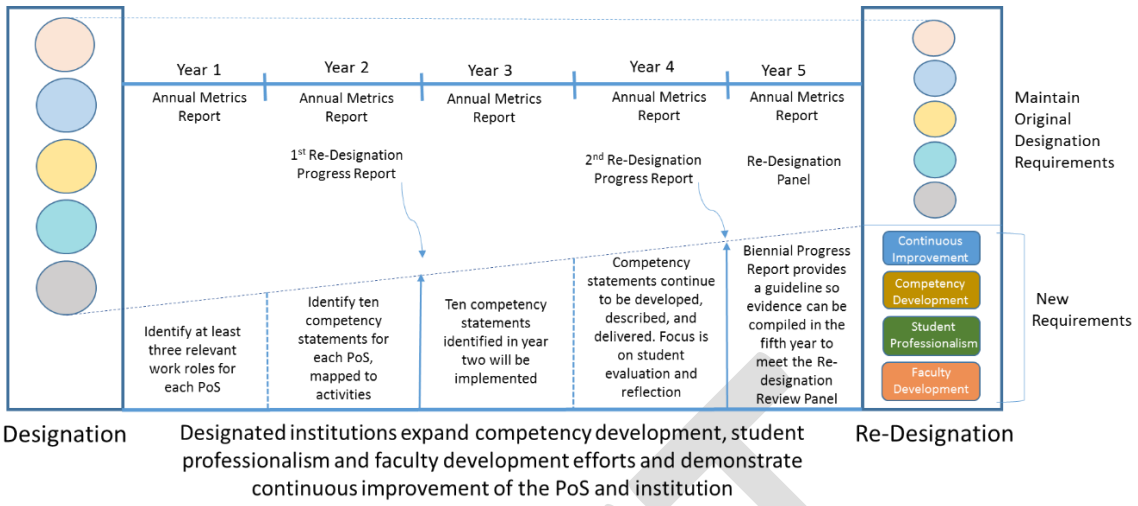

Figure 6: Annual growth toward re-designation in the fifth year

5.2. Biennial Re-Designation Progress Report.

When the institution submits the second Biennial Re-Designation Progress Report, the NCAE-C PMO will assign the institution to a Review Panel cycle. In the fifth year the institution will ensure documentation and evidence to support the self-reviews conducted in the first four years is compiled to submit for re-designation. This documentation and evidence will be collected in the Program Management tool and must be available to the Review Panel six weeks prior to the Review Panel meeting date.

The year between the second Biennial Re-Designation Progress Report and meeting with the review panel will allow the institution to prepare documentation and other evidence to meet re-designation requirements. If the institution has been honestly and correctly providing all required reports in the ensuing four years, this final preparation step should not be onerous. Even though documentation is not required for the Annual Status Report or the Biennial Progress Report, the institution should have ensured documentation and evidence is on-hand in a file ready to be compiled for the final re-designation in year five.

The template for the final re-designation package is at Appendix 7.

Appendix 1. Definitions

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.

Competency is the ability for the individual to complete a task or tasks within the context of a work role.

Continuous Improvement: documentation of a plan, a process, and a regular evaluation schedule that an academic institution and/or academic unit have to enhance the overall quality of its PoS.

Continuous Improvement Plan: documentation of a structured set of actions the academic institution and/or academic unit plans to perform to enhance the overall quality of its PoS.

Continuous Improvement Process: documentation of the continuous improvement plan executed and evaluation of the results of the current continuous improvement plan.

Continuous Improvement – Regular Evaluation Schedule: periodic evaluation of the continuous improvement process documentation and assessment metrics to enhance the overall quality of the PoS.

Course outcomes are the expectations that the academic institution and the PoS is anticipating students to be able to demonstrate when completing a course.

Curriculum Map and Plan: documentation of how the PoS courses are mapped to the Program-Level learning outcomes, and documentation of the courses where program outcome assessment indicators provide evidence for the Program-Level learning outcomes.

An **example** is defined as a characteristic or set of characteristics to illustrate a requirement or set of requirements. Examples provided in this document were not intended for the purpose of replication rather as a general illustration of how the required information can be presented.

An **institution** is a U.S. legal entity authorized to award associate degrees or higher. All institutions applying to the CAE-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 **institutional Point-of-Contact (POC)** is a designated faculty member from the applying institution who will serve as the liaison between the institution and the NCAE-C Program Management Office (PMO). The Institution POC must be a faculty member who has input into the applying PoS curriculum.

A **Knowledge Unit (KU)** is a thematic grouping that encompass multiple, related KU outcomes and learning topics.

A **Knowledge Unit (KU) outcome** is a specific assessment of a concept associated with a particular KU.

KU Alignment: the process of documenting how the KUs and KU outcomes are aligned to the relevant courses in the PoS.

A p**rogram of study (PoS)** is a defined series of elements that leads to the completion of a degree, a certificate or other defined set of outcomes by the institution.

A **program outcome assessment indicator** (assessment metric) is a measure conducted by a faculty member of students' academic performance, student growth, and/or other measure of students' performance of one or more Program-Level learning outcome(s).

Program-Level Learning Outcomes are a description of what graduates should know or be able to do upon completion of the program of study. Combined, these serve as a key measure of graduates' success from the program of study and should be assessed by the identified program outcomes assessment indicators. Each Program of Study should have multiple Program-Level learning outcomes that are consistent with the needs of the program's focus and various constituencies.

Appendix 2. Overview of CAE Designation Requirements

Part 1: CAE-Cyber Defense and CAE-Cyber Operations

1. Introduction to designation requirements

The Program of Study (PoS) validation requirements for NCAE-C–Cyber Defense (aka "CAE-CD") and NCAE-CO Cyber Operations (aka "CAE-CO") programs include evidence of self-study that all academic institutions submit in the application tool. Academic institutions are required to outline faculty, student, curriculum, and continuous improvement information. In addition, any PoS being submitted for validation must have program-level learning outcomes identified and on file at the submitting institution, preferably on the program's website/webpage. Those program-level learning outcomes will then be aligned to the courses in the PoS. The self-study will include documentation of the identified knowledge units (KUs) for the PoS and the alignment of the KUs to the relevant courses in the PoS. No elective courses should be indicated in the KU alignment, as all students should take all courses indicated in the KU alignment.

2. Self-Study Overview (for purposes of initial designation)

1. <u>PoS Curriculum</u> a) The cybersecurity PoS offered by the institution b) Cybersecurity work roles alignment (see 2.3) c) Course syllabi and courses requiring applied lab exercises (for KU aligned courses only) d) Curriculum map and plan with assessment documentation e) Knowledge units (KUs) alignment f) Graduate thesis/dissertation/equivalent guidelines and process (Masters and Doctoral programs only)	**2. <u>Students</u>** a) Student enrollment/graduation in the PoS(s) b) CAE-CD: sample student certificate/notification on transcript/official letter c) Students' work products (papers, assignments, labs etc.) d) Student participation in extra-curricular activities.
3. <u>Faculty Members</u> a) Cyber Program(s) of study PoC b) Full-time, part-time, and adjunct faculty members and faculty qualifications (publications, research, industry involvement, certifications etc.) related to PoS c) Faculty support of enrolled students d) Process of faculty promotion/reappointment (e.g. Faculty policy manual)	**4. <u>Continuous improvement</u>** a) Continuous improvement plan b) Continuous improvement process c) Regular evaluation schedule.

Appendix 2. Overview of CAE Designation Requirements, Page Two

Part 2: CAE-Cyber Research

A U.S. institution of higher education will achieve the CAE-R Designation if all requirements in criteria C1 to C9 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 endoresement, 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 NCAE-C Activities, CAE Community and CAE Community of Practice in Cyber Research (CAE-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).

Appendix 3. Competency Development Documentation

The ABCDE Essential Elements framework

Competency statements are based on the essential elements of competency. Within every competency, there are five elements. An actor (A) performs a behavior (B) within a context (C) to an acceptable degree (D) according to the normative expectations of an employer (E).

A **Actor**	**Who?**	An identification of the knowledge, skills, and prior experiences a student would need to bring with them if they are to enact this competency successfully. This might, for example, identify courses students will need to have already taken and/or knowledge or skills they will have already needed to have mastered.
B **Behavior**	**What?**	References a task within an established work role, with a link to either DoD DCWF (https://public.cyber.mil/cw/dcwf/) or NICE Workforce Framework SP 800-181 (https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final). The identification of a task and the articulation of this within a competency statement ensures the educational opportunity is directly related to the workplace.
C **Context**	**How?**	The context is the description of the specifics of this activity including reference to the technology provided to the student, any documents provided, any additional resources a student might be able to access, and/or any limitations or constraints brought into the experience.
D **Degree**	**How much?**	Provides a measure of how much time a student will be given to complete the activity and defines accuracy and completion expectations. Parameters of accuracy, completion and time relate to a potential employer's expectations of what would be 'good enough' to do the job.
E **Employability**	**Other expectations**	To be successful within the workplace one needs to have professional skills, such as teamwork, communication and problem-solving, as well as established ethical values. Reference should be made to the skills listed within the NCAE-C's Careers Preparation National Center (https://www.montreat.edu/student-life/montreat-360/)

Competency Statements

The program representative and/or the designation Point of Contact (PoC) will be expected to upload competency statements to the e-library using the format shown in Table 2 (below).

ABCDE Model	Attributes ABCDE	Value
Actor	Actor	
	Description	
Behavior	Work role	
	Task	
	Task details	
Condition/Context	Scenario	
	Limitations	
	Technology	
	Documentation	
Degree	Complete	
	Correct	
	Time	
Employability		
Notes (optional)		

Table 2: Structure of competency statements within the e-library

Appendix 4. Student Professional Development Requirements.

An overview of NCAE-C resources and examples to assist in student ethics education, professional skills, career awareness, and career pathways. Re-designating institutions are required to demonstrate a commitment to student professional development and will provide metrics on how students are introduced to cybersecurity ethics, cyber work roles/job positions/career pathways, teamwork, communication, and leadership.

Student Professional Development	Examples (not an exhaustive list)	Goals/Objectives
Cybersecurity ethics	- Montreat 360- https://www.montreat.edu/student-life/montreat-360/ - cybersecurity ethics course - Cyber course assignments/independent study - Cybersecurity ethics "bowl"/competition	- Baseline understanding of cybersecurity ethics
Internship & Resume Preparation and Evaluation	- Cyber Career readiness class - Student pre-/post-internship assessment of goals/objectives/competencies (ABCDE) - Internship supervisor feedback on the student's competencies (ABCDE) - Resume Preparation class/activity	- Address workplace professional behavior - Manage internship & career expectations. - Build cyber resume for private and federal internships/positions
Clubs	- Cybersecurity - Women in Cyber - PoS Specific club	- Develop student support network - Share information on events, internships, research topics, jobs - Provide venue for cyber professional speakers & mentors
CAE-C related national cybersecurity competitions & exercises	- Collegiate Cyber Defense Competitions - https://cyberforce.energy.gov/cyberforce-competition/ - CyberForce Competition - https://cyberforce.energy.gov/cyberforce-competition/ - CSAW - https://www.csaw.io/ - Global Collegiate Penetration Testing Competition - https://cp.tc/ - NCAE Cyber Games - https://www.ncaecybergames.org/ - NSA Cyber Exercise (NCX) - National Cyber League - https://nationalcyberleague.org/ - NICE Challenge - https://nice-challenge.com/ - NSA Codebreaker Challenge - https://nsa-codebreaker.org/home	- Provide virtual training ground for participants to develop, practice, and validate their cybersecurity knowledge & skills - Enable participants learn and demonstrate intangible skills such as problem-solving, teamwork, and communications

Student Professional Development	Examples (not an exhaustive list)	Goals/Objectives
Professional Associations and Conferences	- ACM - https://www.acm.org/ - IEEE - https://www.ieee.org/ - AFCEA - https://www.afcea.org/ISACA - https://www.isaca.org/ - ISSA - https://www.issa.org/ - ISC2 – https://www.isc2.org/ - MCPA - https://public.milcyber.org/ - WiCYS - https://www.wicys.org/	- Build professional and peer networks - Identify mentors - Provide sources for scholarships and job listings - Attend national & regional conferences / present research papers
Cyber work roles	- NICE Framework - https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final - DCWF - https://dodcio.defense.gov/Cyber-Workforce/DCWF/ - Mentorship program - Cybersecurity Career Videos	- Provide frameworks identifying tasks and skills required for cyber work roles - Meet with Cybersecurity Professionals to understand their workroles, and technical and professional skillsets needed for those workroles - Videos to show different workroles

Appendix 5. NCAE-C Code of Ethics and Professional Conduct

As a cybersecurity student, you are expected to uphold a code of ethics and professional behavior that promotes the highest standards of integrity, honesty, trustworthiness, and professionalism. This code serves as a guide to help you make ethical decisions and maintain the trust and confidence of your clients, colleagues, and the public.

The following are the principles of the cybersecurity student code of ethics and professional behavior for students attending NCAE-C schools:

1. Respect: Treat others with respect and honesty. Act in a legal and moral fashion regarding others. Respect the laws and regulations that govern your profession and avoid engaging in any activities that could be considered illegal or unethical.
2. Professionalism: Conduct yourself in person and online in a professional manner, and always adhere to ethical standards when dealing with clients, colleagues, and the public. Your actions should be based on sound judgment, integrity, and the highest levels of ethical conduct.
3. Confidentiality: Maintain the privacy and confidentiality of information, especially concerning protected health information, personally identifiable information, or intellectual property entrusted to you.
4. Accountability: Take responsibility for your actions and be accountable for any mistakes or errors that you make. Learn from your mistakes and take steps to prevent them from happening again. Do no harm.
5. Collaboration: Strive to collaborate online and in person with other cyber professionals to make the cyber world safer for all.
6. Attribution: Give credit to others for their work. Only use generative AI with proper attribution and proper permission from your college, university, or employer.
7. Continuous Learning: Continue as a life-long learner to ensure competency in the field. Share your knowledge with others and promote best practices.
8. Reporting: Report to the appropriate authorities any unethical behavior you observe in the course of your work.

By adhering to this code of ethics and professional behavior, cybersecurity students can build a reputation for professionalism, integrity, and respect for the public interest.

The committee consulted existing ethical standards and codes in researching the proposed NCAE-C Student Code of Ethics and Professional Conduct. Organizations consulted: CompTIA, SkillsUsa, IEEE, ACM, ISACA, ISSA, ISC2, InfraGard, Montreat College Cybersecurity Oath, National Cyber League, AFA CyberPatriot, the National Collegiate Cyber Defense Competition, and ChatGPT.

Appendix 6. Annual Status Report, CAE-CD and CAE-CO Designations

This template is representative of the information collected in the Annual Status Report. The actual reporting tool will be automated, and will be available 31 October 2023. Designated institutions with more than two validated programs of study will be afforded space to account for all of them.

Institution Name	
Report Point of Contact	
Report POC email	
Report POC phone	
Report date	
Report academic year	
Designated PoS name	
Secondary Validated PoS	

Part 1. Metrics			
Designated PoS		Secondary Validated PoS	
Select one:	Degree ☐ Certificate ☐	Select one:	Degree ☐ Certificate ☐
Number of students enrolled		Number of students enrolled	
Number graduated/completed		Number graduated/completed	

Part 2. Critical Designation Elements				
• Selecting **Partial** requires a comment to explain why the item is not compliant and the institution's intention to meet the requirement. • Selecting **No** requires an explanation and a plan for how the institution will reach compliance in the next six months. The institution will be required to provide an update report six months after the submission date.	Yes	No	Partial	Comment
1. Requirements for the PoS Validation remain current				
2. Regional accreditation remains current				
3. Cybersecurity posture and plan is adequate & current				
4. The institution maintains and supports the established Center per original designation				
5. Outreach to the community and partners shares expertise and resources with others to improve the practice of cybersecurity in the community				
6. The institution has maintained and continues to expand Articulation and/or Transfer agreements with institutions offering a concentration of cybersecurity				
7. The NCAE-C Designation POC is a full time faculty member with influence over maintenance of the PoS.				
8. The alternate POC is a full-time employee of the institution associated with the Designation and PoS, such as a Dean, a Center Director, Faculty or other management position with expertise in cybersecurity.				
Part 3. Work Roles				
Three cybersecurity work roles from the NCWF or the DCWF that students completing or graduating from the validated PoS would be expected to pursue have been identified				
Ten competency statements (relating to curricular, co-curricular and/or extra-curricular opportunities) have been made available to students				

Appendix 7. Annual Status Report, CAE-R Designation

This template is representative of the information collected in the CAE-R Annual Status Report. The actual reporting tool will be automated.

Institution Full Name	
State Institution Located	
Report Point of Contact	
Report POC email	
Report POC phone	
Report Date	
Report Academic Year	
CAE-R Designated Program Name (List all)	
Part 1. Metrics	
CAE-R Designated Programs	
Number of students enrolled	
Number graduated/completed	

Part 2. Critical Designation Elements • Selecting **Partial** requires a comment to explain why the item is not compliant and the institution's intention to meet the requirement. • Selecting **No** requires an explanation and a plan for how the institution will reach compliance in the next six months. The institution will be required to provide an update report six months after the submission date.	Yes	No	Partial	Comment
1. A commitment letter signed by the leadership of the academic institution documenting awareness of the expectations and responsibilities associated with the CAE-R Designation is kept current with each change of administration.				
2. The institution has a Carnegie Foundation Classification level of R1, R2, D/PU or an NSA approval letter supporting CAE-R Designation.				
3. The institution continues to offer one or more doctoral degree programs which allow a research focus in cybersecurity.				
4. The institution has a minimum of four full-time faculty members, three of which are tenured or tenure track, who are conducting cybersecurity research and directly affiliated with the designated doctoral program(s).				
5. The institution continues to produce peer-reviewed papers in cybersecurity areas so there will be a minimum of 12 distinct cybersecurity-related research products that involve at least 3 tenured or tenured-tracked faculty members by the time the institution re-designates.				
6. The PhD enrollment in the cybersecurity-related doctoral programs average at least four per year with three or more graduates.				
7. The institution is able to show new and sustained research funding of at least two tenured or tenured-tracked faculty.				
8. There are at least two tenured or tenured-tracked faculty members associated with the designated doctoral program involved in external professional and scholarly service in cybersecurity-related research.				
9. The designation POC and the alternate POC have attended required conferences and meetings and evidence or documentation has been saved for the re-designation package.				

Appendix 8. Biennial Progress Report

This template is representative of the information collected in the Biennial Progress Report. The actual reporting tool will be automated, and will be available in 2024. Institutions will enter evidence or documentation of each item in the Program Development Tool; documentation will be compiled in the fifth year in preparation for the re-designation review panel.

Institution Name	
Designation POC	
Report Point of Contact (POC)	
Report POC email	
Report POC phone	
Report date	
Report academic year	
Designated PoS name	
Secondary Validated PoS	

• Selecting **Partial** requires a comment to explain why the item is not compliant and the institution's intention to meet the requirement. • Selecting **No** requires an explanation and a plan for how the institution will reach compliance in the next six months. The institution will be required to provide an update report six months after the submission date.	Yes	No	Partial	Comment
PoS Validation				
Syllabus for each course in the KU Alignment is correctly reflected in PoS documentation				
Overall Assessment Information for each Program-Level Learning Outcome PDF current				
Graduates from a CAE-validated PoS receive documentation that they have completed a NCAE-C designated program				
Students continue to participate in extracurricular activities per original designation				
Labs and other competency development are reflected in PoS documentation				
The three courses identified in the last designation where cyber modules are contained in the syllabus of courses other than the PoS department or college have not changed, or have been replaced by other/additional courses.				
The institution has integrated cyber concepts into courses and academic units (department or college) not included in the validated PoS				
Appropriate mechanisms are in place for detecting and addressing breaches of ethics or other misconduct				
If the NCAE-C Designation POC or alternate POC has changed since original designation, CVs for currently assigned POC/alternate POC have been provided to the NCAE-C PMO				

Biennial Progress Report	Page two: Institution Name			
	Yes	No	Partial	Comment
Participation Requirements: (para 2.1) Faculty members have contributed to CAE events and/or activities for the last two years (check all that apply). If none apply, enter means of participation. Annotate year and specific contribution in the comments section.				
Presented, moderated a panel, chaired a session, lightning talk, or workshop at the annual CAE Community Symposium, Executive Leadership Form, National Cybersecurity Education Colloquium, or other CAE Community or CAE Communities of Practice events				
Actively contributed to the CAE Community of Practice (CoP) activities by serving as a Steering Committee member, initiative co-chair or member of committees or Working Groups				
Hosted a GenCyber Program or other youth or teacher program/camp				
Contributed to outreach, competitions, and/or other activities led by NCAE-C institutions				
Developed and submitted a challenge, module, game, and/or provided feedback of student cyber competitions (name the competition)				
Served as PoS Validation and/or NCAE-C Designation mentor or reviewer				
Served as an active member of a CAE Working Group, a CAE Community Initiative, CoP Steering Committee and/or Initiative, or other significant role in the CAE Community.				
Collaborated with current NCAE-C institutions on research, grants, course development etc.				
Sponsored or advised students for cyber events such as cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community.				
Worked with employers and students to support placement for cyber related internships and jobs				
Collaborated with industry on work roles and curriculum development requirements.				
Maintenance of original designation requirements.				
Maintenance of original designation requirements (para 2.2.)				
The institution's regional accreditation is current				
The institution's cybersecurity posture and plan is adequate and current				
The institution maintains and supports the established Center per original designation				
Outreach to the community and partners shares with others to improve the practice of cybersecurity in the community				
Maintenance of original designation requirements continued from previous page				
The institution has maintained and continues to expand Articulation and/or Transfer agreements in cybersecurity				
The NCAE-C Designation POC is a full time faculty member with influence over the PoS.				
The alternate POC is a full-time employee of the institution associated with the Designation and PoS.				

Biennial Progress Report	Page three: Institution Name			
	Yes	No	Partial	Comment
Continuous Improvement (para 3.1.1 and 3.2.1)				
The institution has a plan and maintains a continuous improvement process for the Program Level Learning Outcomes				
The institution demonstrates a commitment to the growth of designated programs/PoS				
The institution actively integrates cybersecurity across disciplines in the institution				
Students who are not in cybersecurity programs of study have the opportunity to experience how cybersecurity applies to their field of study				
The institution works in the community to expand the practice of cybersecurity				
Competency (para 3.2.2)				
Designated PoS references (at least) three (3) work roles for which their graduating students will be best suited.				
Work roles are kept up to date				
First report: (Year 2 of designation): ten competency statements have been identified for each PoS, mapped to activities, and associated with the three work roles identified in year one. <u>At least five (5) of these are related to classroom activities.</u>				
Second report: (Year 4 of designation): 10 competency statements identified in year two have been implemented within each PoS.				
Second report: Student competencies are evaluated and documented for development and evidence of the institution's compliance with requirements.				
Second report: Student competencies are evaluated and documented for the student's portfolio and evidence for resumes or applications.				
Second report: Range of competency experiences available to students are continuously refined and expanded and identified through competency statements.				
Student Professionalism (para 3.3.)				
The institution can demonstrate and provide metrics on how students are introduced to cybersecurity ethics, work/life skills in demand in the workplace, and cybersecurity career pathways.				
Faculty Development (para 3.4.)				
The designated institution is proactive in opportunities for professional development for the faculty in cybersecurity. The institution can provide documentation and evidence of opportunities afforded faculty members, especially those associated with the designated PoS.				

Appendix 9. Re-Designation Requirements for 5th Year Panel Review

PoS Validation
Provide the Syllabus for each course in the KU Alignment
Provide the overall Assessment Information for each Program-Level Learning Outcome PDF
Provide an example of documentation provided to graduates/completers from a CAE-validated PoS
Describe students' continued participate in extracurricular activities per original designation
Provide documentation of labs and other competency development activities provided in PoS documentation
If the academic unit offers other Cybersecurity degrees, courses or programs of study, provide a short description of each degree or certificate option. (An academic unit, such as a college or department, 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.)
Document the three courses or cyber modules contained in the syllabus of courses other than the PoS academic unit.
Describe mechanisms in place for detecting and addressing breaches of ethics or other misconduct
If the NCAE-C Designation POC or alternate POC has changed since original designation, provide CVs for currently assigned POC/alternate POC
Participation Requirements: (para 2.1) The designation POC and/or the alternate POC have contributed to CAE events and/or activities every year for the last five years. Provide documentation for the items below that apply. If none apply, provide evidence of other means of participation. Ensure date (with year) is annotated for each contribution.
Provide evidence that the designation POC, other faculty, or permanent staff presented, moderated a panel, chaired a session, lightning talk, or workshop at the annual CAE Community Symposium, Executive Leadership Form, National Cybersecurity Education Colloquium, or other CAE Community or CAE Communities of Practice events.
Provide email, letter or other evidence of contribution to the CAE Community of Practice (CoP) activities by serving as a Steering Committee member, initiative co-chair or member of committees or Working Groups.
Provide evidence of hosting a GenCyber Program or other youth or teacher program/camp.
Document contributions to outreach, competitions, and/or other activities led by NCAE-C institutions.
Provide evidence or link to a challenge, module, or game developed for NCAE-C competition(s).
Provide copy of feedback provided on student cyber competitions (name the competition)
Indicate years of service as a PoS Validation and/or NCAE-C Designation mentor or reviewer
Provide information on contributions to a Group, a CAE Community Initiative, CoP Steering Committee and/or Initiative, or other significant role in the CAE Community.
Provide documentation of collaboration on research, grants, or course development with other NCAE-C institutions.
Document sponsorship or advisory contribution to students for cyber events such as cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community.
Document collaboration with employers and students to support placement for cyber related internships and jobs.
Document collaboration with industry on work roles and curriculum development requirements.
Maintenance of original designation requirements (para 2.2.)
Provide documentation of the institution's regional accreditation.
Provide a copy of the institution's cybersecurity posture and plan, OR provide evidence the plan is adequate and current. This could be a letter or other document from the executive responsible for the institution's cybersecurity.
Provide a letter from the President or other executive in authority to testify to the institution's commitment to maintain and support the established Center per original designation.
Document outreach to the community and partnership with local schools, governments or others to improve the practice of cybersecurity in the community.
Provide evidence the institution awards credit in cybersecurity related courses and/or technical prerequisite courses from other academic institutions, community colleges, tech schools, etc. or through alternative means, such as transfer agreements with other academic institutions, articulation agreements, statewide transfer agreements, college in the high school, dual credit, running start, credit for prior learning, credit for military training or occupation, and/or membership in Transfer Evaluation Services (TES).

Continuous Improvement (para 3.1.1 and 3.2.1)
Provide evidence of how the institution demonstrates a commitment to the growth of designated programs/PoS
Provide the plan for continuous improvement process for the Program Level Learning Outcomes.
Provide records of the continuous improvement process, assessments, and the documented plans for improvement; submit as part of the annual reports and at re-designation.
Provide documentation of how the institution actively integrates cybersecurity across disciplines in the institution.
Provide evidence of how students who are not in cybersecurity programs of study have the opportunity to experience how cybersecurity applies to their field of study.
Describe how the institution works in the community to expand the practice of cybersecurity.
Competency (para 3.2.2)
Provide PDF(s) documenting three (or more) work roles.
Document how the three work roles associated with the PoS are shared with students.
Provide the ABCDE Essential Elements framework mapping for each of 10 competency statements. Identify which five of these competency statements are mapped onto specific tasks associated with the identified three work roles.
Document how these competency statements are shared with students.
Provide assessment results for the five cybersecurity competencies for students who are enrolled in the Validated PoS **during the past three academic years**.
Provide PDF for five competency statements relating to co- and/or extra-curricular activities accessed through PoS.
Describe each competency experience available to students.
Describe how the range of competency experiences made available to students are continuously refined and expanded and identified through competency statements.
Student Professionalism (para 3.3.)
Demonstrate and provide metrics on how students are introduced to cybersecurity ethics, work/life skills in demand in the workplace, and cybersecurity career pathways.
Faculty Development (para 3.4.)
Document opportunities for professional development provided for the faculty in cybersecurity, especially those associated with the designated PoS. Include the frequency of opportunities.
Provide documentation of which professional development opportunities the faculty associated with the PoS have attended or experienced.

Appendix 10: Consequences for Failure to Comply

Maintenance of correct contact information in the Program Management Tool is critical to an institution's maintenance of requirements compliance; ***the PMO will only provide notifications of grants opportunities, upcoming events, and other news to the individuals recorded in the tool.***

Failure to Submit Reports

NCAE-C reporting requirements, both the Annual Status Report (para 4.1.) and the Biennial Re-designation Progress Report (para 4.2.) are critical to the success, growth and efficacy of the NCAE-C program. Metrics are used to provide return on investment information to program supporters, and to plan for future growth, development and policies for the program. The Biennial Re-designation Progress Report will be an integral part of the process for re-designation. Adherence to this process will simplify the fifth year review. Institutions that repeatedly fail to provide timely and accurate reporting will not be granted any waivers or continuation of designation should they fail to meet requirements in the fifth year.

If either the Annual Status Report or the Biennial Progress Report are not submitted on dates assigned by the PMO, a message is automatically sent to the POC's supervisor or the appropriate Dean. See Appendix 10, Table 1 for time-dependent consequences.

Time of submission	Consequences
Submit required 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	Day 31 a message is sent to the President, cc to Dean
After 45 days	Day 46 the President is notified the institution is on probation.
After 60 days	Day 61 the Designation is suspended and the President is notified.
Over 90 days	The PMO will annotate the suspension on the public list of designated institutions.
Over 120 days	The designation is rescinded; the President is notified. The PoS Validation remains independently valid; requires re-validation every five years according to Candidates Program requirements.

Appendix 10, Table 1

Failure to Comply with Assigned Re-Designation Cycle

With the continued growth of the NCAE-C program, it is necessary for designated institutions to comply with assigned re-designation cycles and review panels. The PMO will work with institutions needing time or exception to the process, but this must be negotiated when the due dates are assigned.

The program operates year round, and assigned dates may fall during the summer break. The PMO understands that faculty may not be on campus during the summer, but the process is designed so that documentation and process is accomplished over the entire five years of designation. While the PMO will make every effort to avoid scheduling a Re-Designation Review Panel between Jun and August, this may not always be possible.

When the institution submits the second Biennial Re-Designation Progress Report, the NCAE-C PMO will **assign the institution to a Review Panel cycle**. In the fifth year the institution will ensure documentation and evidence to support the self-reviews conducted in the first four years is available to submit for re-designation. This documentation and evidence will be collected in the Program Management tool and must be available to the

Review Panel six weeks prior to the Review Panel meeting date. Failure to submit the required documentation on the due date assigned by the PMO will trigger a message to the POC's supervisor or the appropriate Dean. See Appendix 10, Table 1 for time-dependent additional consequences.

Failure to respond within 15 days to PMO assignment of re-designation cycle.	When the PMO assigns an institution to a review cycle the designation POC is required to acknowledge and agree to the assignment, or submit a request for modification. The PMO will include the alternate POC and the POC's supervisor in the notification. Failure to respond will result in probation until the institution acknowledges the assignment. Notification of probation will go to the President, copy to the Dean and POC.
Submit required re-designation information on or before the due date, six weeks prior to the Review Panel	If the required information is not submitted on time, a message is automatically sent to the POC's supervisor or the appropriate Dean
If there is no response after 7 days	Day 8 a message is sent to the institution President, cc to Dean
If there is no response after 14 days	Day 15 the President is notified **the institution is on probation**. Because the Review Panel members will not have time to review the re-designation documentation, the institution will be offered re-assignment to the next available Review Panel. This could take months. The institution will remain on probation until the re-designation is completed.

Appendix 10, Table 2

Probation. The institution returns to good standing when the non-compliance is resolved.

- Faculty/POC/staff are ineligible for travel assistance to NCAE-C sponsored events during the period of probation.
- The institution is ineligible for Grants or Scholarship solicitations issued by the PMO during the period of probation

Suspension. Suspensions are automatically at least 30 days. Probation restrictions apply. Institutions in a suspension status will meet a PMO-chaired review panel to investigate reasons for the suspension, and current eligibility for designation before returning to good standing.

- The institution will remove all references to NCAE-C Validation and/or Designation from all electronic materials and websites.
- Should the institution hold a current NCAE-C grant, the grant will not be eligible for any proposed option years.
- Institutions in probation for more than 30 days will not be eligible for grants for a one year period.