National Centers of Academic Excellence in Cybersecurity

NCAE-C 2026

Designation/Re-designation Requirements and Application Process

For

CAE-Cyber Defense (CAE-CD)

Prepared by the

2026 Application Process and Adjudication Rubric (APAR)

Cyber Defense Working Group (CDWG)

June 2026

Effective Date: January 2027 (Beginning with Cycle Assignment 30)

20260605_CAE2026_ CAE-CD_Designation_Requirements_Ver2026

This publication was partially supported by the NCAE-C Candidate National Center at Whatcom Community College, under Department of War (DoW) award number HQ0034251E016 and NSA award number H98230-22-1-0331.

OVERVIEW

The following is an overview of the requirements for Designation and Re-designation in the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program for **Cyber Defense (CD)** administered by the National Security Agency (NSA) - NCAE-C Program Management Office (PMO), under the leadership of the United States Department of Defense (DoD) Office of the Chief Information Officer (CIO) - Cyber Academic Engagement Office (CAEO). Details on requirements and application processes are provided in the body of this document. **The CAE Cyber Defense (CAE-CD)** Designation is awarded to degree-granting regionally accredited academic institutions offering cybersecurity-related degrees including majors, minors, and/or certificates at the Associates, Bachelors and graduate levels. Applicant institution must demonstrate that it engages in significant community involvement, academic activities, and institutional practices in cybersecurity, and that the institution has one or more Program(s) of Study (PoS) under consideration meeting the requirements set forth in this document. The goal of the NCAE-C program is to promote and support quality academic programs of higher learning that help work to prepare the nation's cyber workforce. Re-designation and PoS re-validation are required every five years.

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 Program include:

- Shared governance
- Maintain/improve NCAE-C Program standards
- Focus on output (workforce) in cybersecurity
- Recognize 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-increasing excellence so that America can maintain its competitive edge in cybersecurity. "To offensively and defensively defend our network, our information systems, and our data in order to protect a wide range of critical services, we must have a knowledgeable and skilled DoW Cyberspace Workforce that can adapt to the dynamic cyber environment and adjust resources to meet mission requirements" (DoW Cyber Workforce Strategy 2023-2027, 2023, p. 5)

Version and Effective Date

This Designation/Re-designation Requirements and Application Process For CAE-Cyber Defense (CAE-CD) document is version 2.1 (May 2026) and effective January 15, 2027. Please refer to Appendix 5 regarding changes from prior version 2.0 (June 2025).

TABLE OF CONTENTS

INTRODUCTION TO THE CAE-CD APPLICATION PROCESS

Degree-granting academic institutions in the United States (U.S.) wishing to be designated a **National Center of Academic Excellence in Cybersecurity (NCAE-C) in Cyber Defense (CD)** (aka "CAE-CD Designation") for a particular program of study will apply in two parts. The following process applies to both Program of Study (PoS) Validation and CAE-CD Designation. If required, in Step 5 (Figure 1), the applicant appears before the Review Committee or addresses the committee's Request for Information (RFI) messages via the tool and/or email. Only U.S. academic institutions are eligible to apply to the NCAE-C program.

- **CAE-CD Program of Study (PoS) Validation:** The process will begin with the submission of elements pertaining to the academic program of study, including curriculum, student related information, faculty profiles and qualifications, and continuous program improvement information. An institution may opt to have multiple programs of study validated before pursuing Designation, or may achieve Designation with one PoS and return to have additional PoS(s) validated.
- **CAE-CD Designation:** Once one PoS has been validated, the institution may pursue a CAE-CD Designation. To be eligible for CAE-CD Designation, the academic institutions must hold a current regional accreditation as outlined by the Department of Education (https://www.ed.gov/accreditation), and be able to demonstrate all requirements indicated for CAE-CD Designation. While multiple PoS Validations per academic institution are allowed, no duplicates of any CAE-CD Designation type are allowed.

This process and submission timeline apply to both an application for Program of Study (PoS) Validation and to an application for CAE-CD Designation.

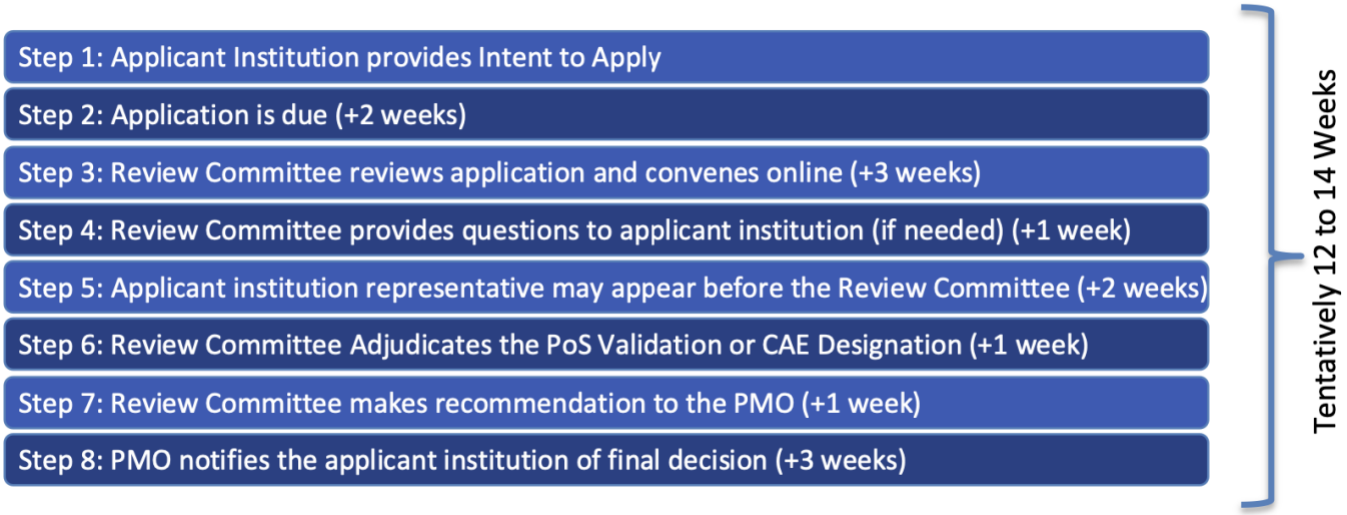

Figure 1. Tentative PoS Validation or CAE-CD Designation Application Process and Submission Timeline

Timelines for submission will be published by the CAE Candidates National Center (CCNC) and cycle assignments are evenly distributed throughout the year. The PMO will make available an automated application tool to collect all required documentation and data. The application tool will collect required metrics and allow uploading of required documentation. All required documentation and data should be available prior to applying. Applying institutions will be assigned to a submission cycle and expected to follow the deadlines indicated in the cycle timeline provided. **Institutions that miss their cycle deadline(s) may be removed from applicant processing and the institution would need to resubmit a checklist to express their interest in continued processing. Removal from applicant processing may impact Validation and/or (Re)designation status.** See Table 1 below for consequences of failure to adhere to application deadlines and related definitions of ***probation*** and ***suspension*** status.

Table 1. Consequences of Failure to Adhere to Cycle Assignment Application Deadlines

Requirement	Consequence
Submit application(s) on or before the due dates in accordance with the Cycle Assignment.	Institutions are required to acknowledge and agree to the cycle assigned by the CAE Candidates National Center. Failure to submit the application(s) in accordance with the cycle assignment timelines, **without prior communication/approval to/from the PMO/Peer Review National Center (PRNC) Director**, may result in removal of processing and require a justification and/or new applicant checklist to confirm intent to re(apply) for Validation and/or Designation. This may impact an institution's Validation and/or Designation status including for re-designating institutions.
Failure to submit by assigned due date:	
- After 15 days:	PMO will send a message to the Point-of-Contact (POC), alternate POC, and Dean to notify them that the institution has been placed on **Probation** (see definition below) AND request justification for failure to adhere to the timeline. Upon review, institution may be reassigned to a new cycle. Note: Cycle reassignments will be handled on a case-by-case basis.
- After 45 days:	PMO will send a message to the POC, alternate POC, Dean, and President to inform them of removal of processing. In the event the Validation/Designation is not active, institution will no longer be in good standing and be placed on **Suspension** (see definition below).
Definitions:	
Probation	• 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. • Institutions in **probation status for more than 30 days will not be eligible for grants for a one year period.**
Suspension	• Suspensions are for a minimum of 30 days. Probation restrictions apply. The institution will **remove all references to NCAE-C** Validation and/or Designation from all electronic materials and websites which includes all logos (NSA, Federal Partners, CAE Community): • Should the institution hold a current NCAE-C grant, the grant will **not be eligible for any proposed option years**.

Qualified cyber professionals and Subject Matter Experts from NCAE-C Academic Institutions and the National Security Agency (NSA) will assess applications. By submitting an application, an institution grants consent to having its application reviewed by assessors approved by the NCAE-C PMO. Institutions not fully meeting all requirements will be provided with a set of questions and/or further clarification requests and given an opportunity to respond to the Review Committee's questions. If needed, the POC will be asked to appear before the Review Committee for further clarifications, followed by a final notification from the PMO (see Figure 1). Each PoS will need to have a designated POC, which may or may not all be the same individual and may or may not be from the same academic unit or department. The CAE will need to have a designated POC who is the person in charge of the established "Center" for cybersecurity at the academic institution (see NCAE-C Designation Criteria No. 4). Mentoring and initial approval of all pre-submission material are required in order to be granted access to the application tool. The first POC from each academic institution submitting a PoS for Validation is expected to "mentor" additional POCs (if applicable) from that same academic institution on PoS Validation requirements. In the case of an academic institution with NCAE-C Designation, the NCAE-C POC should serve in that capacity and be kept aware of all newly submitted PoS for Validations. The PMO will not provide multiple mentors to an institution and expects that POC to 'lead-by-example' within their institution. Incomplete applications will be returned without comment. Designation as a NCAE-C does not carry a commitment of funding.

Justifications

Throughout the application process, both in the PoS Validation and CAE-CD Designation, applicant institutions are provided an optional feature in the application tool to attach a justification file (in one PDF) that they deem needed to clarify issues during the review process.

Synergistic Approach

To achieve NCAE-C status, the institution should demonstrate a synergistic approach involving a proper environment for academic excellence, and faculty and courses to drive Program-Level Learning Outcomes (see Figure 2). A significant factor contributing to the institution's academic effectiveness and credibility will stem from its regional or higher-level accreditation. The synergistic approach builds upon existing institutional foundations as driven by regional accreditation rather than duplicating or supplanting them.

Figure 2. The Synergistic Approach Needed to Become NCAE-C

CAE-CD Requirements Document Annual Review

The PMO, in collaboration with Academic Working Group (WG) from CAE-CD institutions, will conduct an annual review and update (if needed) of the CAE-CD Requirements Document. The CAE-CD Requirements Document Academic WG will consist of reviewers and/or mentors with extensive experience with the CAE-CD requirements. The estimated timeline is shown below:

	JANUARY	MARCH	APRIL	JUNE
	CD ACTION KICK OFF	FEEDBACK DUE	UPDATE DUE TO PMO	FINAL PUBLIC RELEASE
Activities				
	PMO will notify CD WG Co-Chairs of the annual review	Feedback from CD WG due to Co-Chairs and PMO	Co-Chairs will consolidate input in Draft version	PMO will send out updated Requirements Document to CAE-CDs
	Conduct initial review and update before action to WG	PMO and CD WG Co-Chairs will review feedback from the working group	PMO will send updates to CAE-CD institutions for awareness/final thoughts (2 weeks)	PMO will notify Candidates and Peer Review National Centers of the updates for inclusion into training documentation
	Identify Academic WG members (no more than ~30 members)		WG members will support additional review and provide feedback based upon input	
			PMO will determine Cycle effective date, based upon the revision	

Figure 3. The CAE-CD Requirements Document Annual Review Timeline

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 that holds current regional accreditation as outlined by the U.S. Department of Education (https://www.ed.gov/accreditation). Validation and/or Designation is approved only for the individual campus in which applies.

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.

A ***Program 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.

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 institutional ***Point-of-Contact (POC)*** is a designated full-time/permanent faculty member of the institution directly involved with the representative academic program from the applying institution who will serve as the liaison between the institution and the NCAE-C Program Management Office (PMO). This person will be contacted by the PMO and/or the National Centers for all NCAE-C program updates, grants and scholarship opportunities, upcoming events, and other administrative communications. This person is responsible for the Annual Report, Re-designation, and any other important milestones in the institution's NCAE-C participation.

An institutional ***Alternate POC*** is an individual who is a full-time/permanent employee in a professional capacity (not an administrative assistant personnel) and is a secondary contact to the POC. This person may be a Department Chair, an Associate Dean, a "Center" or Program Director, or a Dean.

Competency is the ability of the individual to complete a task in the context of a work role.

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.

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).

Curriculum Map and Plan (Noted in green in Figure 4): 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.

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.

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

KU Alignment (Noted in purple in Figure 4): the process of documenting how the KUs and KU outcomes are aligned to the relevant courses in the PoS.

Continuous Program Improvement (Noted in blue in Figure 4): 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 Program 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 Program Improvement Process: documentation of the continuous program improvement plan executed and evaluation of the results of the current continuous program improvement plan.

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

PART I: PROGRAM OF STUDY (POS) VALIDATION REQUIREMENTS FOR CAE-CD

Overview

The Program of Study (PoS) Validation requirements for NCAE-C – Cyber Defense (aka "CAE-CD") programs include evidence presented in a Self-Study that all academic institutions will submit in the application tool. Academic institutions will be required to provide detailed information related to faculty, student, curriculum, and continuous program improvement. 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 *mapped* to the courses in the PoS. Moreover, the Self-Study will include documentation of the identified KUs for the PoS and the *alignment* of the KUs to the relevant courses in the PoS. Figure 4, the CAE-CD PoS Validation Conceptual Model, provides a graphical representation of the: (1d) Curriculum Map and Plan courses with associated documentation, the (1e) KU alignment courses, and (4) Continuous program improvement plan, process, and evaluation schedule. The examples provided are to be used as illustrations or guides, they are not intended to be a complete assessment of a PoS. **No elective courses should be indicated in the KU alignment**, as all students should successfully complete all courses indicated in the KU alignment.

Self-Study Overview

A documented Self-Study is required for all CAE-CD applications. It includes the following requirements (see Appendix 3 for relevant examples):

1. PoS Curriculum

a) The cybersecurity PoS offered by the institution
b) Cybersecurity work roles crosswalk alignment
c) Courses 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 (see Appx. 3)
f) Graduate thesis/dissertation/equivalent guidelines and process (masters and doctoral programs only)

2. Students

a) Student enrollment/graduation in the PoS(s)
b) CAE-CD: Sample student certificate/notation on transcript/official letter
c) Students' work products (papers, assignments, labs, etc.)
d) Student competency development and ethical conduct

3. Faculty Members

a) Cyber program(s) of study PoC
b) Full-time, part-time, and adjunct faculty members + Faculty qualifications (publications, research, industry involvement, certifications, etc.) related to PoS type
c) Faculty support of enrolled students
d) Process of faculty promotion/reappointment (e.g., faculty policy manual)

4. Continuous Program Improvement

a) Continuous program improvement plan
b) Continuous program improvement process
c) Regular evaluation schedule

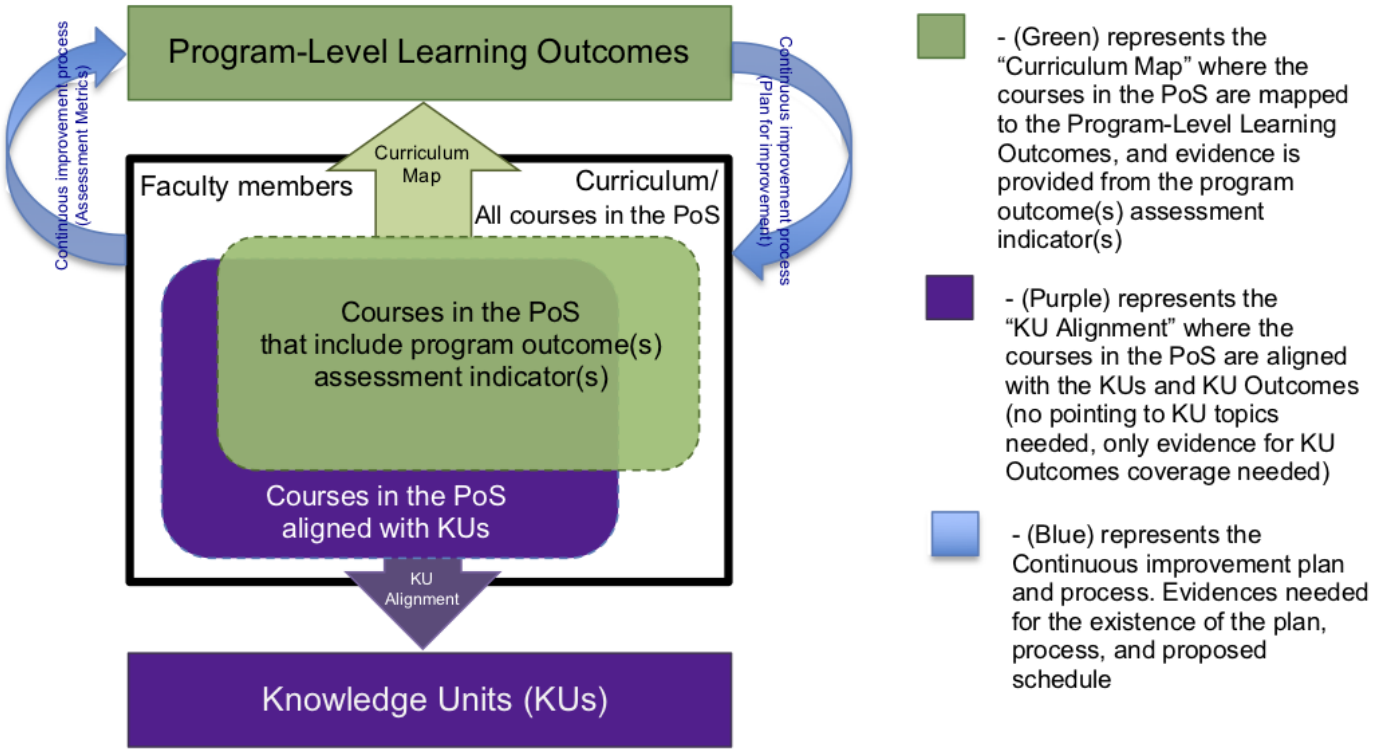

Figure 4. PoS Validation Conceptual Model

Institution Details

The applicant will identify and/or confirm the official initial institution details in the application tool.

Requirements:

- Identify/confirm the official institution name
- Identify the Office of Postsecondary Education (OPE)-ID (https://ope.ed.gov/dapip/)
- Provide link to the homepage of the institution (not department)
- Provide the address of the institution
- Provide contact information for institution President

Additional Information for Grant-Related Opportunities (Not guaranteed):

Applying academic institutions may provide additional evidence of eligibility for NSA grants for the benefit and ease of applying for grants. Doing so will allow DoW and NSA to identify potential NCAE-C institutions for grant solicitations. Specifically, applicants may need to consult their Office of Sponsored Programs, Research Office, the office which will handle any grant submission for the institution, or other entity that administers their grants to obtain a copy of the most recent A-133 Summary of Auditor's Results, DUNS, Cage Code, and Employer Identification Number/Tax Identification Number (TIN#) to ensure the correct numbers are being provided. This same office/entity may have the proofs of the most recent A-133 Summary of Auditor's Results, SAM and ARC registrations (Proof of SAM and ARC registrations may be a simple email from the organization, or a screenshot of the registration).

Information Needed (Optional):

- Provide a copy of the most recent A-133 Summary of Auditor's Results (in PDF)
- Provide the DUNS number
- Provide the CAGE Code
- Provide the Employer Identification Number/Tax Identification Number (TIN#)
- Provide proofs of the SAM and ARC registrations (in PDFs)

Program(s) of Study (PoS) Validation Requirements

1. PoS Curriculum

A U.S. institution of higher education will first apply by submitting an academic program for Program of Study (PoS) Validation. The academic institution must show its curriculum and show that students are enrolled and successfully complete the path and receive recognition. A single academic institution may have multiple PoSs validated, but only one is required to proceed to CAE Designation. All institutions applying for PoS Validation must be a U.S. institution and regionally accredited.

NOTE: Maintenance of the validated PoS is a condition for the CAE Designation. While institutions are expected to update and improve curriculum and PoS elements for the purposes of remaining current with technology and practice, and to demonstrate continuous program improvement, any courses or curriculum elements used to satisfy KU alignment requirements must remain aligned to those KUs to maintain Validation, and thence to maintain Designation. **If designated institutions wish to change a course or KU-aligned curriculum elements, two options are available:**

a. Make changes to courses and curriculum elements used in a validated PoS, taking care that the changes maintain the KU alignment.
b. Pursue and receive Validation of a second PoS that qualifies for CAE-CD, and after receiving the second Validation, make changes to the original PoS that may change the KU alignment. This preserves the requirement that designated institutions have at least one validated PoS. The institution may then make the desired change to the validated PoS and re-submit for Validation aligned to different KUs.

PoS is defined as sets of courses that are designed to develop Program-Level Learning Outcomes in the student population over time. It is possible to have multiple cybersecurity PoSs at an academic institution, in different departments, providing students with different knowledge and skills. Degree plans or Program plans can document the options available to a student and form a basis for determining the correct path. Program sequence diagrams that define the relationship between courses (prerequisites) can be useful in assisting students as they navigate the classes. Cohorts are another mechanism that can assist in the navigation of program plans. Transcripts, or other institutional completion records, can document student completion of validated PoS.

CAE-CD Designations have a requirement to align courses to NCAE-C Knowledge Units (KUs) and provide a Curriculum Map and Plan (see Figure 4). The application tool will simplify the KU alignment as well as the Curriculum Map and Plan submission process. The Cybersecurity Work Roles Crosswalk Alignment is the link between the NCAE-C program and the cybersecurity workforce, and is the means by which the PMO communicates to employers and potential students which PoS may most closely match their hiring requirements or study interests. Graduate programs (Masters and Doctoral) should provide evidence of institutional documentation for thesis, dissertation, graduate project course, and/or graduate experiential learning course.

a. The Cybersecurity PoS offered by the institution

The applicant will identify the official title of the cybersecurity PoS offered by the institution and the academic leadership relevant to that PoS. Courses identified in the *Curriculum Map and Plan* as well as the *KU Alignment* must be mandatory for all students completing the PoS. If the application is approved, only the PoS identified in this criterion is allowed to be marketed as a validated PoS. An applicant shall not make reference to NCAE-C on their website or other promotional materials until the applicant receives official approval of the application for NCAE-C Designation. To initiate the application, the applicant will first need to identify the cybersecurity type PoS offered by the institution (CAE-CD-Associate, CAE-CD-Bachelor, CAE-CD-Masters, CAE-CD-Doctoral), identify if the CAE-CD PoS is a *Technical* or *Non-Technical* PoS (refer to section 1e for proper KU alignment), and state the official title of the cybersecurity PoS.

Requirements (All required):

1. State the official program title of the cybersecurity PoS (including: degree level, if applicable, minor, concentration, certificate). If validated, the PoS title will be displayed on a NCAE-C website list, thus, it must be the official program title (Examples: AAS in Computer Technology with a Cybersecurity Certificate; BS in Cybersecurity; BS in Computer Science with Cybersecurity Minor; MS in Information Technology with concentration in Cybersecurity Management; Ph.D. in Cybersecurity Management). ***State **only** the official program title of the PoS as found in the institution's published catalog. The text provided will be printed on the Validation/Designation certificate, if approved. Do NOT include any other text aside from the official program title of the PoS in this field ***
2. Provide a link to the institutional webpage where the PoS is documented (i.e., provide the URL to program's course catalog, curriculum webpage, etc.).
3. Identify department(s) official name(s) as it appears in the accreditation where PoS resides.
4. Academic institutions applying for original Designation (not Re-designation) will affirm that PoS curriculum has been in existence for at least three (3) years and has one (1) year of students that have completed the PoS curriculum at the time of submission. This ensures the PMO that the applicant PoS has reached a level of maturity and has the continuing support of the Institution. Academic institutions currently designated CAE-CD applying for Re-designation have already met this requirement, and will, for the purposes of Re-designation, annotate any changes to the original PoS and ascertain that all changes maintain the original KU alignment OR will identify an alternate validated PoS that meets this requirement.
5. Identify the administrative head of the academic unit housing the PoS (Dean, Associate Dean, Department Chair, etc.) including name, phone number, and e-mail address.
6. List the courses from the PoS that are part of both:
    a. All courses in the Curriculum Map and Plan that are used to assess the Program-Level Learning Outcomes (Course Number/Course Name/Course Descriptions as appears in the catalog, excluding General Education courses) (identify the KU aligned courses in this list); **and**
    b. All courses that are part of the KU alignment.
7. Provide evidence for PoS Curriculum Sheet in PDF (see Appendix 3 - Example 1a).

b. Cybersecurity Work Roles Crosswalk Alignment

The applicant will state three cybersecurity work roles from the DoD Cyber Workforce Framework (DCWF) (https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework) and/or NICE Workforce Framework for Cybersecurity (NIST Special Publication 800-181, https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center) that are most relevant to their applying or re-designating PoS. DCWF establishes the DoD's authoritative lexicon based on the work an individual is performing. It describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive 8140.01. The NICE Workforce Framework for Cybersecurity (NICE Framework) provides a common language to describe cybersecurity work and the knowledge and skills required to complete that work. While an applying institution may consider its PoS to produce graduates in many work roles, this criterion calls for the three work roles that are the most relevant to that PoS. The identified cybersecurity work roles should be aligned with the type of courses (curricular experiences), as well as other co-curricular and extracurricular experiences that students are engaged in through the PoS. The identified cybersecurity work roles inform the development of competency activities that provide the students with an opportunity to complete a task(s) from these work roles. By providing students with activities clearly aligned to tasks within cybersecurity work roles (see section 2d below), institutions inform students about their career choices, prepare them for job applications and interviews, and increase their competitiveness in the workforce. Building the crosswalks between the PoS and three work roles 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 contribute to building the competencies of PoS graduates in alignment with government and industry needs.

Requirement:

1. Identify three (3) distinct work roles from the DCWF and/or the NICE Framework that align with closest relevance to the applying or re-designating cybersecurity PoS. Institutions may choose distinct work roles from either framework or both, depending on their program's focus.

c. Course Syllabi and Courses Requiring Applied Lab Exercises (For KU Aligned Courses Only)

The applicant will provide syllabi of all courses in the KU Alignment (see section 1e below) and identify those that require applied labs exercises (hands-on) that develop competencies in the cyber domain, provide lab exercises guidelines and highlight lab requirements in the syllabus. A typical course syllabus includes the official name and number of the course, the term it is offered, who teaches the course, the textbook(s) assigned, relevant course information (course descriptions, course learning outcomes, etc.), supplemental material (if applicable), course topic coverage outline and/or a weekly/module schedule to indicate list of lectures, topics/reading, assignments, labs assigned, course grade components, and grading scale/system.

Requirements (All required):

1. Provide a concise syllabus of each course in the KU Alignment (all must be from the last three (3) years and properly labeled with the term in which the course was taught and faculty name) (in PDF).
2. For KU aligned courses that require applied lab exercises (i.e., hands-on labs that develop competencies) in the cyber domain, highlight the lab(s) on the syllabus, and highlight in which unit/week the lab(s) are required for the lab(s) provided (all must be from the last three years). A minimum of three (3) distinct KU aligned courses are required to have hands-on labs.
3. Provide the guidelines (i.e., what students are asked to do) of one lab exercise from each course that requires applied lab exercises and indicate within the guidelines the course that each lab is used (all must be from the last three years, a minimum of three (3) labs from three distinct KU aligned courses are required) (in PDF).

d. Curriculum Map and Plan with Assessment Documentation

Program-Level Learning Outcomes are the basis for determining the effectiveness of a NCAE-C program in developing the cybersecurity workforce. Each PoS should have a defined set of Program-Level Learning Outcomes as documented by the academic institution to the regional (or other) accreditation. The number of Program-Level Learning Outcomes may vary depending on the academic institution and level of the program. The Program-Level Learning Outcomes are the basis for continuous program improvement efforts. No elective or optional courses should be included in the Curriculum Map and Plan, as all students should take all courses used to assess the Program-Level Learning Outcomes.

Requirements (All required):

1. State the Program-Level Learning Outcomes of the PoS.
2. Provide documentation of the Program-Level Learning Outcomes (link to academic institutional webpage with the outcomes and/or PDF document of the outcomes).
3. Provide evidence for the Program-Level Learning Outcomes *Curriculum Map and Plan* that identified the PoS courses where the outcomes are assessed (Combined to a single PDF) (see Appx. 3 example 1d1).
4. Provide documentation for the *General Information* for each Program-Level Learning Outcome (Combined to a single PDF). For each Program-Level Learning Outcome, "General Information" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Term it was assessed (if completed); (c) Course(s) used for the assessment; (d) Total number of assessed students (see Appx. 3 example 1d2).
5. Provide documentation for the *Assessment of Indicators* for each Program-Level Learning Outcome (Combined to a single PDF). For each Program-Level Learning Outcome, "Assessment of Indicators" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Course used for the assessment; (c) Program outcome assessment indicator(s) used to assess the Program-Level

Learning Outcome (assessment metric(s)); (d) Performance expectations; (e) Average assessment score for the assessed students; (f) overall performance rating of assessed students (see Appx. 3 example 1d3).

6. Provide documentation for the *Overall Assessment Information* of each Program-Level Learning Outcome (Combined to a single PDF). For each Program-Level Learning Outcome, "Overall Assessment Information" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Course used for the assessment; (c) Program outcome assessment indicator(s) used to assess the Program-Level Learning Outcome (assessment metric(s)); (d) Overall performance rating of assessed students; (e) Qualitative analysis of the assessment results; (f) Qualitative statement/plan for improvement(s) resulting from the assessment; (g) Indication of when the recommended improvement(s) are projected to be implemented (see Appx. 3 example 1d4).

e. Knowledge Units (KUs) Alignment

The NCAE-C program will rely upon the institutional accreditation for sufficiency of program construction and maintenance. Courses, or other academic elements, should be institutionally approved per the institutional requirements for accreditation and aligned to the KUs. The PoS content as demonstrated by KU alignment will be used to determine if the courses together as a whole constitute sufficient material in quantity and form. All CAE-CD programs need to cover the foundational, appropriate core, and required optional KUs per academic program type (Certificate, Associate, Bachelors, Masters, or Doctoral) as indicated in Figure 5. **No elective or optional courses should be included in the KU alignment, as all students should take all courses indicated in the KU alignment.** One course may align with one or more KU(s), however, a course should not be aligned to an excessive number of KUs given the challenge of so many KU Outcomes covered within a single course. For example, typically one course should not be aligned to more than five (5) KUs. One KU may align to multiple courses, however, this is not recommended. KU alignment is only needed for courses that are identified for alignment with the KUs. Course learning outcomes will also be aligned (as a set) to the relevant KU(s), while the KU Outcomes will be shown (as a set) to provide guidance on the coverage (see Appendix 3 - Example 1e1). As part of the application, the academic institution will provide information on the academic year that each of the KU aligned course was last offered. Additionally, the academic institution will provide explanation on how they manage multiple sections of the KU aligned courses in some form of equivalency.

Requirements:

1. Provide a narrative on the description of the PoS, explain the overall KU alignment to the PoS.
2. For graduate programs (MS or Doctoral) that seek exemption from the three (3) Foundational KUs and five (5) Technical or Non-Technical Core KUs, provide evidence that students are admitted with the foundational and core knowledge.
3. Provide the KU Alignment Summary Table for the PoS (in PDF) (see Appendix 3 - Examples 1e2).
4. Identify PoS courses that are part of the KU alignment.
5. Provide *course learning outcomes* for all KU aligned courses as documented in official academic institution documentation (Course catalog, program website, etc.).
6. Provide the academic year each KU aligned course was last offered.
7. In the case of multiple sections of a KU aligned course, provide explanation on how they all are managed to ensure consistent student learning outcomes are met. If no multiple sections offered, provide a statement to attest to that.

CAE-CD PoS Validation KUs:

The core or other set of PoS courses that all students in the PoS attend are aligned to chosen KUs (see Figure 5. CAE-CD KU requirements below for each degree level).

Appendix 1 provides a list of **Required and Optional Knowledge Units for the CAE-CD Program**. The full list and details on each KU can be found at: https://www.cyber.mil/ncae-c/document-library. *Appendix 2* provides an overview of the **KU Alignment Requirements for CAE-CD**.

1. **Associate Programs align to a total of 11 KUs consisting of:** three (3) Foundational KUs, five (5) Technical or Non-Technical Core KUs, and three (3) Optional KUs (see Figure 5).

2. **Bachelors Programs align to a total of 22 KUs consisting of:** three (3) Foundational KUs, five (5) Technical or Non-Technical Core KUs, and 14 Optional KUs (see Figure 5).
3. **Masters Programs align to a total of 22 KUs consisting of:** three (3) Foundational KUs, five (5) Technical or Non-Technical Core KUs, seven (7) Optional KUs, and additional seven (7) KUs for thesis and/or institutional equivalent (i.e., graduate project or experiential learning course in lieu of seven (7) additional KUs) **or** align to 22 KUs (3 Foundational, 5 Core, 7 Optional, & 7 Additional, see Figure 5). Graduate programs must provide evidence that their students are admitted with foundational and core knowledge, or else describe how this knowledge is included in the program. If valid evidence is provided, graduate programs are exempt from the three (3) Foundational KUs and five (5) Technical or Non-Technical Core KUs.
4. **Doctoral Programs align to:** three (3) Optional KUs and additional seven (7) KUs for dissertation or institutional equivalent **or** align to 18 KUs (3 Foundational, 5 Core, 3 Optional, & 7 Additional, see Figure 5). Graduate programs provide evidence that their students are admitted with foundational and core knowledge or it is included in the program. If valid evidence is provided, graduate programs are exempt from the three (3) Foundational KUs and five (5) Technical or Non-Technical Core KUs.

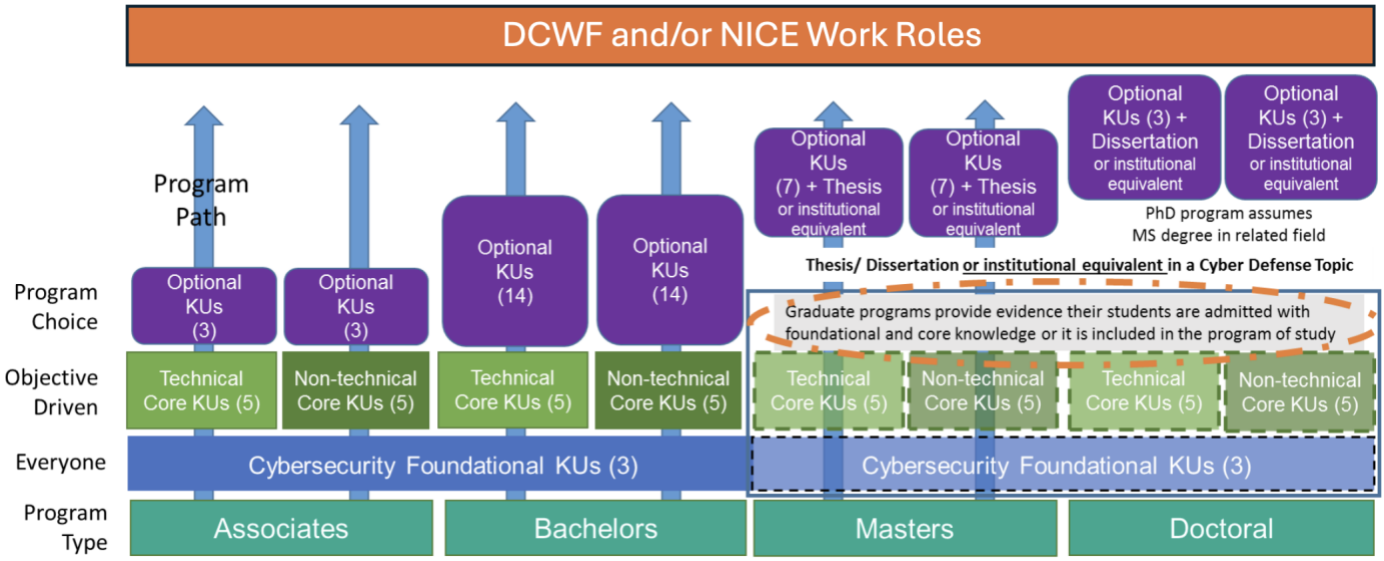

Figure 5. CAE-CD Knowledge Units Alignment Requirements

f. Graduate Thesis/Dissertation/Equivalent Guidelines and Process (Masters & Doctoral Programs Only)

Graduate programs (Masters and Doctoral) that elect to use the Graduate Thesis/Dissertation/Equivalent in lieu of the additional seven (7) KUs, should provide evidence of institutional documentation and process for thesis, dissertation, or equivalent.

Masters degree programs may include traditional Master Thesis or equivalent such as: graduate project course, graduate experiential learning course, or graduate practicum with a preference for industry advisor interactions. Master Thesis/equivalency should include one or more dedicated term-long course(s) indicated as "Thesis", "Project", "Capstone", "Experiential Learning", or "Practicum" preferably towards the end of the student's PoS and should be supervised by a qualified faculty member. The student (or small group of up to two students) develops a final project/capstone and/or experiential learning as a paper and/or applied project that integrates best practices in the context of cybersecurity. Concepts and national cybersecurity standards underlying the student's project and/or experiential learning are articulated; the problem is clearly stated; measurable goals are specified; and strategies to implement the project and/or experiential learning goals are provided. For Master degree program only, it is acceptable to have a Graduate Project/Capstone/Experiential Learning/Practicum course(s) or traditional two-term "Thesis" course(s) as an option for students **(an exception to the 1d "no elective or optional courses" rule)**. In this situation, this/these course(s) cannot be aligned to any other KU(s) beyond the seven (7) additional KUs (see Figure 6).

Master Technical CAE-CD (Total 22 KUs)																				
PoS Courses in KU Alignment	Foundational			Technical Core					Optional							Aditional or Graduate Thesis/Dissertation/Equivalent							
	CSF	CSP	ISC	BSP	BNW	NDF	BCY	OSC	NTP	ANT	LCS	CTH	ACR	DFS	NWF	7 KUs for Graduate Project Course							
ISEC690 (Project) or ISEC701+ISEC702 (Thesis)	No other KUs can be selected! Due to alignment of Project OR Thesis															x	x	x	x	x	x	x

Figure 6. CAE-CD Knowledge Units Alignment Restriction for MS Project/Thesis Case

Doctoral degree programs may include Traditional Dissertation (Ph.D./D.Sc.) or equivalency such as professional doctorate applied research project. The Traditional Dissertation should show clear and demonstrable focus on cybersecurity and should be supervised by a qualified faculty member. The work should represent at least two years effort by the student on the research. Professional Doctorate Equivalency should show clear and demonstrable focus on cybersecurity and should be supervised by a qualified faculty member. The work should represent at least one-year effort by the student on the applied research. The Traditional Dissertation and the Professional Doctorate Equivalency should include a formal scheduled defense.

Requirement (Masters/Doctoral):

1. Provide institutional evidence for the requirements and process of the graduate Thesis/Dissertation/Equivalent (in PDF).

2. Students

All of the following elements should be directly relatable to the defined PoS as documented in the application.

a. Student Enrollment/Graduation in the PoS(s)

The applicant will demonstrate that the PoS(s) submitted has been offered for a minimum of three years, and has at least one class that has completed or graduated from the PoS. Demonstration that a PoS has actual student outputs is an essential part of the application. A minimum of three students should be used to document actual attainment of the Program-Level Learning Outcomes as defined in the PoS.

Requirements (All required within the last three (3) years):

1. Provide student enrollment (unduplicated/headcount) in PoS for the last three years (each year separately).
2. Provide an official institutional letter for the enrollment (unduplicated/headcount) and graduation in the PoS for the last three years, each year separately (letter from the Registrar, Institutional Effectiveness, or equivalent. Letters from a program director or a POC are not acceptable) (in PDF).
3. Provide at least three (3) redacted student transcripts, showing the student graduated or attended within the last three years and clearly highlight the courses taken that are in the KUs alignment. All KU-aligned courses must appear on the transcript.

b. Sample student certificate/notation on transcript/official letter

Graduates from CAE-CD validated PoS should receive documentation from the institution recognizing their completion of the NSA Validated PoS and if the academic institution also holds an NSA NCAE-C, recognition should be made for their completion from a PoS that is also under an NSA NCAE-C designated “Center”.

Requirement:

1. Provide a sample certificate, draft of official letter, or proposed notation on transcript to be issued to students completing the PoS indicating they completed the NSA Validated PoS and if the academic institution also holds an NSA CAE-C, recognition should be made for their completion from a PoS that is also under an NSA NCAE-C designated “Center”.

c. Students' Work Products (papers, assignments labs, etc.)

Sample student work products are important to evaluate the quality and depth of students' work during the PoS. Student work products are (but not limited to): papers, assignments, projects, presentations, lab exercises, test questions.

Requirement (All required within the last three (3) years):

1. Provide samples of six students' work products from six different assignments (six files total) within the last three years. Samples can be (but not limited to): papers, assignments, projects, presentations, lab exercises, test questions from at least two courses in the PoS that are in the KU alignment. Student names should be removed prior to submission. Students work products should not include grades or grading comments, only the original students work. Combine the guidelines (i.e., what students are asked to do) for students work products, **indicate the course and the KU that each is associated with**, and one sample student work (name redacted) into a single file for each of the student's work (in six separate PDFs).

d. Student Competency Development and Ethical Conduct

Requirement 1b listed the requirements for the applying or re-designating PoS. A focus on competency provides an effective bridge between the students' educational experiences and the workplace, and competencies connect students' learning (through their academic program, co-curricular, and extra-curricular activities) to cybersecurity work roles. Within the NCAE-C and in terms of the process of Re-designation, competency means the ability of the student to complete a task within the context of a work role. Every competency can be described through the Essential Elements (ABCDE) framework. The five essential elements to every competency are the **a**ctor, **b**ehavior (task), **c**ontext, **d**egree, and **e**mployability (as shown in Table 2).

Table 2. The NCAE-C Essential Elements (ABCDE) Framework of Competency

Elements	Purpose	Element Descriptions
Actor	Who?	Who is involved in this competency? What background knowledge/experience/previous learning are necessary for this competency?
Behavior	What?	What is being done? Maps directly onto tasks from either the DCWF or the NICE Framework.
Context	How?	How is this task being done? With what resources, affordances and constraints?
Degree	How much?	From an employer's perspective, what possible measures of time, accuracy or completion might be expected from someone who is competent with this task.
Employability	Professional skills	What professional skills are necessary to be competent with this task?

The alignment of competency activities with identified cybersecurity work roles supports students' discovery of different areas in cybersecurity where they can competently apply their acquired knowledge and skills within the context of a work role, this supports students in making connections between these opportunities and resume bullets and/or talking points in interviews. The activities also support the development of the professional skills required by employers. 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. Documentation of student participation in extracurricular activities can demonstrate program opportunities for students. Appendix 4 offers an overview of NCAE-C resources to assist in ethics education, professional skills development, career awareness, and career pathways.

Requirements (All required):

1. **Identify 5 to 10 most relevant work role tasks from DCWF or NICE Framework** (given that one task can be used for more than one competency statement) from the previously identified work roles in Requirement 1b that students engage with as part of competency activities delivered within the curriculum and/or within co-curricular and extra-curricular activities. At least five of these tasks must be delivered within the PoS. Only the tasks used for the competency statements should be selected here.
2. **Identify and list 10 competency statements** relating to the PoS that are available to students to engage with as part of competency activities. Refer to the Competency in Education Handbook for further guidance and examples. At least five of these competency statements must be related to curricular activities that all students experience within the PoS and the remaining statements may focus on co-curricular and/or extra-curricular experiences offered as part of the PoS. (Combined to a single PDF). Examples of activities:
    - **Curricular Activities:** e.g., classroom activities, required labs, assigned hands-on exercises and/or games, capstone or research projects that are part of the academic curriculum, **and/or**
    - **Co-curricular activities:** e.g., optional lab sessions, faculty-guided research, student club activities focused on relevant topics, workshops, seminars, or enrichment programs that complement the formal curriculum, **and/or**
    - **Extracurricular Activities:** e.g., cyber competitions, participation in cyber-ranges outside of course requirements, internships/coops, community outreach or service activities, conferences, professional association events.
3. **Provide a brief statement of how the 10 identified competency statements were implemented and evaluated** with the PoS students to demonstrate that they successfully performed these competencies during the past three years.
4. **Provide three (3) distinct pieces of evidence from different instructional contexts within the PoS that demonstrate student engagement in ethical education** (see examples in Appendix 4 – e.g., an ethics course, module, assignment, independent study, introduction and attestation to the NCAE-C Code of Ethics and Professional Conduct, Montreat Professionalism and Ethics Toolkit, competitions to enhance baseline knowledge in ethics) (in a PDF file). **Note:** Submitting the same assignment or activity across multiple terms does not satisfy this requirement.
5. **Provide evidence of three students' participation in separate extracurricular activities within the last three years**, which may include (but are not limited to): experiential learning activities, local/regional/national cyber exercises and competitions, outreach to community colleges and high schools, computer check-up days, summer internship program, industry guest lectures, etc. Provide dates and descriptions for each piece of evidence provided.

3. Faculty Members

Faculty members are the instrument that delivers the PoS content to students via courses and other learning experiences. The cybersecurity faculty should have appropriate experience associated with the PoS and courses they are assigned. The NCAE-C program will rely upon the institutional accreditation process to determine the correct credentials to be a faculty member. An examination of faculty members' curriculum vitae (CV) or resume as part of the review process can determine the appropriate level of cybersecurity experience, knowledge, and preparation. A portion of the faculty responsible for the program is required to be full-time members teaching at the PoS, with the remainder being adjuncts or part-time. The institution's accreditation-based documentation for faculty academic credential qualifications will be the basis for this PoS Validation requirement. **Faculty members must support enrolled students by serving as mentors or advisors to student-led activities, and by participation or sponsorship of cybersecurity exercises and competitions (including in-class competition) within the last three years.** Evidence must include links to student clubs, cyber defense exercises, link to team roster on a competition website, link to social media about the exercise,

or other forms of official acknowledgement that include a full-description of the activity, the date, and the nature of the participation.

Requirements (All required within the last three (3) years):

a. Identify the Point-of-Contact (POC) for the PoS (a full-time/permanent faculty member of the institution directly involved with the representative academic program) including name, phone number, and e-mail address. The POC is expected to take full responsibility and provide support for the Validation and/or Designation. This means ensuring programs are fully supported by the institution long term. Note: This will be the person who will be contacted by the PMO and/or the National Centers for all NCAE-C program updates, grants and scholarship opportunities, upcoming events, and other administrative communications. Also, identify the Alternate POC for the PoS. The individual assigned to this role is one whom is a full-time/permanent employee in a professional capacity (not an administrative personnel) and is a secondary contact to the POC.
b. Identify all faculty members in the program including name, phone number, and e-mail address, highest degree earned, field and year, academic rank, type of academic appointment (Tenure Track, Tenured, Continuing Contract, Non-Tenure Track, etc.), full-time, part-time, or adjunct status, and years of academic experience. Also, provide an updated CV or resume for each faculty member teaching course(s) in the KU alignment with their cybersecurity or related qualifications identified. These CVs should be abbreviated to up to four (4) pages each to address necessary elements including maintenance of currency, publications, research, industry involvement, Continuing Professional Education (CPE), presentations, certifications, workshops attended, professional registration and/or certification (if applicable), level of activity in professional organization, professional development, and consulting or summer work in industry (high, medium, or low). The applying institution must be included in the CV or resume. (One PDF per faculty member teaching course(s) in the KU alignment, 10 max).
c. Provide evidence for faculty members' support of enrolled students by serving as mentors or advisors to student-led activities, and by participation or sponsorship of cybersecurity exercises and competitions (including in-class competition) within the last three years. Evidence must include link(s), such as: link to student clubs, link to cyber defense exercises, link to team roster on a competition website, link to social media about the exercise, or other forms of official acknowledgment that include a full-description of the activity, the date, and the nature of the participation (Two (2) pieces of evidence minimum. All links and evidence information provided within a single PDF).
d. Provide evidence for the institutional process of faculty promotion/reappointment (e.g., the relevant section of the Faculty Policy Manual). Highlight the specific section on promotion and/or add a note on the first page with the section and/or page numbers where this process is found. If there is no faculty promotion/reappointment process, write a justification with an explanation (in a single PDF).

4. <u>Continuous Program Improvement</u>

A key element to ensure vitality and functionality over time is a strong continuous program improvement plan, process, and regular evaluation schedule. A process-driven continuous program improvement plan directed at the Program-Level Learning Outcomes is an essential element of the program. At regular academic intervals, selected Program-Level Learning Outcomes should be assessed by an analysis of student work via the learning outcome assessment indicators to demonstrate whether attainment of defined levels of performance is being achieved. This is done by assessing specific elements of student performance against defined rubrics to demonstrate student level of achievement. This is not just using course grades, but rather a granular analysis of specific assignments that demonstrate competence associated with the defined Program-Level Learning Outcomes. For each Program-Level Learning Outcome item, a defined set of student work elements will be identified, associated rubrics developed to score them defined, and a desired standard of student achievement defined. Then, student work will be scored to see if the program is meeting the desired level of attainment for each of the Program-Level Learning Outcomes. As a normal part of the process, one or more steps should be initiated to improve student attainment of the Program-Level Learning Outcomes over time. The changes will be evaluated at a future assessment period. All of the associated process

improvement activities should be driven by the faculty associated with the PoS, not by random individual actions. Records of the assessments, the process, and the documented plans for improvement, should be kept and submitted as part of the annual reports and at Re-designation. Documentations for continuous program improvement plan, process, and regular evaluation schedule are expected to match those that the academic institution files with their accreditation body(ies).

a. Continuous Program Improvement Plan for the PoS

The *Continuous Program Improvement Plan* for the PoS commonly includes four parts that the academic institution and/or academic unit documents to enhance the overall quality of its PoS:

- Strategic process planning goals for the PoS
- The Program-Level Learning Outcomes for the PoS
- Description of the assessments of the Program-Level Learning Outcomes
- Proposed changes to enhance the quality of the PoS

Requirement:

1. Provide documentation of a Continuous Program Improvement Plan for the PoS (in PDF).

b. Continuous Program Improvement Process for the PoS

The *Continuous Program Improvement Process* commonly includes the four parts of the plan indicated above with a clearly identified end of a given process cycle (see Figure 7). Evidence must be provided of specific improvement efforts linked to assessment of the designated metrics. An institution should be prepared to adjust the process upon completion of a Continuous Program Improvement Process cycle.

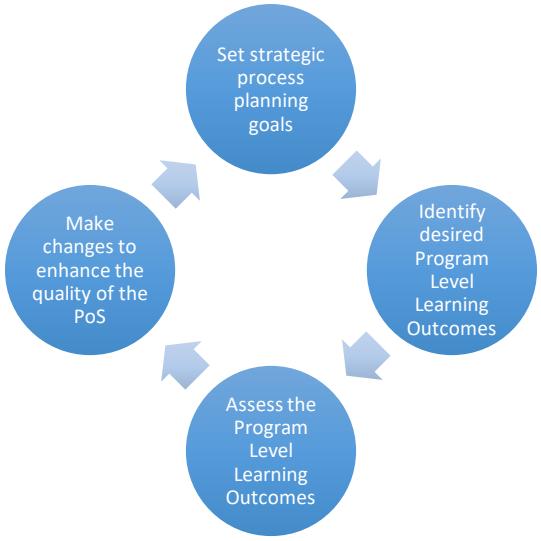

Figure 7. Continuous Program Improvement - Regular Evaluation Cycle

Requirement:

1. Provide documentation of the Continuous Program Improvement Process with specific improvement efforts linked to assessments (in PDF).

c. Continuous Program Improvement - Regular Evaluation Schedule for the PoS

Continuous Program Improvement - Regular Evaluation Schedule for the PoS may include (but not be limited to) a yearly, quarterly, each term, or monthly curriculum committee meeting set to evaluate the Program-Level Learning Outcomes, the assessment indicators, all other metrics, discussing the continuous program improvement plan and process along with adjustments needed.

Requirement:

1. Provide documentation of the Continuous Program Improvement - Regular Evaluation Schedule (in PDF).

PART II: CAE-CD APPLICATION – NCAE-C DESIGNATION/RE-DESIGNATION CRITERIA

Overview

Table 3 provides the required criteria for CAE-CD Designation/Re-designation.

Table 3. Summary of CAE-CD Designation/Re-designation Required Criteria

1. Accreditation: The academic institution must be a U.S. institution of higher education that holds current regional accreditation authorized by the U.S. Department of Education to award associate degrees or higher to apply for any NCAE-C Designation.
2. Institution 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 NCAE-C program including established "Center" for cybersecurity, identified NCAE-C POC, as well as acknowledging minimum participation expectations, including annual update of required metrics, attendance at annual events, and active participation in the CAE Community.
3. Evidence of Sound Cybersecurity Posture and Plan: Institutions shall have a sound institutional cybersecurity posture including a dedicated official to oversee implementation to provide an overview of the institution's ability to protect critical information and systems processing that information. A signed letter on official letterhead from the officer assigned with direct responsibility for institutional cybersecurity, attesting to the fact that the institution has a solid cybersecurity posture and plan in place, along with examples of cybersecurity plan implementations through awareness, training and tutorials, log in security banners, etc. will suffice.
4. Established "Center" for Cybersecurity: An officially established "Center" (either physical or virtual) for Cybersecurity providing program guidance and oversight, general cyber defense information, collaboration and outreach opportunities among students, faculty, other academic units/departments in the same institution, and other institutions, and a website that is dynamic, current and visible within the institution and the external community at large that also list the PoS Validated program(s). The "Center" must have an external board of advisors (maybe shared with other programs).
5. Affirmation of the NCAE-C Core Values and Guiding Principles: Applicant institutions will affirm their commitment to the NCAE-C Core Values as part of the Designation application, and are expected to follow the Guiding Principles indicated on each of the three NCAE-C Core Values (not to be submitted, affirmed only).
6. Sustainability: The institution must demonstrate the necessary resources, capacity and processes for the cybersecurity program to be successful are provided on a continuing basis.
7. Faculty Professional Development: The institution must provide evidence of faculty access to cybersecurity professional development including time release (e.g., course load reduction, sabbatical) and/or financial support for faculty (e.g., attendance in cybersecurity training/events, attaining certificates/further education, etc.), connection to industry/practitioners (e.g., ongoing access to guest lecturers working in the cybersecurity industry and government, faculty exchange program with industry and/or government, summer research programs for faculty, etc.). Provide flyers, posters, letters, etc.
8. Cybersecurity Academic Integration: Demonstrate cybersecurity content is integrated into additional degree programs within the academic institution.
9. Program Involvement: The academic institution must demonstrate how cybersecurity practices are extended beyond the normal boundaries of the institution. Show how cybersecurity concepts developed at the academic institution are shared with others to improve the practice of cybersecurity in the community.
10. Transfer of Credit/Articulation Agreements: Provide evidence of Articulation/Transfer agreements with institutions offering a concentration or cybersecurity (or related field) degrees/areas of study/track or certificates (United States Military Academies are exempt). Examples include statewide transfer agreements, articulation agreements, credit for prior learning, credit for military training, or membership in Transfer Evaluation Services (TES) with evidence of several transfer credits institutions in the geographic area.

CAE-CD Designation/Re-designation Criteria

The following criteria form the necessary documentation to demonstrate that the institution has the necessary resources, capacity, and processes to be a successful CAE-CD, and in the case of Re-designation that it is also involved in the CAE Community. All of the criteria are required of all CAE-CD applicants, both initial and at Re-designation.

1. Accreditation

The academic institution must be a U.S. institution of higher education, degree-granting institution offering cybersecurity-related degrees including majors, minors, and/or certificates at the Associates, Bachelors and graduate levels, and regionally accredited, as outlined by the U.S. Department of Education (http://ope.ed.gov/accreditation/), to hold any NCAE-C Designation.

Requirement:

a. Provide URL at the academic institution's domain to demonstrate that the academic institution is regionally accredited at the time of application.

2. 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-C program. The letter must express institutional commitment to excellence in the cybersecurity field and support of the program the institution is submitting for NCAE-C Designation, identify the NCAE-C Point of Contact (POC) from the institution, state institutional support of an official Cybersecurity "Center" within the institution, identify regional accreditation information, and list the program(s) of study supporting the requested Designation. Submission of this letter acknowledges minimum participation expectations including: submission of an Annual Report or annual update of application data in the application tool; attendance at the CAE in Cyersecurity Community Symposium each year; regular communication with the NCAE-C PMO, the CAE Community, and the CAE Community of Practice – Cyber Defense (CoP-CD) and actively participate in the CAE Community and support the NCAE-C programs. This letter must be submitted early in the process to demonstrate that the institution supports the application, executive leadership acknowledges and supports the NCAE-C program, and the institution is committed to meeting all required criteria throughout the life of the Designation.

Requirements (all required):

a. Provide a letter of intent and endorsement to participate in the NCAE-C program (in PDF, do not mail) that:
   1. Is written on official institution letterhead, signed by the Provost or higher and addressed to (Do not mail the letter):
      National Security Agency
      Attn: CAE Program Director
      9800 Savage Road
      Ft. Meade, MD 20755-6804
   2. Identifies regional accreditation information.
   3. Expresses institutional commitment to excellence in the cybersecurity field.
   4. Identify and provide institutional support of an established "Center" for Cybersecurity within the institution.
   5. Identify the NCAE-C Point of Contact (POC) from the institution.
   6. Lists the program(s) of study supporting the requested Designation.

b. Provide acknowledgement to follow the minimum participation expectations of a NCAE-C:
   1. Submission of a mandatory Annual Report with all required information.
   2. Attendance at either (or both) the NCAE-C PMO Meeting and CAE in Cybersecurity Community Symposium each year.

3. Regular communication with the NCAE-C PMO, the CAE Community, and the CAE and the CAE Candidates National and Peer Review Centers, including responding to email, offers input and suggestions for workshops, programs, etc.
4. Active participation in the CAE Community and support of the NCAE-C program, including acting as a mentor or application reviewer, participation on working groups, supporting program initiatives, briefing or lecturing for the CAE Lecture Series, webinars, and so on.

3. Evidence of Sound Cybersecurity Posture and Plan

Institutions shall have a sound institutional cybersecurity posture and plan including a dedicated official to oversee its implementation to provide an overview of the institution's ability to protect critical information and systems processing that information. The institution must demonstrate that they have the proper cybersecurity resources including a dedicated official, such as the CISO or CIO, with formal responsibility for the institution's cybersecurity posture and plan, that the cybersecurity posture and plan is maintained and functionally appropriate to mitigate cyber-attacks to the institutional information assets, and that the institution has a formal cybersecurity awareness program.

Requirements (all required):

a. Provide a signed letter on official letterhead from the officer assigned with direct responsibility for institutional cybersecurity, attesting to the fact that the institution has a sound cybersecurity posture and plan in place (in PDF).
b. Provide the name, title, and job description for the individual responsible for the institution cybersecurity program.
c. Provide six (6) separate examples of how the institution implements its cybersecurity plan through awareness, training and tutorials, log in security banners, user acknowledgements, online help and good security practice guides (e.g., Students, faculty and staff are required to take computer based training or online tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc.) (in six separate PDFs).

4. Established "Center" for Cybersecurity

The institution must have an officially established entity (either physical or virtual) serving as the focal point for its cyber curriculum and practice. The "Center" shall provide the following services: program guidance and oversight; general cyber defense information; and collaboration and outreach opportunities among students, faculty, and other institutions. Additionally, the "Center" must be supported by a website that is current and visible within the institution and the external community at large. The "Center" must have an external board of advisors – local/national industry professionals, faculty from other institutions, etc. to provide programmatic guidance over the activities of the "Center" and the NCAE-C program as a whole. This board provides a connection between the program(s), "Center", college/department, and the local community. The external board of advisors can be shared with other programs in the college/department.

Requirement (all required):

a. Provide URL at the academic institution's domain to demonstrate that the academic institution has an established Website for the "Center" for Cybersecurity including:
   - The "Center" Website (URL) is visible within the institution and the external community at large.
   - "Center" POC is noted.
   - Information about and link to the program page of the Validated PoS(s).
   - Faculty members.
   - Links to student cybersecurity activities available to students at the institution and beyond.
   - News that includes both internal and external cybersecurity news. Internal news should highlight cybersecurity activities and efforts at the institution and/or other cybersecurity activities of students

and faculty representing the institution. External cybersecurity news should highlight up-to-date trending cybersecurity information.
- Link to the institutional security resources and awareness.
- Up-to-date links to key cybersecurity resources for students such as cyber competitions.
- Documentation on the Industry Advisory Board/Committee.

5. <u>Affirmation of the NCAE-C Core Values and Guiding Principles</u>

NCAE-C at the academic institution is characterized by several common attributes including academic excellence and institutional excellence. These attributes are built upon a foundation of ethical behavior, a sharing environment, and a willingness to lead by example. These form the core values and guiding principles of the NCAE-C program. Applicant institutions will affirm their commitment to the NCAE-C Core Values as part of the *Designation* application, and are expected to follow the *Guiding Principles* indicated on each of the three Core Values (not to be submitted, affirmed only).

a. **The *Ethical Behavior* Core Value:** The academic institution must encourage and support ethical behavior by students, faculty, administrators, and professional staff. It is expected that academic institutions with NCAE-C Designation will have in place all the Guiding Principles noted below.

Guiding Principles

- The academic institution has appropriate systems, policies, and procedures that reflect the support for and importance of ethical behavior for students, faculty, administrators, and professional staff in their professional and personal actions.
- The academic institution has in place published policies and procedures to support legal and ethical behaviors.
- The academic institution has systems, policies, and procedures that provide appropriate mechanisms for addressing breaches of ethical behavior.
- The academic institution has in place systems for detecting and addressing breaches of ethical behaviors, or other mechanisms to deter academic misconduct, such as honor codes, plagiarism detection tools, and disciplinary systems to manage inappropriate behavior.

b. **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.

Guiding Principles

- The academic institution has appropriate mechanisms for facilitating collaboration between institutions, both NCAE-C and non-NCAE-C institutions.
- The academic institution has appropriate mechanisms to share resources, instructional material, faculty, and/or facilities between institutions, both NCAE-C and non-NCAE-C institutions.
- The academic institution engages students, faculty, administrators, professional staff, and practitioners in practices of successful information/resources sharing or joint events.

c. **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.

Guiding Principles

- The institution leads multidisciplinary cybersecurity activities and/or programs.
- The institution leads cybersecurity outreach activities.
- The cybersecurity program functions are conducted as part of an institutional and/or college/departmental effort, beyond a single isolated professor's efforts. This can include connection to the institution's mission, vision and strategic plans.

6. Sustainability

Sustainability of programs at the academic institution is an important component of the NCAE-C program. Having full-time permanent faculty members associated with the "Center" and PoS Validated program(s) are needed to run the continuous program improvement aspects of the program as well as elements such as outreach and ensure the continuous commitment to the NCAE-C program Core Values at the institution. Having these full-time permanent administration personnel, and POC (who may be a faculty member as well) identified in the application is part of assuring that the institution has the necessary resources, capacity, and processes for the cybersecurity program(s) to be successful.

Requirements (all required):

a.-e. Identify the administrative head of academic unit housing the established "Center" for Cybersecurity (Dean, Associate Dean, Department Chair, etc.) including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution. Also, provide CV of the administrative head of academic unit housing the established "Center" for Cybersecurity (in PDF).

f.-h. Identify the Point-of-Contact (POC) for the NCAE-C Designation (one applying for) and/or established "Center" for Cybersecurity (Department chair, faculty lead, NCAE-C POC, etc.) including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution. Also, provide CV of the POC and indicate year the individual joined the academic institution (in PDF). CVs may not be more than four (4) pages.

i.-k. Identify the alternate POC for the NCAE-C Designation (one applying for) and/or established "Center" for Cybersecurity including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution. Also, provide CV of the alternate POC for the NCAE-C Designation (one applying for) and/or established "Center" for Cybersecurity (in PDF).

7. Faculty Professional Development

Professional development for faculty at the academic institution is an important component of the NCAE-C program. Ongoing access to working professionals and practitioners during their time in a NCAE-C program is needed for faculty in order to maintain and improve the program as well as a crucial component of elements such as outreach, industry and government connections, awareness of the quality of the faculty and students at the institution, etc. There are many formats for such professional development opportunities, but the obvious elements are guest lecturers working in cybersecurity industry and government. Faculty development may be in the form of encouragement and time release (e.g., course load reduction, sabbatical) and/or financial support to attend and participate in cybersecurity training, professional certifications, teaching certificates, continuing education credits, doctoral programs, relevant conferences, faculty exchange program with industry and/or government, summer research programs for faculty, and/or other events. Identifying these professional development opportunities for faculty in the application is part of assuring that the institution has the necessary resources, capacity, and processes for synergistic success. The established "Center" for Cybersecurity at the institution is the likely sponsor for these activities or shared with the department/college in which it is housed. What is important is that these professional development activities are not only available to faculty, but also, that the institution demonstrates that the faculty participated in these activities regularly during the academic year.

Requirement (evidence within the last three (3) years):

a. Provide six (6) separate examples of cybersecurity professional development opportunities for faculty in the application over the past three years. Evidence files can be flyers, posters, letters, attendance records, or other evidence of actual participation in professional development for faculty (in six different PDFs).

8. Cybersecurity Academic Integration

The institution shall demonstrate that cybersecurity is not treated as an isolated discipline and cybersecurity concepts are also integrated into additional degree programs within the institution **outside the PoS(s)** applied for or previously validated. For example: healthcare students learning about privacy and patient data protection, or accountants learning about data backup and protection, or students in law school and/or

criminal justice learning about privacy laws and cyber-crime. Courses in this criterion cannot be courses in the applied for or previously validated PoS.

Requirements (all required):

a. Identify three (3) different courses and their academic unit(s) (department/college/etc.) at the institution where students from the non-validated PoS (or non-PoS(s) applied for Validation) at other academic unit(s) (department/colleges) are exposed to cyber concepts.
b. Provide the syllabi of the three (3) different courses identified where cyber modules are clearly highlighted from other academic unit(s) departments/colleges. Combine the syllabus, guidelines (i.e., what students are asked to do) of the work, and one sample student work into a single file for each of the three courses (Three separate PDFs).

9. Program Involvement

a. **Outreach (For new CAE applicant (Candidate) and Re-designating Institutions):** One of the core values of the NCAE-C program is the sharing of cyber defense expertise. The institution must demonstrate how cyber defense practices are extended beyond the normal boundaries of the institution. Outreach activities help show how cyber defense concepts developed at the institution are shared with others, and how employers, theory, and practice are incorporated into the curriculum. Moreover, outreach activities allow the cybersecurity program to engage with the government and industry to provide pathways for graduates while maintaining an appropriate curriculum to place graduates into those jobs.

Outreach Requirements (Three (3) pieces of evidence for Candidates and four (4) for Re-designations): Three (3) pieces of evidence are required for new CAE applicant institutions (Candidate institutions) and four (4) pieces of evidence are required for Re-designating institutions. For Candidate institutions, these outreach efforts must all have occurred within the last three years, with at least one occurring within the last year. For re-designating institutions, these outreach efforts must have occurred during the current period of Designation and should be spread across the 5-year period (not all in one year).

Options (Submit a total of (3) pieces of evidence for new CAE applicant (Candidate) or a total of four (4) pieces of evidence for Re-designating Institutions):

1. Provide evidence of how the institution has **shared cyber-related curriculum and/or faculty with other schools**, including K-12 schools, community colleges, and/or technical schools to advance cyber defense knowledge. Identify specific materials provided, to whom the material was provided, when, and for what purpose. A good resource in the October Cyber Awareness Month is a link to resources: https://staysafeonline.org/. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties' websites, etc. is encouraged (in PDF).
2. Provide evidence of **faculty member/employee sponsorship or oversight of students for cyber events for the community at large**. These events must be outreach focused and include cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training, and the surrounding community (in PDF).
3. Provide evidence of the methods used by the institution to reach out to potential employers. This could be to support student placement for cyber-related internships and jobs. (e.g., Career Fairs, adding new employers job postings to HandShake, Partnerships, Memorandum of Understanding (MOUs)) (in PDF).
4. Provide evidence of **outreach to federal and/or regional government departments and agencies** in support of cybersecurity policies and practices (e.g., CISA, State or local agencies, National Guard, etc.). Examples of outreach are hosting of agencies' events on-campus and/or faculty members serve as volunteers on agencies' working groups or advisory committees.

5. Provide evidence of **obtaining input on curriculum** to meet industry needs (in PDF).
6. **Re-designated institutions only:** Provide evidence of faculty members **collaborating with current NCAE-C institutions** on research, grants, course development, etc.

b. **Participation (Applies to Re-designating institutions only):** The *Share* and *Lead by Example* core values inspire the participation and contribution to the NCAE-C program requirements. Achieving the *shared governance* and *maintain/improve* NCAE-C Program objectives are dependent on the participation of Designation POCs. *Shared governance* refers to the collaboration between the PMO, designated institution representatives, and federal partners to develop strategy and implement program standard procedures for the CAE Community, the Candidates' Program and Communities of Practice. The *maintain and improve* objective is also dependent on participation of Designation POCs to help develop and manage curriculum and other resources for student and faculty development. For re-designating institutions, these participation efforts must have occurred during the current period of Designation. A total of eight (8) CAE meetings are required, four (4) from 9b1 and four (4) from 9b2 (see below) spread across the 5-year period (not all in one year). Provide evidence of annual participation leading up to Re-designation for attending mandatory CAE annual meetings and participation in CAE Community events. If unable to attend either of the mandatory meetings, justification must be provided.

Participation Requirements (Institutions must separately provide eight (8) pieces of evidence, four (4) from 9b1 and four (4) 9b2):

1. The primary Point of Contact (POC) and/or the alternate POC at CAE designated institutions must **confirm attendance at one (1) mandatory CAE annual meeting each year**. Provide four (4) pieces of evidence in a PDF file, of annual attendance leading up to Re-designation. If unable to attend, provide justification.
   - NCAE-C Program Management Office (PMO) Annual Meeting, Or
   - CAE in Cybersecurity Annual Symposium (held annually)

2. Re-designating institutions must also **participate, in at least four of the following CAE Community events**, either in person or in a virtual environment in the past five years. Provide four (4) pieces of evidence in a PDF file, for annual attendance leading up to Re-designation. If unable to attend, provide justification.

   Examples are as follows:

   - NCAE-C events such as CAE Regional workshops, or similar regional or topic focused event
   - CAE Tech Talks and/or Forums
   - CAE Orientation Meeting
   - CAE Candidates/Reviewers, Careers Preparation or Education Pathway National Center event
   - NCyTE workshop or event
   - CAE Community of Practice (CoP) in Cyber Defense (CD) event
   - CAE Virtual Monthly Meetup
   - CAE Lecture Series

Note: Evidence for participation may be provided as a copy of email, letter, attendance or participation or attestation by a committee or event chair.

c. **Contributions (Applies to Re-designating institutions only):** Re-designating institutions must make meaningful contributions to the welfare and growth of the NCAE-C program each year. These contributions are on behalf of the institution, meaning the POC, alternate POC, or other faculty member

may be the contributor, and it is not required that the same individual contribute each year. Different individual may provide the contribution each of the five years of the Designation period.

Contribution Requirements:

1. Institutions must demonstrate evidence of a minimum of four (4) contributions over the duration of the five-year Designation period.

   Examples are as follows:

   - Participation in the NCAE-C grants program as a single grantee, coalition lead, or coalition member.
   - Supporting a DoW Cyber Service Academy (CSA) grant at the institution.
   - Service for one year as a PoS Validation and/or NCAE-C Designation mentor, reviewer, advisor, or active chair of a Working Group, CoP-CD Initiative, or any other leadership role.
   - Active membership in a CAE Working Group, CAE Community Initiative, CoP-CD Steering Committee and/or Initiative, or engagement in another active role within the CAE Community. A detailed justification AND evidence must accompany this role. ***Listing 'other active roles in the CAE Community' without valid justification will disqualify the contribution.***
   - Contribution by faculty members from the institution to the CAE Community through presentations in CAE in Cybersecurity Symposiums, providing feedback to competition organizers (NCAE Cyber Games, NCL, CCDC, etc.), delivering talks, lecture series, presentations, chairing sessions, lightning talks, and/or workshops at meetings and/or other events hosted by the CAE in Cybersecurity Community, NCAE-C CoP-CD, CNC, NCyTE, and/or CAE Tech Talk/Forum.
   - Participation by faculty and/or staff in the FBI Citizens Academy and regular involvement in their respective FBI Citizens Academy Alumni Association, or leadership/assistance in regional events affiliated with InfraGard (https://www.infragard.org/).
   - Contribution of curricular resources by faculty members to the CLARK Center (https://www.clark.center/home), and/or providing three meaningful reviews of curricular resources to CLARK.

10. Transfer of Credit/Articulation Agreements

Transfer of Credit/Articulation Agreements to/from other academic institutions are important and needed to demonstrate the pipeline in cybersecurity, in the context of offering a concentration and/or cybersecurity (or related field) degrees/areas of study/track and/or certificates. Agreements should be with community colleges, technical schools, minority colleges/universities, other colleges/universities, and/or with high schools (cyber-related or technical pre-requisites, not just general pathway programs). United States Military Academies are exempt (provide justifications).

Requirement:

a. Provide evidence that 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 or has agreements for transferring their courses to other schools. Examples include but are not limited to: transfer agreements of credit to/from community colleges, articulation agreements, statewide transfer agreements, articulation 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) (in PDF).

PART III: NCAE-C POST-DESIGNATION REPORTING REQUIREMENTS

Overview

Academic institutions holding any NCAE-C Designations (e.g., CAE-CD) must update their relevant qualifying Designation criteria information yearly by an annual report or in the reporting tool.

Continuous Program Improvement Plan and Process

A key element to ensure vitality and functionality over time is a strong continuous program improvement plan and process. A continuous program improvement process directed at the Program-Level Learning Outcomes is an essential element of the program. All NCAE-C Designations are required to show a continuous program improvement plan and process, during the Re-designation process every fifth year.

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 and newly assigned institution POCs will send a Program Representative to an orientation meeting within six months of Designation date. PMO will notify institutions when dates are scheduled.
- 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 in Cybersecurity Community Symposium and/or the annual PMO Meeting and/or regional CAE Community Meetings
- Maintain validated program and Designation requirements
- Maintain continuous program improvement plan and process

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.

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 4 for time-dependent additional consequences).

Table 4. 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 NCAE-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 designated Program of Study	Can result in reconsideration of the Designation, may include visiting committee or other visit. NSA reserves the right to rescind Designation(s) under circumstances where critical program 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 in the application tool and notification via email to the PMO.

3. Major Changes to Designated Program of Study(ies) (PoSs)

It is the role of the POC and/or other institutional staff overseeing the NCAE-C Designation to ensure that the information about the validated PoS(s) is/are up to date and reflecting the current courses in the program(s), the KU alignment, as well as Curriculum Map and Plan. Failure to keep validated PoS(s)' information up to date, can result in reconsideration of the Designation, may include a visiting committee or other visit. NSA reserves the right to rescind Designation(s) under circumstances where critical program requirements are not met any time during the Designation period.

4. Continuous Program Improvement Plan and Process

A strong continuous program improvement plan and a process for regular implementation of the plan are key elements to ensure vitality and functionality of the PoS over time. A process-driven continuous program improvement plan directed at the Program-Level Learning Outcomes is an essential element of the program. At regular academic intervals, selected Program-Level Learning Outcomes should be assessed by an analysis of student work to demonstrate whether attainment of defined levels of performance is being achieved. This is done by assessing specific elements of student performance against defined rubrics to demonstrate student level of achievement. This is not just using course grades, but rather a granular analysis of specific assignments that demonstrate competence associated with the defined Program-Level Learning Outcomes (i.e., the program outcome assessment indicators).

For each Program-Level Learning Outcome indicated in the Curriculum Map and Plan, a defined set of student work elements will be identified, associated rubrics developed to score them defined, and a desired standard of student achievement defined. Then, student work will be scored to see if the program is meeting the desired level of attainment for each of the Program-Level Learning Outcomes. A minimum of one, preferably two assessment items (i.e., the Program-Level Learning Outcome assessment indicator(s)) shall be chosen to measure each Program-Level Learning Outcome. These assessment indicator(s) will be graded at least once every three years (see Appendix 3 - Examples 1 and 2 for requirement 1d1: Curriculum Map and Plan). It is not necessary to assess all Program-Level Learning Outcomes every year, nor is it desirable as changes should be gradual and measurable. Improvement efforts should be spaced out so that some Program-Level Learning Outcomes are assessed every year. For each assessment indicator, the class assignment and associated rubric used to measure the Program-Level Learning Outcome shall be provided (see Appendix 3 - Examples for requirements 1d2 and 1d3).

As a normal part of the continuous program improvement process, one or more steps should be initiated to improve the Program-Level Learning Outcomes over time. The changes will be evaluated by the academic institution at a future assessment period. All of the associated process improvement activities should be driven by the faculty associated with the PoS, not by random individual actions. Records of the assessments, the process, and the documented plans for improvement, should be kept and submitted as part of the annual reports and at Re-designation.

PART IV: RECURRING REVIEW OF NCAE-C DESIGNATION INSTITUTIONAL CRITERIA

Academic institutions holding any NCAE-C Designations (e.g., CAE-CD) must formally renew their PoS(s) Validation and NCAE-C Designation every five years.

APPENDIX 1 – REQUIRED AND OPTIONAL KNOWLEDGE UNITS LIST FOR CAE-CD

(3) Foundational (all required): IT Systems Components (ISC), Cybersecurity Fundamentals (CSF), and Cybersecurity Principles (CSP).

(5) Core KUs required of all PoS. Individual programs choose to align to Technical or Non-Technical Core KUs depending on the nature of their PoS. Associates and Bachelors programs are required to align courses in the PoS to the Technical or Non-Technical KUs. Graduate programs may either align to these KUs, or may provide detailed documentation on how the institution verifies that students have met these KUs. For example, the institution may document a system in place that allows for checking of prior courses and/or other experiences of entering graduate students to demonstrate the Foundational and Core KUs or require them to take courses and/or other experiences to achieve the Foundational and/or Core KUs lacking before entering or during the program.

The five (5) technical **core** KUs are:

- Basic Scripting and Programming (BSP)
- Basic Networking (BNW)
- Network Defense (NDF)
- Basic Cryptography (BCY)
- Operating Systems Concepts (OSC)

The five (5) non-technical **core** KUs are:

- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)
- Cybersecurity Planning and Management (CPM)

Optional KUs (62 total) can be adopted by any program as needed to document their program of study. Additionally, opposing core KUs may be used as optional KUs (i.e., If technical core is chosen, then non-technical core may be used as optional KUs and if non-technical core is chosen, then technical core maybe used as optional KUs). Optional KUs include:

Advanced Algorithms (AAL)	**Formal Methods (FMD)**	**Operating Systems Theory (OST)**
Advanced Cryptography (ACR)	**Fraud Prevention and Management (FPM)**	**Operating System Administration (OSA)**
Advanced Network Technology and Protocols (ANT)	**Hardware Reverse Engineering (HRE)**	**Pre-OS Boot Environment (PBE)**
AI Fundamentals (AIF)	**Hardware/Firmware Security (HFS)**	
Algorithms (ALG)	**Host Forensics (HOF)**	**Penetration Testing (PTT)**
Analog Telecommunications (ATC)	**IA Architecture (IAA)**	**Privacy (PRI)**
Basic Cyber Operations (BCO)	**IA Compliance (IAC)**	**QA/Functional Testing (QAT)**
Business Continuity and Disaster Recovery (BCD)	**IA Standards (IAS)**	**Radio Frequency Principles (RFP)**
Cloud Computing (CCO)	**Independent/Directed Study/Research (Emerging Topics) (IDR)**	**Secure Programming Practices (SPP)**
Cyber Crime (CCR)	**Industrial Control Systems (ICS)**	**Software Assurance (SAS)**
Cyber-Physical Systems (CPS)	**Introduction to Theory of Computation (ITC)**	**Software Reverse Engineering (SRE)**
Cybersecurity Ethics (CSE)	**Intrusion Detection/Prevention Systems (IDS)**	**Software Security Analysis (SSA)**
Data Administration (DBA)	**Life-Cycle Security (LCS)**	**Supply Chain Security (SCS)**
Data Structures (DST)	**Low Level Programming (LLP)**	**Systems Cert. and Accreditation (SCA)**
Database Mgmt. Systems (DMS)	**Machine Learning Fundamentals (MLF)**	**Systems Programming (SPG)**
Databases (DAT)	**Media Forensics (MEF)**	**Systems Security Engineering (SSE)**
Device Forensics (DVF)	**Mobile Technologies (MOT)**	**Threat Intelligence (THI)**
Digital Communications (DCO)	**Network Forensics (NWF)**	**Virtualization Technologies (VVT)**
Digital Forensics (DFS)	**Network Security Administration (NSA)**	**Vulnerability Analysis (VLA)**
Embedded Systems (EBS)	**Network Technology and Protocols (NTP)**	**Web Application Security (WAS)**
Forensics Accounting (FAC)	**Operating Systems Hardening (OSH)**	**Wireless Sensor Networks (WSN)**

https://www.cyber.mil/ncae-c/document-library

APPENDIX 2 – KU ALIGNMENT REQUIREMENTS FOR CAE-CD

Program of Study (PoS) Validation - Knowledge Units (KUs) requirements per academic level; See Appendix 1 for a the CAE-CD list of KUs. All PoS align to the three Foundational KUs, and five Technical or five Non-Technical KUs. Each Designation also has a requirement to align to Optional KUs. The number of Optional KUs is determined by the academic level of the program.				
Designation	Optional KUs	Foundational KUs	Core KUs (Choose technical **OR** non-technical)	
CAE-CD, Associates	3	IT Systems Components Cybersecurity Foundations Cybersecurity Principles	Non-Technical	Cyber Threats Policy, Legal, Ethics and Compliance Security Program Management Security Risk Analysis Cybersecurity Planning and Management
CAE-CD, Bachelors	14		Technical	Basic Scripting and Programming Basic Networking Network Defense Basic Cryptography Operating Systems Concepts
CAE-CD, Masters	7	Graduate programs must demonstrate that students have received subject matter preparation equivalent to the foundational and core KUs or alignment to required KUs or include it in the program.		
CAE-CD, Doctoral	3			

APPENDIX 3 – EXAMPLES OF POS VALIDATION REQUIREMENTS

Example for requirement 1a: PoS Curriculum Sheet:

CYBER DEFENSE

MASTER OF SCIENCE (M.S.)

Curriculum | Total Credits: 30

PREREQUISITE COURSES **Credits**

Applicants who do not have adequate academic backgrounds may be required to take one or more of the following 500-level graduate courses during the first two terms of the program.

CISC	501	Computer Organization and Architecture	3
CISC	502	Mathematics in Computing	3
CISC	503	Data Structures and Algorithms	3
MSIT	501	Foundations of Programming, Data Structures, and Algorithms	3

Students must take all 10 required courses. Students who wish to take an elective (above the 10 required courses) must request approval from the program office before registration.

DEGREE PROGRAM COURSES

Required Courses

CISC	640	Operating Systems	3
CISC	650	Computer Networks	3
CISC	680	Software Engineering	3
ISEC	615	Fundamentals of Cybersecurity	3
ISEC	620	Applied Cryptography	3
ISEC	640	Database Security	3
ISEC	650	Computer and Network Forensics	3
ISEC	660	Advanced Network Security	3
ISEC	690	Information Security Project	3
MSIT	630	Database Systems	3

Example 1 for requirement 1d1: Curriculum Map and Plan:

Program-Level Learning Outcomes Curriculum Map and Plan
Program Title: BS in Cybersecurity
Updated: 2026.XX.XX

Program-Level Learning Outcomes: *Graduates should be able to…*	ABC 106	ABC 110	ABC 116	ABC 140	ABC 145	ABC 205	ABC 214	ABC 215	ABC 216	ABC 226	ABC 227	ABC 228	ABC 229
1. *[Program-Level Learning Outcome 1, Ex. "Apply security principles and practices to maintain operations in the presence of risks and threats"]*				I			R	R	A (2026 -27)	R	R	R	R
2. *[Program-Level Learning Outcome 2, Ex. "Communicate professionally with customers and co-workers"]*				I			R	R	A (2026 -27)				
3. *[Program-Level Learning Outcome 3]*			I		R	R	R	R	R	R	R	R	A (2026 -27)
4. *[Program-Level Learning Outcome 4]*										I	R	R	A (2026 -27)
5. *[Program-Level Learning Outcome 5]*						A (2025 -26)	R	R					
6. *[Program-Level Learning Outcome 6]*	I	R	A (2025 -26)										

I, R, and A indicate the courses in which each Program-Level Learning Outcome is: introduced (I), reinforced (R), and formally assessed (A). The number of Program-Level Learning Outcomes may vary depends on the academic institution and level of the program.

Example 2 for requirement 1d1: Curriculum Map and Plan:

Program-Level Learning Outcomes Curriculum Map and Plan
Program Title: MS in Cybersecurity Management
Updated: 2026.XX.XX

Program-Level Learning Outcomes: *Graduates should be able to…*	ABC 6002	ABC 6003	ABC 6005	ABC 6007	ABC 6009
1. *[Program-Level Learning Outcome 1, Ex. "Communicate cybersecurity management concepts professionally"]*	A1		A2		
2. *[Program-Level Learning Outcome 2, Ex. "Develop organizational policies related to cybersecurity for effective operations"]*				A1	A2 (2026-27)
3. *[Program-Level Learning Outcome 3]*	A1			A2	
4. *[Program-Level Learning Outcome 4]*	A1				A2 (2026-27)
5. *[Program-Level Learning Outcome 5]*		A1	A2		

A1 and A2 indicate the courses in which each Program-Level Learning Outcome is: formally assessed via Indicator 1 (A1) and formally assessed via Indicator 2 (A2). The number of Program-Level Learning Outcomes may vary depends on the academic institution and level of the program.

Example for requirement 1d2: **General information for Program-Level learning outcome**

Need to be submitted for each Program-Level Learning Outcome

Date report submitted	09-20-20xx
Program faculty who contributed to this report	Jane Doe
Program-Level learning outcome	Apply security principles and practices to maintain operations in the presence of risks and threats
Course(s) that formally assess(es) this program-level learning outcome (at its highest level, see Curriculum Map and Plan)	ABC 216 Industrial Control Systems Security
Number of students assessed for this program-learning level outcome	23
Quarter/Semester students were assessed (e.g., Winter 2024)	Winter 20xx

Example for requirement 1d3: **Assessment of indicators for the Program-Level learning outcome (add more rows if necessary)**

Can be one or more assessment indicators for each Program-Level Learning Outcome. Need to be submitted for each Program-Level Learning Outcome.

Program-Level Learning Outcome: Apply security principles and practices to maintain operations in the presence of risks and threats					
Course(s) that formally assess(es) this program-level learning outcome: ABC 216 - Industrial Control Systems Security					
Assessment Indicator(s) (taken from rubric)	**Teaching and learning activities:** List the most significant teaching and learning activities used by program faculty to facilitate the learning of this indicator in their class(es).	**Graded assignment(s) that formally assesses each indicator at its highest level**	**Performance expectations:** identify the percentage range for each level of performance by replacing the "xx's" below	**Average score for the indicator as a percent**	**How well did the students perform?** (right-click on the checkbox and select 'properties' and 'checked')
Snort: Snort alerting on ICS protocols and placed in correct area of network	Snort is introduced in ABC 140. Students learn how to setup and configure Snort to alert on common types of attacks by instructor demonstration and practice. In ABC 216 student learn how to modify snort rules for ICS protocols and practice these skills in the lab.	Group Project	Below expected levels: 0 – xx % At expected levels: xx – xx % Above expected levels: xx – 100 %	61%	☒ below expected levels ☐ at expected levels ☐ above expected levels
Networking: VLANs and router configured correctly. Traffic restricted via ACLs	Students learn about VLANs and router configuration during the four quarter networking sequence. This assignment is basically a review of those skills, although they must set up a customized network to meet the requirements of the assignment.	Individual applied (hands-on) lab	Below expected levels: 0 – 70 % At expected levels: 71 – 89 % Above expected levels: 90 – 100%	100%	☐ below expected levels ☐ at expected levels ☒ above expected levels

Example for requirement 1d4: **Overall assessment of a Program-Level learning outcome** (please be thorough in all responses). Need to be submitted for each Assessment Indicator(s) in each Program-Level Learning Outcome.

Program-Level Learning Outcome: Apply security principles and practices to maintain operations in the presence of risks and threats	
Course(s) that formally assess(es) this program-level learning outcome: ABC 216 - Industrial Control Systems Security	
Assessment Indicator: Snort: Snort alerting on ICS protocols and placed in correct area of network	
Overall, how well did the students perform on this Program-Level learning outcome? (right-click on the checkbox and select 'properties' and 'checked')	☒ below expected levels ☐ at expected levels ☐ above expected levels
Analyze assessment of indicator results documented by the "Average score for the indicator as a percent" and "How well did the students perform?": What does the information in the previous reporting suggest to you about the performance expectations, the teaching strategies, and student learning?	There are two areas where students consistently underperformed: Snort and CSET. In addition, some topics were basically review and students should have performed better. These include setting up a VPN and the network demonstration. CSET is basically an automated tool for documentation and does not require technical knowledge to run. This was the easiest part of the project but some students did not bother doing it or underperformed. It is very difficult to get students to document their work and this needs to be emphasized more in the program. The Snort part of the project required them to develop new rules for the ICS protocols. Underperformance indicates they may not quite understand how Snort works.
Next steps: Plans for reinforcing effective teaching and learning strategies and for improving student learning (clearly identify what will be done, by whom, by when, and how you will assess the impact of the changes)	More lecture on Snort and writing snort rules in ABC 216. Emphasize Snort in the earlier classes. A preliminary exercise in the CSET tool. More lecturing on Snort and CSET. Assessment will be based on how the students perform on the project in spring of 20XX.
Projected quarter/semester of implementing "next steps"	Spring 20XX
Results of "next steps" implementation – this section is to be completed the following year (describe how the implementation of the above "next steps" impacted teaching and learning in the program)	SNORT was incorporated into ABC 215 as an assignment. This seemed to help students for ABC 216 and some improvement was seen because of this. Additional lectures were given relating to SNORT as well. Drastic improvement could be seen as the class performed up to expected results averaging around 80%. Students were also given additional lectures and resources relating to CSET. This allowed students to be more adept at using CSET and creating appropriate final projects. The results increased as well by about 10%
Suggestions for improving this report or process (if any)	[Suggestion text here]

Example for requirement 1e1: **Knowledge Unit (KU) Alignment for CAE-CD** – The PoS courses are aligned to chosen KUs and KU outcomes (see A. CAE-CD KU requirements below for Designation level). One course may align with multiple KUs. One KU may align to multiple courses. Provide all course outcomes for each course that is aligned with KU(s) and provide a URL or other evidence for the course outcomes indicated at the academic institution via the institutional Web site or within course syllabi. KU alignment is needed for courses that are aligned to the KUs only.

Program of Study Title: BS in Cybersecurity (add more rows if necessary)

Course Number	Course Name	Course Outcomes	KU Alignment	KU Outcomes (Listing only, no assessment of outcomes. KU Topics are recommended and not required for alignment)
ABC 216 *(choose course from submitted PoSs)*	Industrial Control Systems Security	Upon successful completion of this course, each student should be able to... 1. Describe Supervisory Control and Data Acquisition (SCADA) and control systems. 2. Configure SCADA devices. 3. …	(CSF) Cybersecurity Foundations	1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security. 2. Describe potential system attacks and the actors that might perform them. 3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks. 4. Describe appropriate measures to be taken should a system compromise occur. 5. Properly use the Vocabulary associated with cybersecurity.
			(NDF) Network Defense	1. Describe the key concepts in network defense (defense in depth, minimizing exposure, etc.). 2. Explain how network defense tools (firewalls, IDS, etc.) are used to defend against attacks and mitigate vulnerabilities. 3. Analyze how security policies are implemented on systems to protect a network.

Example for requirement 1e2: **Knowledge Unit (KU) Alignment Summary Table for CAE-CD PoS** – The Knowledge Unit (KU) Alignment Summary Table for CAE-CD PoS provides an overview of the Courses-to-KU for the PoS. Below see two examples of KU Alignment Summary Tables.

Example a: KU Alignment Summary Table for Associates Non-Technical CAE-CD PoS with Five Courses in KU Alignment.

Associates Non-Technical CAE-CD (Total 11 KUs)											
PoS Courses in	Foundational			Non-Technical Core					Optional		
KU Alignment	CSF	CSP	ISC	CTH	CPM	PLE	SPM	SRA	BCY	BNW	CSE
INT 110						x				x	
INT 130	x	x	x	x							
INT 210							x				
INT 320								x	x		
INT 420	x				x						x

Column A: Lists only the PoS courses that are aligned to KUs

Cybersecurity Foundational KUs (3)

Non-technical Core KUs (5)

Optional KUs (3)

x An 'x' was placed at the intersection for every KU that is aligned with one/or more courses

Example b: KU Alignment Summary Table for Master Technical CAE-CD PoS with Eight Courses in KU Alignment.

Master Technical CAE-CD (Total 22 KUs)																							
PoS Courses in KU Alignment	Foundational			Technical Core					Optional							Aditional or Graduate Thesis/Dissertation/Equivalent							
	CSF	CSP	ISC	BSP	BNW	NDF	BCY	OSC	NTP	ANT	LCS	CTH	ACR	DFS	NWF	7 KUs for Graduate Project Course							
CISC640								x															
CISC650					x	x			x	x													
CISC680											x												
ISEC615	x	x	x									x											
ISEC620							x						x										
ISEC640				x																			
ISEC650														x	x								
ISEC690																x	x	x	x	x	x	x	x

Column A: Lists only the PoS courses that are aligned to KUs

Cybersecurity Foundational KUs (3)

Technical Core KUs (5)

} Included in the PoS

Optional KUs (7)

Additional KUs (7)

This graduate program uses the Graduate Project course (ISEC690) in lieu of the Additional seven (7) KUs evidence of institutional documentation and process for the term-long Graduate Project course is provided (Criterion 1f)

This graduate program does NOT assume that their students are admitted with foundational and core knowledge (aside from the general program prerequisites) and includes the Cybersecurity Foundational KUs (3) and Technical Core KUs (5) in the program.

x An 'x' was placed at the intersection for every KU that is aligned with one/or more courses

APPENDIX 4 – EXAMPLES OF STUDENT PROFESSIONALISM

Student Professionalism	Examples (not an exhaustive list)	Goals/Objectives
Cybersecurity ethics	- Montreat College - Professionalism and Ethics Toolkit https://www.montreat.edu/cybersecurity/professionalism-ethics-toolkit/ - Montreat College - Cybersecurity Code https://www.montreat.edu/cybersecurity-code/ - Montreat College - Career Readiness Course https://www.montreat.edu/cybersecurity/professionalism-ethics-toolkit/course/ - Montreat College - Internship Handbook with Supervisor Evaluations https://www.montreat.edu/wp-content/uploads/2024/11/Internship-Manual-2024.pdf - Montreat College - Workshops - https://www.montreat.edu/cybersecurity/professionalism-ethics-toolkit/workshops/ - NCAE-C Code of Ethics and Professional Conduct including responsible use of AI (https://www.caecommunity.org/cop-cyber-defense/cop-cd-student-code-of-ethics) - Cybersecurity ethics course or module/topic - Cyber course assignments/independent study - Cybersecurity ethics "bowl"/competition	- Baseline understanding of cybersecurity ethics
Internship, resume preparation, and evaluation	- Cyber career readiness class - Certification preparation - Cybersecurity mentorship, apprenticeships, and bootcamps - Student pre-/post-internship assessment of goals/objectives/competencies (ABCDE) - Internship supervisor feedback on the student's competencies (ABCDE) - Resume preparation and mock interviews activity/assignment - Industry mentorship initiatives (e.g., SANS Cyber Talent Immersion Academy), and Federal workforce programs (e.g., DHS Cybersecurity Talent Initiative)	- Address workplace professional behavior - Manage internship and career expectations - Build cyber resume for private and federal internships/positions
Cybersecurity experiential learning and jobs	- University run Security Operation Center (SOC) - Information Technology (IT) department - Field trip to SOCs	- Enable students to learn cybersecurity skills needed - Address workplace professional behavior - Meet with cybersecurity professionals to understand their work roles, and technical and professional skillsets needed for those work roles
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 and mentors
Cybersecurity competitions and exercises	- NCAE Cyber Games - https://www.ncaecybergames.org/ - NSA Cyber Exercise (NCX) - NSA Codebreaker Challenge – https://nsa-codebreaker.org/ - XPCyber - https://www.xpcyber.com/ - National Cyber League - https://nationalcyberleague.org/	- Provide virtual training environment for participants to develop, practice, and validate their cybersecurity knowledge and skills - Enable participants to learn and demonstrate intangible skills such as problem-solving, teamwork, and

	- Collegiate Cyber Defense Competitions (CCDC) - https://www.nationalccdc.org/ - CyberForce Competition - https://cyberforce.energy.gov/cyberforce competition/ - CSAW - https://www.csaw.io/ - Global Collegiate Penetration Testing Competition - https://cp.tc/ - Other cyber competition	communications
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 and regional conferences/present research papers
Cyber work roles	- DCWF - https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework - NICE Workforce Framework for Cybersecurity - https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-current-versions	- Provide frameworks that identify tasks that are required for cyber work roles - Meet with cybersecurity professionals to understand their work roles, and technical and professional skillsets needed for those work roles - Videos to show different work roles
Community engagement	- Cybersecurity clinics - Cybersecurity awareness training for K-12 and/or seniors	- Enable students to learn and demonstrate intangible skills such as teamwork, communications, and engaging the community - Build professional and peer networks - Build volunteering activities to be included in resume

APPENDIX 5 – CHANGES FROM PRIOR VERSION 2.0 (JUNE 2025)

The following are the changes implemented in this document, version 2.1 (May 2026), from the prior published version 2.0 (June 2025) and effective January 2027:

Page(s)/Requirement:	Overview of Changes:
Overview in p. ii	Update quote and minor text typos corrected.
Throughout the document	Minor text typos corrected.

2026 APPLICATION PROCESS AND ADJUDICATION RUBRIC (APAR) - CYBER DEFENSE WORKING GROUP (CDWG)

Cyber Defense Working Group

NCAE-C PMO Leads

Sheri Kelly, National Security Agency (NSA)

Jason Smith, National Security Agency (NSA)

CAE-CD WG Co-Chairs

Yair Levy, Nova Southeastern University

Anne Kohnke, University of Detroit Mercy

Members

Shankar Banik, The Citadel

Ayad Barsoum, St. Mary's University

Debasis Bhattacharya, University of Hawaii Maui College

Gretchen Bliss, University of Colorado Colorado Springs

Kelli Burgin, Montreat College

Michael Burt, NCAE-C Candidates National Center

Anna Carlin, Fullerton College

Bei-Tseng "Bill" Chu, University of North Carolina – Charlotte

Deanne Cranford-Wesley, North Carolina Central University

Max Gorbachevsky, Utica University

Faisal Kaleem, Metropolitan State University

Stanley Mierzwa, Kean University

Jake Mihevc, Mohawk Valley Community College

Stephen Miller, NCAE-C Reviewers National Center & NCyTE

Michael Nowatkowski, Augusta University

Anthony Pinto, University of West Florida

Chris Rondeau, Bossier Parish Community College

Gary Sparks, Metropolitan Community College

Stu Steiner, Eastern Washington University

Blair Taylor, Towson University

Diego Tibaquirá, Miami-Dade College

Stephen Troupe, Whatcom Community College

Michael Tu, Purdue University Northwest

Tobi West, Coastline College

Michael Whitman, Kennesaw State University