National Centers of Academic Excellence in Cybersecurity

NCAE-C 2024

Designation Requirements and Application Process

For

CAE Cyber Operations (CAE-CO)

Prepared by the

Application Process and Adjudication Rubric (APAR)

Cyber Operations Working Group (COWG)

November 2024

20241101_CAE2022_CAE-CO_Designation_Requirement_Ver2.02

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

OVERVIEW

The following is an overview of the requirements for designation in the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program for **Cyber Operations (CO)** administered by the National Security Agency (NSA). Details on each requirement and application processes are provided in the body of this document. **The CAE Cyber Operations (CAE-CO)** designation is awarded to regionally accredited four-year, and graduate-level academic institutions. The CAE-CO designation, while complementing the CAE Cyber Defense (CAE-CD) designation, provides an in-depth focus on technologies and techniques related to specialized cyber operations such as exploitation, reverse engineering, etc. The program being evaluated, while firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, must educate students on cyber operations in an interdisciplinary manner. Applicant institution must demonstrate that it engages in significant community involvement, academic activities, and institutional practices in cybersecurity, and that the institution has a 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 produce the nation's cyber workforce.

NCAE-C Core Values and Guiding Principles Overview

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

NCAE-C Program Objectives

The objectives of the NCAE-C Program include:

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

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

TABLE OF CONTENTS

OVERVIEW i
NCAE-C Core Values and Guiding Principles Overview i
NCAE-C Program Objectives i
Table of Contents ii
Introduction to the CAE-CO Application Process 1
Justifications 2
Synergistic Approach 2
Definitions 3
PART I: PROGRAM OF STUDY (POS) EVALUATION REQUIREMENTS for CAE-CO 4
Overview 4
Self-Study Overview 4
Institution Details 5
Program of Study (PoS) Evaluation Requirements 6
1. PoS Curriculum 6
2. Students 10
3. Faculty Members 12
4. Continuous Improvement 13
PART II: CAE-CO APPLICATION – NCAE-C DESIGNATION CRITERIA 15
Overview 15
CAE-CO Designation Criteria 16
1. Accreditation 16
2. Institutional Commitment 16
3. Evidence of Sound Cybersecurity Posture and Plan 17
4. Established “Center” for Cybersecurity 17
5. Affirmation of the NCAE-C Core Values and Guiding Principles 18
6. Sustainability 19
7. Professional Development 19
8. Commitment to Support the CAE-CO Program 20
PART III: NCAE-C POST-DESIGNATION REPORTING REQUIREMENTS 21
Overview 21
1. Annual Report of Institutional Metrics 21
2. Maintain Correct Contact Information 23
3. Major Changes to the Designated Program of Study (PoS) 23
4. Continuous Improvement Plan and Process 23
PART IV: RECURRING REVIEW OF NCAE-C DESIGNATION INSTITUTIONAL CRITERIA 24
2. A 5-Year Report on Continuous Improvement 24
Appendix 1 – Mandatory and Optional Knowledge Units list for CAE-CO 25
Appendix 2 – EXAMPLES OF PoS Evaluation Requirements 26
Application Process and Adjudication Rubric (APAR) – Cyber Operations Working Group (COWG) 33

INTRODUCTION TO THE CAE-CO APPLICATION PROCESS

Academic institutions in the United States (U.S.) wishing to be designated a **Center of Academic Excellence in Cybersecurity (CAE-C) in Cyber Operations (CO)** (CAE-CO Designation) for a particular program of study will apply in two (2) parts. The following process applies to both CAE-CO Program of Study (PoS) Validation and CAE-CO Designation. It is proposed that if needed, in Step 5 (Figure 1), the applicant may appear before the Review Committee by webinar to address questions on the application. Only U.S. academic institutions are eligible to apply to the NCAE-C program.

- **CAE-CO Program of Study (PoS) Evaluation:** The first step in the CO two-step 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 improvement information. An institution will then proceed to CAE-CO designation once a PoS is positively evaluated.
- **CAE-CO Designation:** Once a CAE-CO PoS has been successfully evaluated, the institution may pursue a CAE-CO designation. To be eligible for CAE-CO Designation, the academic institutions must hold a current regional accreditation as outlined by the Department of Education (https://www.ed.gov/accreditation), and able to demonstrate all requirements indicated for CAE-CO Designation. No duplicates of any CAE Designation type is allowed.

This process and timeline apply to either application for Program of Study (PoS) Evaluation or for CAE-CO Designation.

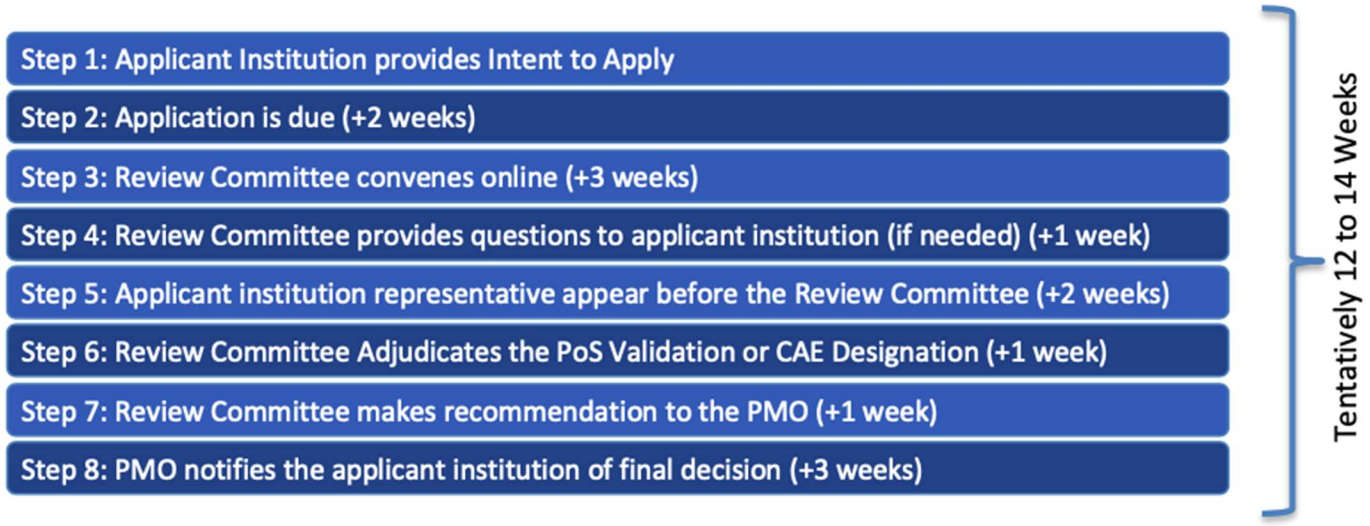

Figure 1. Tentative CAE-CO PoS Evaluation or CAE-CO Designation Application Process and Timeline

Timelines for submission are published by the CAE Candidates National Center and are distributed throughout the year. The program office 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.

Qualified cyber professionals and Subject Matter Experts from NCAE-C Academic Institutions, National Security Agency (NSA), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and other government partners 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, and if needed the Point-of-Contact (POC) will be asked to appear before the Review Committee for further clarifications, followed by a final notification from the PMO (See Figure 1). The PoS will need to have a designated POC. The NCAE-C 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 POC’s (if applicable) from the same academic institution on PoS Validation requirements. **When a new application checklist is submitted from a school that is already CAE-C Designated, the current POC must be notified, regardless of designation type, of intent to apply.** Preferably, the current NCAE-C POC should serve in the same capacity for newly submitted applications. 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 Evaluation and CAE-CO Designation, applicant institutions are provided an optional feature in the application tool to attach a justifications file (in one PDF) that they deem needed to clarify issues during the review process.

Synergistic Approach

To achieve CAE-CO 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). Much of the synergistic approach sufficiency associated with the academic institution will come from the regional (or higher) accreditation associated with the institution. The synergistic approach builds upon existing institutional foundations as driven by regional accreditation rather than duplicating or supplanting them.

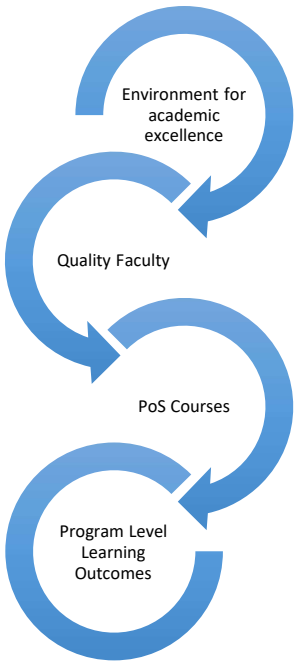

Figure 2. The Synergistic Approach Needed to Become NCAE-C

Definitions

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

An ***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 whom 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.

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

Continuous Improvement (Noted in blue in Figure 3): documentation of a plan, a process, and a regular evaluation schedule that an academic institution and/or academic unit have to enhance the overall quality of its PoS.

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

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

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

PART I: PROGRAM OF STUDY (POS) EVALUATION REQUIREMENTS FOR CAE-CO

Overview

The Program of Study (PoS) Evaluation requirements for the Center of Academic Excellence in Cyber Operations (CAE-CO) programs include evidence of Self-Study that all academic institutions will submit in the application tool. Academic institutions will be required to outline faculty, student, curriculum, and continuous improvement information. In addition, any PoS being submitted for Evaluation 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 3, the CAE CO PoS Evaluation Conceptual Model, provides a graphical representation of the: (1d) Curriculum Map and Plan with the associated documentation, the (1e) KU alignment courses, and (4) Continuous improvement plan, process, and evaluation schedule – see Appendix 3 - Examples 4a to 4c below. The examples provided are to be used as illustration or guide, they are not intended to be a complete assessment of a PoS. No elective 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. Also, no elective courses should be aligned to Mandatory KUs (See Appendix 1). However, both core and elective courses can be aligned to Optional KUs. Additionally, for (1b) Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf) crosswalk alignment, only identification of the category(ies) that the PoS is aligned to, is required. See categories on Table 1, p. 11 of NIST.SP.800.181: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and/or Investigate (IN).

Self-Study Overview

Self-study is required of all CAE-CO applications. It includes the following requirements (See Appendix 3 for relevant examples):

1. PoS Curriculum

a) The Cybersecurity PoS Offered by the Institution
b) NICE Framework 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)

2. Students

a) Student enrollment/graduation in the PoS
b) Cyber Operations Recognized
c) Students work products (papers, assignments, labs, etc.)
d) Student participation in extracurricular activities
e) Students' cybersecurity research
f) Cyber Operations Interdisciplinary Student Exposure

3. Faculty Members

a) Cyber Program 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 Improvement

a) Continuous Improvement plan
b) Continuous Improvement process
c) Regular evaluation schedule

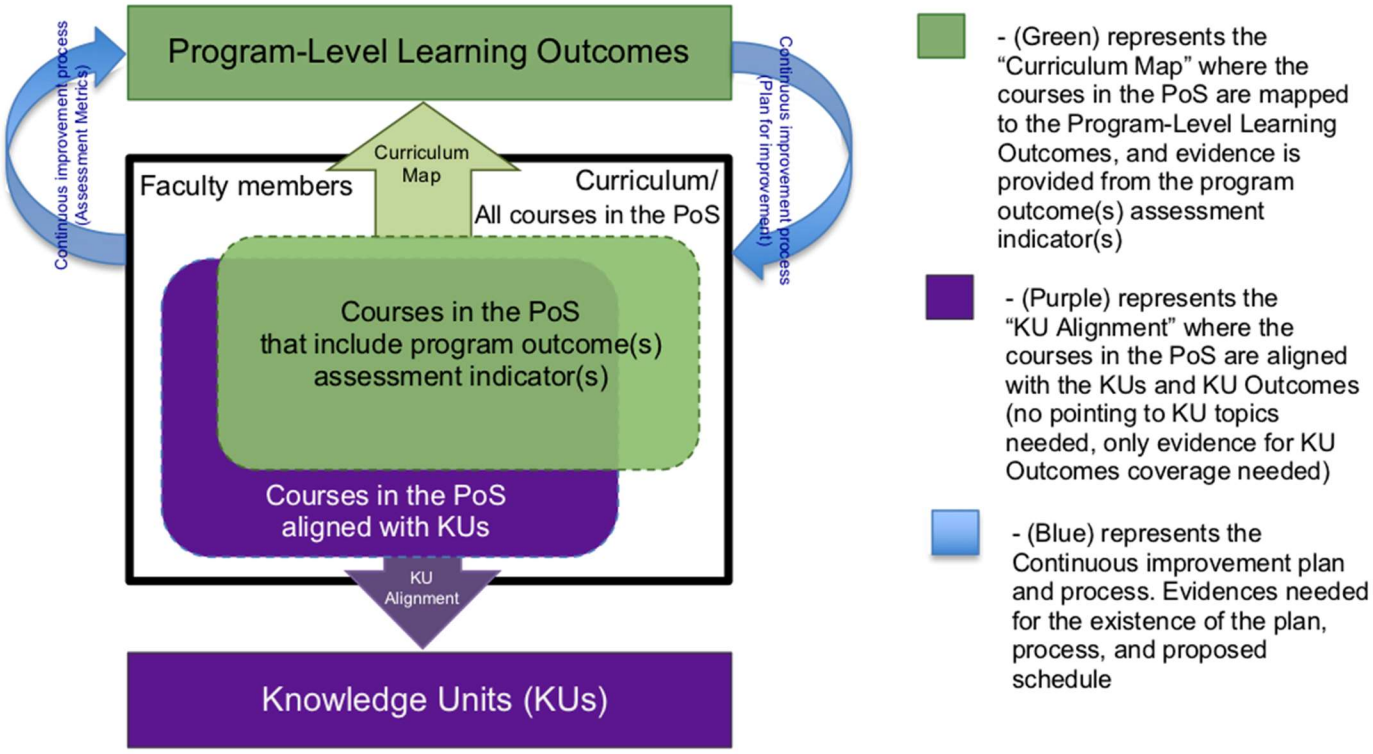

Figure 3. PoS Evaluation Conceptual Model

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
- Provide link to the homepage of the institution (not department)
- Provide the address of the institution

Additional Information for Grant Related Opportunities (Not guaranteed):

Applying academic institutions are highly encouraged to provide further evidence of eligibility for NSA grants for the benefit and ease of applying for grants. Doing so will allow 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 administer 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 screen shot 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 of Study (PoS) Evaluation Requirements

1. PoS Curriculum

A U.S. institution of higher education will first apply by submitting an academic program for Program of Study (PoS). The academic institution must show its curriculum and show that students are enrolled and successfully complete the path and receive recognition. A PoS is required to proceed to CAE-CO Designation. All institutions applying for PoS Evaluation must be U.S. institution and regionally accredited.

PoS is defined as sets of courses that are designed to develop Program-Level learning outcomes in the student population over time. 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 navigation of program plans. Transcripts, or other institutional completion records, can document student completion of evaluated PoS.

CAE-CO Designations have a requirement to align courses to NCAE-C Knowledge Units (KUs) and provide Curriculum Map and Plan (See Figure 3). The Application Tool will simplify the KU alignment as well as the Curriculum Map and Plan submission process. KUs are 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.

a. The Cybersecurity CAE-CO PoS offered by the institution

The applicant will identify the official name of the cybersecurity CAE-CO 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. Completion of the CAE-CO PoS Evaluation should not be advertised or used in marketing. Applicant may not make reference to NCAE-C until applicant receives official approval of the application for CAE-CO Designation. To initiate the application, applicant will first need to identify the cybersecurity type PoS offered by the institution (CO-Bachelor, CO-Masters, or CO-Doctoral) and state the official name of the cybersecurity PoS.

Requirements (All needed):

- State the official name of the cybersecurity type PoS curriculum name (including: degree level, if applicable, minor or concentration). If validated, the PoS name will be displayed on a NCAE-C website list, thus, it must be the official name (Examples: BS in Cyber Operations; BS in Computer Science with Specialization in Cyber Operations; MS in Computer Engineering with concentration in Cyber Operations). ***State **only** the official PoS curriculum name. The text provided will be printed on the validation/designation certificate, if approved. Do NOT include any other text aside from the official PoS curriculum name in this field ***
- Provide a link to the institutional site where the PoS is documented (i.e. link to program's course catalog, curriculum webpage, etc.).
- Identify department(s) official name(s) as it appears in the accreditation where PoS resides.
- Applicant 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.
- Identify the administrative head of academic unit housing the PoS (Dean, Associate dean, Department Chair, etc.) including name, phone number, and e-mail address.
- Identify the Point-of-Contact (POC) for the PoS (Department chair, faculty lead, NCAE-C POC, etc.) including name, phone number, and e-mail address.
- List all courses that are part of the PoS Curriculum Map and Plan (Course Number/Course Name/Course Descriptions as appears in catalog, excluding General Education courses) and identify those that are part of the KU alignment (identify the KU aligned courses in the list).
- Provide evidence for PoS Curriculum Sheet in PDF (See Appendix 3 - Example 1a).

b. NICE Framework Crosswalk Alignment

The applicant will state the cybersecurity PoS crosswalk alignment with the Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf). See categories on Table 1, p. 11 of NIST.SP.800.181: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and/or Investigate (IN).

Requirement:

- Identify the Workforce Framework for Cybersecurity (NICE Framework) category(ies) that the PoS is best aligned to (may check more than one).

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 needed):

- Provide a concise syllabus of each course in the KU Alignment (all must be from the last three (3) years) (in PDF).
- For KU aligned courses that require applied labs 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 (3) years).
- 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 (3) years) (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 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 needed):

- State the Program-Level Learning Outcomes of the PoS.
- Provide documentation of the Program-Level Learning Outcomes (link to academic institutional webpage with the outcomes and/or PDF document of the outcomes).
- Provide evidence for the Program-Level Learning Outcomes *Curriculum Map and Plan* that identified the PoS courses where the outcomes are assessed (Combined to single PDF) (See Appx. 3 example 1d1).
- Provide documentation for the *General Information* for each Program-Level Learning Outcome (Combined to 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; (c) Course used for the assessment; (d) Total number of assessed students (See Appx. 3 example 1d2).
- Provide documentation for the *Assessment of Indicators* for each Program-Level Learning Outcome (Combined to 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).

- Provide documentation for the *Overall Assessment Information* of each Program-Level Learning Outcome (Combined to 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 Knowledge Units (KU) criterion is the heart of the Cyber Operations (CO) designation. More than any other designation criteria, it paints the target for providing a rigorous cyber operations education.

The CO Student Outcomes (SOs) outline the core attributes of cyber operators. The KUs are designed to produce graduates that meet the SOs. Mandatory KUs (MKUs) form the main knowledge and skills of cyber operators. All graduates of every CO program must cover all the MKUs. A set of Optional KUs (OKUs) are chosen by schools based on their specific areas of expertise within the field of cyber operations. This division of mandatory and optional KUs helps diversify the national collection of CAE-CO designated programs.

In order to operate effectively cyber operators must have a deeply technical understanding of the underlying architectures and protocols of cyberspace. Therefore, CO programs of study (PoS) must be based on a computer science or computer engineering core. The main material required in the program core is covered in M2: Computer Science Foundations. On top of the foundational academic program schools will need to offer several specialized courses in cyber in order to meet the KU requirements for academic validation.

Cyber Operations Student Outcomes

Graduates of cyber operation programs will be able to:

1. Operate ethically at all times, respect the rights of all citizens, and obey all applicable laws and authorities.
2. Apply logical and algorithmic thinking to navigate and produce effects in cyberspace.
3. Detail the architecture and functions of operating systems and computer networks.
4. Develop systems software using assembly and low-level languages.
5. Describe the motivations, methods, and goals of cyber threat actors.
6. Protect the confidentiality and integrity of data at rest and in transit.
7. Perform static and dynamic analysis of software to identify vulnerabilities.
8. Reverse engineer software and network protocols.
9. Secure data, computer systems, and networks from cyber attacks.
10. Plan and execute offensive cyber operations in contested environments.

Mandatory Knowledge Units

The MKUs are organized logically, starting with foundational knowledge and culminating with the specialized knowledge and skills needed by cyber operators. All programs must align core courses to all 10 MKUs. No elective courses should be aligned to MKUs because all graduates of the PoS must take every course that either partially or fully covers every MKU.

Optional Knowledge Units

OKUs represent specialized areas of study connected to cyber operations. In most cases a single course similarly named is required to fully cover an OKU.

All graduates of the PoS must take courses that fully cover at least 4 OKUs. Both core and elective classes can be aligned to OKUs. If every graduate from a PoS takes courses that fully cover more than 4 OKUs, still only 4 OKUs should be aligned – it is up to the applicant to select "the best" 4. Aligning more than the minimum OKUs causes extra work for both schools and program reviewers and there are no added benefits.

Only if there are multiple elective pathways through a PoS may a program align more than 4 OKUs. In this case, every pathway that leads to graduation must cover at least 4 OKUs. If alternate pathways cover non-overlapping OKUs, it will be necessary to align more than 4 OKUs, but still only the minimum set of OKUs should be aligned.

Aligning Courses to KUs

Every KU contains learning outcomes and topics. There are no fixed requirements for the number of core hours or semester weeks needed to cover a KU, but the KU learning outcomes help to define the appropriate depth of coverage. The KU Notes provide further guidance but do not define strict requirements. While it is not required that every learning outcome be explicitly assessed as written, applicant schools should be able to defend their coverage of the learning outcomes. All KU topics must be addressed by the aligned courses. KU topics are deliberately broad so schools can apply their discretion and expertise. More specific guidance is available if requested.

A KU may be covered by one or more courses. When multiple courses are aligned to a KU, it is assumed that all of them partially cover the KU and that together they fully cover the KU. Programs should never align multiple courses to a KU purely to show strength of coverage. There is no such thing as 110% coverage; either a KU is fully covered or it is not. If there are multiple courses that fully cover a KU, then schools should align only the minimal set or the single course with the primary coverage. 4 or more courses aligned to a single KU may be more of an indication of poor KU coverage than strong because it risks diluting the KU.

Single courses can fully and partially cover more than 1 KU. There is no limit on the number of KUs that can be aligned to a single course, but 4 or more KUs against a single course may be an indication of weak KU coverage.

Hands-on Activities

Cyber operations is an applied academic discipline not a theoretical one. Students learn the knowledge and skills they need by doing. Therefore, the heavy use of hands-on labs and programming assignments is the best practice in cyber operations education. It is expected that students graduating from CO-designated programs will be adept at operating in virtualized sandboxed environments. Coverage of every KU (with the exception of M1: Cyber Policy, Law, and Ethics) must include hands-on activities. Examples of hands-on activities include configuring and deploying cyber tools, writing and executing programs and scripts, and conducting tasks in defensive and offensive cyber operations.

Prerequisites

The KUs are not intended to define a complete Bachelor of Science program of study and do not identify all prerequisites. For example, an introductory programming course is needed to support M5: Systems Programming, but it is not specified. Additionally, not all core computer science and computer engineering content is addressed by the KUs. For example, computer science programs typically require a course in programming language theory, but there are no KUs for this topic. On the other hand, core computer science topics such as algorithms and data structures are critical for cyber operators so they are addressed in M2: Computer Science Foundations.

Graduate programs

Both graduate and undergraduate programs use the same set of KUs, but graduate programs may be held to a more in-depth standard of coverage. Graduate programs may align KUs to prerequisite courses that are required for admittance into the program but that are not taught in the graduate PoS itself.

Special Note on Definitions

The NIST Computer Security Resource Center glossary provides helpful definitions and links to primary sources for many of the technical terms used in the KUs.

Requirements:

- Provide a narrative on the description of the PoS, explain the overall KU alignment to the PoS.
- Provide the KU Alignment Summary Table for the PoS (in PDF) (See Appendix 3 - Example 1e2).
- Identify PoS courses that are part of the KU alignment.
- Provide *course learning outcomes* for all KU aligned courses as documented in official academic institution documentation (Course catalog, program website, etc.).
- In the case of multiple sections of a KU aligned course, provide documentation on how they all are managed in some form of equivalency.
- Provide the academic year each KU aligned course was last offered.

CAE-CO PoS Evaluation KUs:

Appendix 1 provides a list of **Mandatory and Optional Knowledge Units for the CAE-CO Program.** The full list and details on each subject can be found at:
https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-co_knowledge_units.pdf

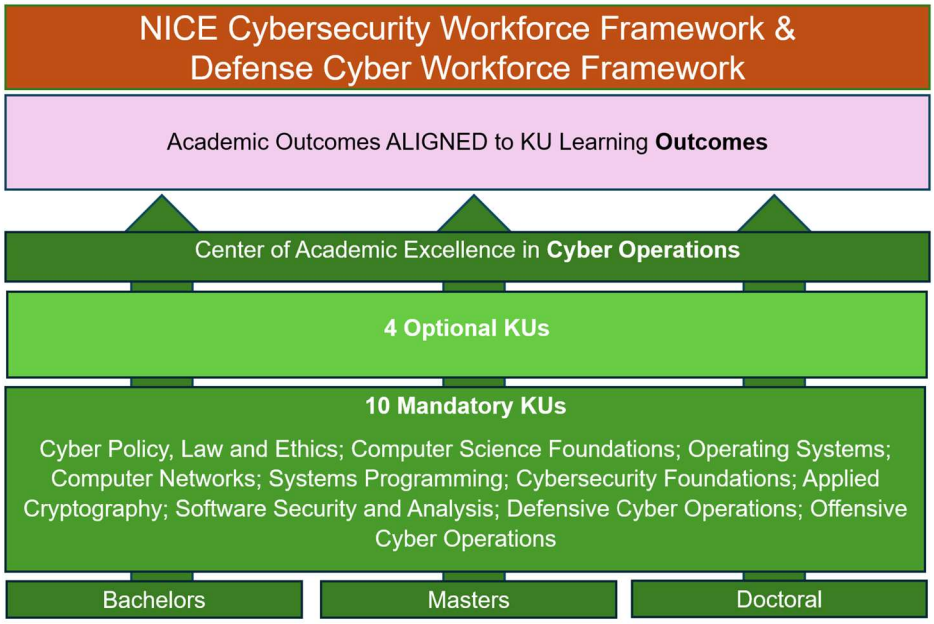

Figure 4. CAE-CO Knowledge Units Alignment Requirements

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

The applicant will demonstrate that the PoS submitted has been offered for a minimum of three (3) 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 (3) students should be used to document actual attainment of the Program-Level Learning Outcomes as defined in the PoS.

Requirements (All needed):

- Provide student enrollment (unduplicated/headcount) in PoS for the last three (3) years (each year separately)
- Provide official institutional letter for the enrollment (unduplicated/headcount) and graduation in the PoS for the last three (3) years, each year separately (letter from Registrar, Institutional Effectiveness, or equivalent) (in PDF)
- Provide at least three (3) redacted student transcripts, showing the student graduated or attended within the last three (3) years and clearly highlight the courses taken that are in the KUs alignment. All courses aligned to the 10 Mandatory KUs and at least four (4) Optional KUs (aligned courses for Optional KUs must be at the institution) must appear on the transcripts. Provide a cover page for each transcript to state the 10 Mandatory KUs and the four (4) (or more) Optional KUs that each given transcript is aligned with (combined to a single PDF per transcript).

b. Cyber Operations Recognized

Cyber operations must be explicitly recognized as a degree program or a focus area or a specialization or a concentration and students must meet requirements to be awarded such recognition. Students who participate sufficiently in the cyber operations curriculum (i.e. take and pass courses that completely satisfy all of the mandatory KU requirements and at least four (4) of the optional KU requirements described PoS Evaluation for CO) must be distinguished from other students through the awarding of a degree, certificate, or a reference to a focus area or specialization on their transcript and/or degree.

Requirement:

- Provide a sample certificate, draft of degree, certificate, or a reference to a focus area or specialization on their transcript and/or degree to be issued to students indicating they completed the NSA Evaluated PoS and if the academic institution is also a NCAE-C, should recognize their completion from a NCAE-C designated academic institution.

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 needed):

- Provide samples of six (6) students' work products from six (6) different assignments (six (6) files total). Samples can be (but not limited to): papers, assignments, projects, presentations, lab exercises, test questions from at least two (2) 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's work (name redacted) into a single file for each of the student work (in six (6) separate PDFs).

d. Student Participation in Extracurricular Activities

Documentation of student participation in extracurricular activities can demonstrate program opportunities for students.

Requirements (All needed):

- Provide evidence of three (3) student participation in extracurricular activities within the last three (3) years, which may include (but not limited to): experiential learning activities, local/regional/national cyber exercises and competitions, outreach to community colleges and high schools, computer check-up days, CAE-CO Summer Internship Program, industry guest lectures, etc.
- Provide dates and description for each evidence provided.

e. Students' Cybersecurity Research

Students' cybersecurity research products demonstrate deeper breath of the PoS. Sample student cybersecurity research products are important to evaluate the quality and depth of students' research work during the PoS.

Requirement:

- Provide samples of three (3) students' cybersecurity research products (papers, assignments, projects, presentations, etc.) (three (3) files total). Student names should be removed prior to submission. Students' cybersecurity research products should not include grades or grading comments, only the original students work. Combine the guidelines (i.e. what students are asked to do) of the cybersecurity research, indicate the course it is associated with, and one sample student work (name redacted) into a single file for each of the student work provided (in three (3) separate PDFs).

f. Cyber Operations Interdisciplinary Student Exposure

The goal of the CAE-CO program is to produce graduating students with a well-rounded educational foundation that enables them to better function in the world of specialized cyber operations. To best achieve this, a designated CAE-CO program must expose students to cyber operations in an interdisciplinary manner. Cyber operations must not be treated as an isolated specialization, with classes focused solely on cyber operations tools, techniques, and principles. Instead, a cyber operations student must be exposed to the underlying technologies that make up the cyber domain, as well as the policy, social, legal and ethical aspects of conducting cyber operations. This should be done by integrating cyber operations information, as appropriate, into the courses of many other academic disciplines (e.g., computer science, engineering, math, IT, business, law), as well as integrating elements of those disciplines into cyber operations classes, when they do exist as stand-alone offerings (which, for some topics, may be appropriate to do so). Thus, a curriculum suitable to satisfy the academic interdisciplinary requirements for PoS Evaluation as a cyber operations program should demonstrate that the relevant information from these disciplines has been integrated into the cyber operations PoS courses.

Requirements (All needed):

- Identify the PoS courses that interdisciplinary components from other disciplines (i.e. policy, social, human factor, legal and ethical aspects of conducting cyber operations) have been integrated into the cyber operations PoS courses
- Provide samples of the work of three (3) different students from three (3) different courses (one example from each course) where interdisciplinary components from other disciplines have been integrated into the cyber operations PoS courses. Students sample work should not include grades or grading comments, only the original students' work. Combine the guidelines (i.e. what students are asked to do) of the work or assignment, the course it is associated with, and sample work from one student (name redacted) into a single file for each of the three (3) courses (Three (3) separate PDFs).

3. <u>Faculty Members</u>

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 CAE-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 (3) 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 needed):

- Identify the Point-of-Contact (POC) for the PoS (Department chair, faculty lead, NCAE-C POC, etc.) including name, phone number, and e-mail address.
- Identify the alternate POC for the PoS including name, phone number, and e-mail address.
- 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.
- Provide a 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), publications, 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) (One PDF per faculty member teaching course(s) in the KU alignment, 10 max).
- 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 (3) years. Evidence must include link(s), such as: link to student clubs, link to cyber 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 (all links and evidence information provided within a single PDF).
- Provide evidence for institutional process of faculty promotion/reappointment (e.g. Faculty Policy Manual) (in PDF).

4. <u>Continuous Improvement</u>

A key element to ensure vitality and functionality over time is a strong continuous improvement plan, process, and regular evaluation schedule. A process-driven continuous 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 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 improvement plan, process, and regular evaluation schedule are expected to match those that the academic institution files with their accreditation body(ies).

a. Continuous Improvement Plan for the PoS

The *Continuous Improvement Plan* for the PoS commonly includes four (4) parts that the academic institution and/or academic unit documents to enhance the overall quality of its PoS:

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

Requirement:

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

b. Continuous Improvement Process for the PoS

The *Continuous Improvement Process* commonly includes the four (4) parts of the plan indicated above with a clearly identified end of a given process cycle (See Figure 5). 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 Improvement Process cycle.

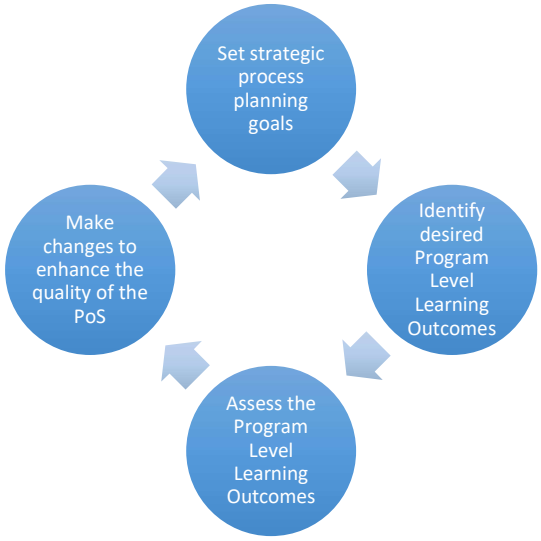

Figure 5. Continuous Improvement - Regular Evaluation Cycle

Requirement:

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

c. Continuous Improvement - Regular Evaluation Schedule for the PoS

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

Requirement:

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

PART II: CAE-CO APPLICATION – NCAE-C DESIGNATION CRITERIA

Overview

The table below provides the required criteria for CAE-CO Designation. All data for CAE-CO designation is now stored in an online Application Tool provided by the NCAE-C PMO. To improve accountability, the history and purity of the data is documented.

Table II.1. Summary of CAE-CO Designation Required Criteria

1. Accreditation: The academic institution must be U.S. institution of higher education and regionally accredited to hold any NCAE-C designation.
2. Institutional Commitment: A letter of intent and endorsement, signed by the Provost or higher, documenting that the institution is aware of the expectations and responsibilities associated with the 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 Evaluated program. 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 (3) 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. Professional Development: The institution must provide evidence of faculty and student access to cybersecurity professional development including time release and/or financial support for faculty (attendance in cybersecurity training/events, attaining certificates/further education, etc.), connection to industry/practitioners (e.g., guest lecturers working in the cybersecurity industry and government, faculty exchange program with industry and/or government, internship opportunities for students, summer research programs for faculty, etc.). Provide fliers, posters, letters, etc.
8. Commitment to Support the CAE-CO Program: Support could be in the form of student applicants to the CAE-Cyber Operations Summer Internship Program, comprehensive faculty participation in Knowledge Unit review and changes, mentorship of another institution applying for the CAE-CO designation, and/or faculty support in the form of briefing or teaching during the CAE-Cyber Operations Summer Internship Program.

CAE-CO 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-CO, 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-CO applicants, both initial and at re-designation.

1. Accreditation

The academic institution must be U.S. institution of higher education and regionally accredited, as outlined by the Department of Education (http://ope.ed.gov/accreditation/), to hold any NCAE-C designation.

Requirement:

- 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 NCAE-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 Community Symposium each year; regular communication with the NCAE-C PMO, the CAE Community, and the CAE Regional Hubs (CRH); 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 needed):

- Provide a letter of intent and endorsement to participate in the NCAE-C program (in PDF, do not mail) that:
  - Is written on official institution letterhead, signed by the Provost or higher and addressed to:
    National Security Agency
    Attn: CAE Program Director
    9800 Savage Road
    Ft. Meade, MD 20755-6804
  - Identifies regional accreditation information.
  - Expresses institutional commitment to excellence in the cybersecurity field.
  - Identify and provide institutional support of an established "Center" for Cybersecurity within the institution.
  - Identify the NCAE-C Point of Contact (POC) from the institution.
  - Identify the name of a designated NCAE-C Institutional Accounts Administrator (A person who oversees the NCAE-C accounts across the institution - one who is authorized to switch POCs, activate new users, etc.)
  - Lists the program of study supporting the requested designation.
- Provide acknowledgement to follow the minimum participation expectations of a NCAE-C:
  - Submission of an Annual Report with all required information.
  - Attendance at either (or both) the NCAE-C Principal's Meeting and CAE Community Symposium each year.

- Regular communication with the NCAE-C PMO, the CAE Community, and the CAE Regional Resource Center, including responding to email, offers input and suggestions for workshops, programs, program decisions, etc.
- 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 Tech Talks or CAE Forum 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 needed):

- 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).
- Provide the name, title, and job description for the individual responsible for the institution cybersecurity program.
- 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 (6) 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 needed):

- 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 Evaluated PoS.
  - Faculty members.
  - Links to student cybersecurity activities available to students at the institution and beyond.
  - News that include 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. Affirmation of the NCAE-C Core Values and Guiding Principles

NCAE-C at the academic institutions are 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 (3) Core Values (not to be submitted, affirmed only).

1. **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.

2. **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.

3. **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 Evaluated program are needed to run the continuous 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 to be successful.

Requirements (all needed):

- 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.
- Provide CV of the administrative head of academic unit housing the established "Center" for Cybersecurity (in PDF).
- 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.
- Provide CV of the POC and indicate year the individual joined the academic institution (in PDF).
- 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.
- Provide CV of the NCAE-C Designation (one applying for) and/or established "Center" for Cybersecurity alternate POC (in PDF).

7. Professional Development

Professional development for faculty and students 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 by both faculty and student 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, internship opportunities for students, joint events with the institutional career development and student job placement center focused on cybersecurity, etc. Faculty development maybe in the form of encouragement and time release and/or financial support to attend and participate in cybersecurity training, professional certifications, relevant conferences, faculty exchange program with industry and/or government, summer research programs for faculty, and/or other events are critical. Identifying these professional development opportunities for faculty and students 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 it is housed at. What is important is that these activities are available to faculty and students, while occurring regularly during the academic year.

Requirement:

- Provide six (6) separate examples of professional development opportunities provided to faculty and students over the past three (3) years. Evidence files can be fliers, posters, letters, attendance records, or other evidence of professional development for faculty and students (in six (6) different PDFs).

8. Commitment to Support the CAE-CO Program

The CAE-CO applying institution must demonstrate commitment to the CAE-CO program. Examples of support could be in the form of student participation in the CAE-Cyber Operations Summer Internship Program, participation at advanced CO competitions. Moreover, comprehensive faculty participation in KU review and changes, faculty participation in CAE-CO related activities offered by the PMO, and faculty support in the form of acting as a mentor or application reviewer, participation on working groups, supporting program initiatives, briefing or teaching during the CAE-Cyber Operations Summer Internship Program, Tech Talks and/or CAE Forum webinars.

Requirement:

- Provide evidence that the institution encourages and supports the success of the CAE-CO Program. First-time applicants to the CAE-CO Program should provide the supporting documents for 8a, existing CAE-CO institutions applying for redesignation should provide the supporting documents for 8b1 to 8b5 (in PDF).

  8a. ***For first-time applications to the CAE-CO Program*****:** applicants must make a stated commitment to support the CAE-CO Program which is demonstrated with the official signature applied to this CAE-CO application and checking the corresponding box in the application tool to attest such commitment. Examples of support could be in the form of student applicants to the CAE-CO Summer Program, comprehensive faculty participation in Knowledge Unit review and updates, mentorship of another institution applying for the CAE-CO designation, and/or faculty support in the form of briefing or teaching during the CAE-CO Summer Program (Combined into one PDF).

  8b. ***For redesignation applications to the CAE-CO Program*****:** applicants upload documentation (8b1 to 8b5) in the application tool to show how the applying institution has supported the CAE-CO Program which must include support with, at a minimum, two (2) of the five (5) options below, over the course of the past five-year CAE-CO designation window (Combined into one PDF).

  8b1. Provide CAE student applicants to the CAE-CO Summer Program.

  8b2. Faculty participation in Knowledge Unit review and updates.

  8b3. Mentorship of another institution applying for the CAE-CO Designation.

  8b4. Faculty support in the form of briefing or teaching during the CAE-CO Summer Program.

  8b5. Other support for the CAE-CO program. Please provide additional detailed description of this support in the justifications file. Checking this box without providing valid justification will not be counted.

PART III: NCAE-C POST-DESIGNATION REPORTING REQUIREMENTS

Overview

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

Continuous Improvement Plan and Process

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

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 institution PoC will attend an orientation meeting in conjunction with their designation ceremony or within six (6) months of designation date.
- The appointed POC is expected to represent the academic institutions by participating in program activities and projects. Participation may include, but is not limited to, acting as an Advisor, Mentor, or Reviewer; participation in program management Working Groups; providing input on questions and projects sponsored by the PMO; contribute curriculum/resources for the use of NCAE-C designated institutions.
- Submit annual report on or before the due date established by the NSA PMO
- Send a Program Representative to an annual CAE Community Symposium and/or the annual POC Meeting and/or regional CAE Community Meetings
- Maintain designated program
- Maintain continuous 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 (January 30).

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 IV.1 for time-dependent additional consequences).

Table IV.1. 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 Evaluation 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 Evaluation and/or CAE 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 Evaluation 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.

3. Major Changes to the Designated Program of Study (PoS)

It is the role of the POC and/or other institutional staff overseeing the NCAE-C designation to ensure that the information about the evaluated PoS(s) is/are up to date and reflecting the current courses in the program, the KU alignment, as well as Curriculum Map and Plan. Failure to keep evaluated PoS(s)' information up to date, 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.

4. Continuous Improvement Plan and Process

A strong continuous 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 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 (2) 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 (3) 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 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 (CAE-CD, CAE-CO, & CAE-R) must formally renew their PoS(s) Evaluation and NCAE-C designation every five (5) years in accordance with the Re-Designation requirements available at:

https://public.cyber.mil/ncae-c/documents-library/

1. A 5-Year Report of Institutional Metrics

An aggregated document of the past five (5) Annual Reports of Institutional Metrics (See IV.1 above).

2. A 5-Year Report on Continuous Improvement

An aggregated document of the past five (5) years changes and progress as it pertains to the Continuous Improvement Plan and Process (See IV.4 above).

APPENDIX 1 – MANDATORY AND OPTIONAL KNOWLEDGE UNITS LIST FOR CAE-CO

CAE-CO KUs valid after October 2024:

Mandatory – 10 required	Optional – 4 of 11 required
M1: Cyber Policy, Law, and Ethics	**O1: Programmable Logic**
M2: Computer Science Foundations	**O2: Computer Architecture**
M3: Operating Systems	**O3: Microcontrollers**
M4: Computer Networks	**O4: Hardware Reverse Engineering**
M5: Systems Programming	**O5: Cyber Forensics**
M6: Cybersecurity Foundations	**O6: Wireless and Mobile Security**
M7: Applied Cryptography	**O7: Virtualization**
M8: Software Reverse Engineering	**O8: Cloud Security**
M9: Defensive Cyber Operations	**O9: Critical Infrastructure Security**
M10: Offensive Cyber Operations	**O10: Cyber Risk Management**
	O11: Game Theory
Candidate Optional Knowledge Units	
Memory Forensics	
Machine Learning	
Artificial Intelligence	
Cryptanalysis	
Human Factors in Information Security	
Cyber Operations Policy and Doctrine	

CO KUs Revision Proposal_v1.docx (cyber.mil)

APPENDIX 2 – EXAMPLES OF POS EVALUATION REQUIREMENTS

Example for requirement 1a: CAE-CO PoS Curriculum Sheet:

Cyber Operations, B.S.

Graduates with a Bachelor of Science in Cyber Operations have a strong background in computing and networking. They are well prepared to enter one of the fastest growing business areas in the twenty-first century and typically assume jobs such as Computer Security Analyst, Web Security Manager, Webmaster, Database Manager, and Networking Analyst.

Each graduate will have an understanding of network security, computer security, database design, computer programming - including current client-side and server-side technologies, intranets, communications protocols, and privacy.

Students in this program may be eligible for the Fast Track program. Contact the Beacom College of Computer and Cyber Sciences.

System-wide General Education Requirement (30 Credits)

Majors who test directly into MATH 201 will not need to complete MATH 114, but must take 3 credits of general electives.

Required Courses (78 Credits)

- CIS 275 - Web Application Programming I 3 credits
- CIS 375 - Web Application Programming II 3 credits
- CSC 105 - Introduction to Computers 3 credits
- CSC 134 - Introduction to Cyber Operations 3 credits
- CSC 150 - Computer Science I 3 credits
- CSC 234 - Software Security 3 credits
- CSC 250 - Computer Science II 3 credits
- CSC 300 - Data Structures 3 credits
- CSC 314 - Assembly Language 3 credits
- CSC 321 - Information Security Management 3 credits
- CSC 328 - Operating Environments 3 credits
- CSC 163 - Hardware, Virtualization, and Data Communication 3 credits
- CSC 285 - Networking I 3 credits
- CSC 385 - Networking II 3 credits
- CSC 404 - Foundation of Computation 3 credits
- CSC 420 - Cellular and Mobile Communications 3 credits
- CSC 428 - Reverse Engineering 3 credits
- CSC 432 - Malware Analysis 3 credits
- CSC 436 - Offensive Network Security 3 credits
- CSC 437 - Survey of Enterprise Systems 3 credits
- CSC 438 - Defensive Network Security 3 credits
- CSC 456 - Operating Systems 3 credits
- MATH 201 - Introduction to Discrete Mathematics 3 credits
- CIS/CSC 300/400 or MATH 123 and above, except CIS 350. (9 credits)

Electives (12 Credits)

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

Program-Level Learning Outcomes Curriculum Map and Plan
Program Name: BS in Cybersecurity
Updated: 2020.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 (2020-21)	R	R	R	R
2. *[Program-Level Learning Outcome 2, Ex. "Communicate professionally with customers and co-workers"]*				I			R	R	A (2020-21)				
3. *[Program-Level Learning Outcome 3]*			I		R	R	R	R	R	R	R	R	A (2021-22)
4. *[Program-Level Learning Outcome 4]*										I	R	R	A (2021-22)
5. *[Program-Level Learning Outcome 5]*						A (2019-20)	R	R					
6. *[Program-Level Learning Outcome 6]*	I	R	A (2019-20)										

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 Name: MS in Cybersecurity Management
Updated: 2020.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 (2020-21)
3. *[Program-Level Learning Outcome 3]*	A1			A2	
4. *[Program-Level Learning Outcome 4]*	A1				A2 (2020-21)
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	09-20-2018
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 2020)	Winter 2020

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 (4) 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-CO** – The PoS courses are aligned to chosen KUs and KU outcomes. 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 Name: 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. …	Networking (hands-on labs required) (M4)	Students will have a thorough understanding of how networks work at the infrastructure, network and applications layers; how they transfer data; how network protocols work to enable communication; and how the lower-level network layers support the upper ones. They will have a thorough knowledge of the major network protocols that enable communications and data transfer.
			Security Fundamental Principles (i.e., first Principles) (M8)	1. Students will possess a thorough understanding of the fundamental principles underlying cyber security, how these principles interrelate and are typically employed to achieve assured solutions, the mechanisms that may be built from or due to these principles. 2. Given a particular scenario, students will be able to identify which fundamental security design principles are in play, how they interrelate and methods in which they should be applied to develop systems worthy of trust. 3. Students will understand how failures in fundamental security design principles can lead to system vulnerabilities that can be exploited as part of an offensive cyber operation.

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

Example a: KU Alignment Summary Table for Bachelor CAE-CO PoS with 10 Courses in KU Alignment.

CAE-CO Program (14 KUs)														
PoS Courses in KU Alignment	10 Mandatory KUs										4 Optional KUs			
	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	O1	O2	O3	O5
CS2000: Data Structures		X												
CS2500: Algorithms		X												
CS3000: Programming in C					X									
CS3200: Operating Systems			X											
CS3500: Computer Networks				X										
CY1000: Intro to Cyber	X					X								
CY2200: Cyber Defense						X	X							
CY2500: Cyber Forensics														X
CY3000: Systems Programming					X									
CY3500: Software Reverse Engineering								X						
CY4000: Cyber Operations									X	X				
CY4200: Secure Software Enginering									X					
CPE2000: Digital Logic Design		X									X			
CPE2300: Computer Architecture												X		
CPE2500: Microcontrollers													X	
MATH2200: Discrete Math		X												

Column A: List only the courses that are aligned to KUs

10 Mandatory KUs

4 Optional KUs

X An 'X' is placed at the intersection of for every KU that is aligned with one or more courses

APPLICATION PROCESS AND ADJUDICATION RUBRIC (APAR) – CYBER OPERATIONS WORKING GROUP (COWG)

Cyber Operations Working Group

Co-Chairs

Drew Hamilton, Texas A&M University

Seth Hamman, Cedarville University

Members

Shankar Banik, Citadel

Annie Becker, National Security Agency

John Franco, University of Cincinnati

Salamah Salamah, University of Texas at El Paso

Jason Smith, National Security Agency

The APAR-COWG would like to thank Lynne Clark, Art Conklin, Tony Coulson, Karen Leuschner, Lori Pfannenstein, and Corrinne Sande for their foundational drafts that led to this document. Additionally, the APAR-COWG would like to thank the following individuals from the Cyber Defense (CD) working group for their foundational work on the CD Requirements Document from which this document emerged from: Yair Levy (Nova Southeastern University), Eric Berkowitz (College of Lake County), Gretchen Bliss (University of Colorado Colorado Springs), Chutima Boonthum-Denecke (Hampton University), Marvin L. Bright (Bowie State University), Eric Brown (Tennessee Tech University), Michael Burt (Prince George's Community College), lan Carter (Green River College), Bill Chu (University of North Carolina – Charlotte), Jane Cothran (Trident Technical College), Jose R. de la Cruz (Polytechnic University of Puerto Rico), Erik Fretheim (Western Washington University), Ernie Friend (Florida State College at Jacksonville), Greg Gogolin (Ferris State University), Mark Hufe (Wilmington University), Faisal Kaleem (Metropolitan State University), Anne Kohnke (University of Detroit Mercy), Margaret Leary (Northern Virginia Community College), Xiuwen Liu (Florida State University), Laura Malave (St. Petersburg College), Kalyan Mondal (Fairleigh Dickinson University), Kim Muschalek (San Antonio College), Anthony Pinto (University of West Florida), Cheryl Purdy (Owensboro Community and Technical College), James Ramsay (University of New Hampshire), Syed Raza (Talladega College), Chris Rondeau (Bossier Parish Community College), Corrinne Sande (Whatcom Community College), Ambareen Siraj (Tennessee Tech University), Ping Wang (Robert Morris University), Deanne Wesley (Forsyth Technical Community College), and Michael Whitman (Kennesaw State University).