National Centers of Academic Excellence in Cybersecurity

CAE 2021

Proposed Designation Requirements and Application Process

For

CAE-Cyber Defense (CAE-CD)

Prepared by the

Application Process and Adjudication Rubric (APAR)

Working Group (WG)

June 2021

OVERVIEW

The following is an overview of the requirements for designation in the National Centers of Academic Excellence in Cybersecurity (CAE-C) program for **Cyber Defense (CD)** 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 Defense (CAE-CD)** designation is awarded to regionally accredited academic institutions offering cybersecurity-related degrees including majors, minors, and/or certificates at the Associates, Bachelors and graduate levels. Applicant institution must demonstrate that it engages in significant community involvement, academic activities, and institutional practices in cybersecurity, and that the institution has one or more Program(s) of Study (PoS) under consideration meeting the requirements set forth in this document. The goal of the CAE-C program is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

CAE-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.

CAE-C Program Objectives

The objectives of the CAE-C Program include:

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

DRAFT

TABLE OF CONTENTS

Overview i
CAE-C Core Values and Guiding Principles Overview i
CAE-C Program Objectives i
Table of Contents ii
Introduction to the CAE-CD Application Process 1
Justifications 2
Synergistic Approach 2
Definitions 3
PART I: PROGRAM OF STUDY (POS) VALIDATION REQUIREMENTS for CAE-CD 4
Overview 4
Self-Study Overview 4
Institution Details 5
Program(s) of Study (PoS) Validation Requirements 6
1. PoS Curriculum 6
2. Students 10
3. Faculty Members 11
4. Continuous Improvement 12
PART II: CAE-CD APPLICATION – CAE-C DESIGNATION CRITERIA 14
Overview 14
CAE-CD Designation Criteria 14
1. Accreditation 14
2. Institution Commitment 15
3. Evidences of Sound Cybersecurity Posture and Plan 15
4. Established "Center" for Cybersecurity 16
5. Affirmation of the CAE Core Values and Guiding Principles 16
6. Sustainability 17
7. Professional Development 18
8. Cybersecurity Academic Integration 18
9. Outreach 19
10. Transfer of Credit/Articulation Agreements 20
PART III: CAE-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 Designated Program of Study(ies) (PoSs) 23
4. Continuous Improvement Plan and Process 23
PART IV: CAE-C RECURRING REVIEW OF CAE-C DESIGNATION INSTITUTIONAL CRITERIA 24
1. A 5-Year Report of Institutional Metrics 24
2. A 5-Year Report on Continuous Improvement 24
Appendix 1 – Required and Optional Knowledge Units list for CAE-CD 25
Appendix 2 – KU Alignment Requirements for CAE-CD 26
Appendix 3 – Examples of PoS Validation Requirements 27
Application Process and Adjudication Rubric (APAR) - Working Group (WG) 34

DRAFT

INTRODUCTION TO THE CAE-CD APPLICATION PROCESS

Institutions wishing to be designated a **Center of Academic Excellence (CAE) in Cyber Defense (CD)** for a particular program of study will apply in two parts. The following process applies to both Program of Study (PoS) Validation and CAE-CD Designation. It is proposed that if needed, in Step 5 (Figure 1), the applicant appears before the Review Committee by webinar for the PoS validation and in person for the CAE-CD Designation review.

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

This process and timeline apply to either application for Program of Study (PoS) Validation only, or for CAE-CD Designation.

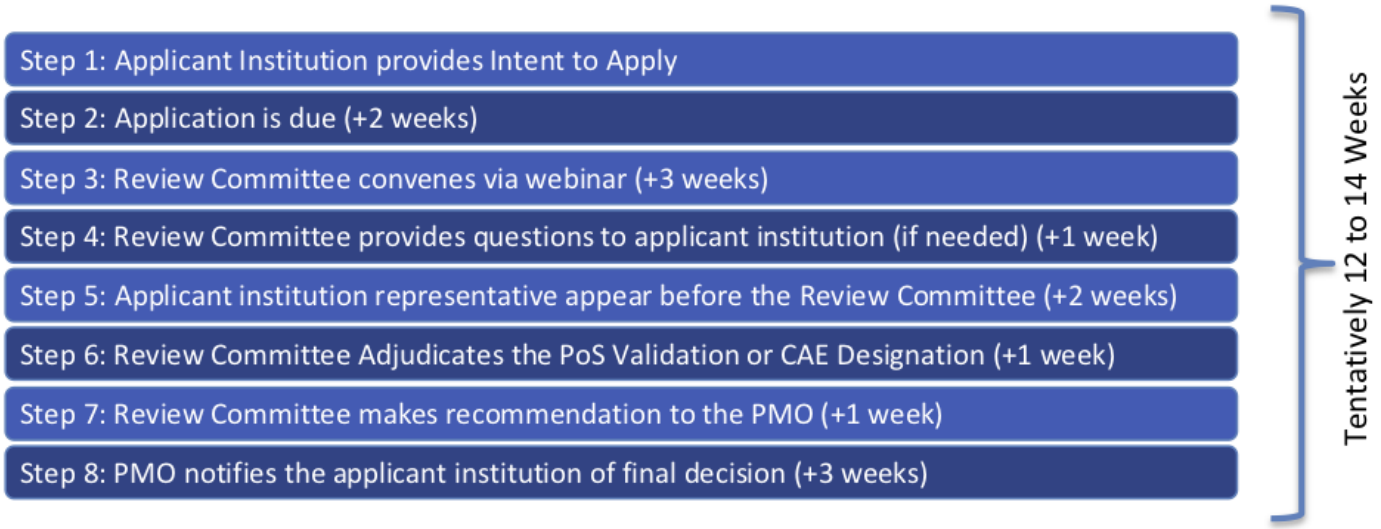

Figure 1. Tentative PoS Validation or CAE-CD Designation Application Process and Timeline

Timelines for submission will be published by the CAE-C Program Management Office (PMO) 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 CAE 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 CAE 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 (online for PoS, and in-person for CAE-CD Designation) for further clarifications, followed by a final notification from the PMO (See Figure 1). Each PoS will need to have a designated POC, which may or may not all be the same individual and may

or may not be from the same academic unit or department. The CAE will need to have a designated POC who is the person in charge of the established "Center" for cybersecurity at the academic institution (See CAE-C Designation Criteria No. 4). Mentoring and initial approval of all pre-submission material are required in order to be granted access to the Application Tool. The first POC from each academic institution submitting a PoS for Validation is expected to "mentor" additional POCs (if applicable) from that same academic institution on PoS validation requirements. In the case of an academic institution with CAE Designation, the CAE POC should serve in that capacity and be kept aware of all newly submitted PoS for Validations. The PMO will not provide multiple mentors to an institution and expects that POC to 'lead-by-example' also within their institution. Incomplete applications will be returned without comment. Designation as a National CAE-C does not carry a commitment of funding.

Justifications

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

Synergistic Approach

To achieve CAE-C status, the institution should demonstrate a synergistic approach involving a proper environment for academic excellence, and faculty and courses to drive Program-Level Learning Outcomes (See Figure 2). 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.

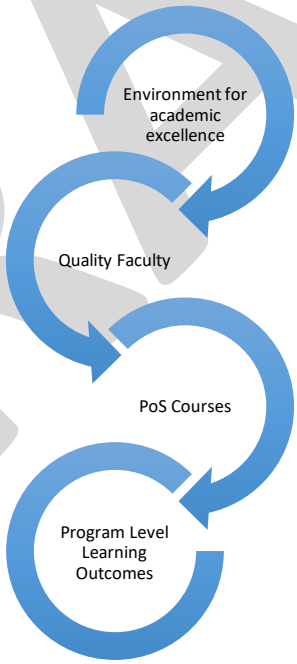

Figure 2. The Synergistic Approach Needed to Become CAE-C

DRAFT

Definitions

An ***institution*** is a legal entity authorized to award associate degrees or higher. All institutions applying to the CAE-C program must hold current regional accreditation as outlined by the 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.

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) VALIDATION REQUIREMENTS FOR CAE-CD

Overview

The Program of Study (PoS) Validation requirements for CAE Cyber Defense (CAE-CD) programs include evidences 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 validation must have Program-Level Learning Outcomes identified and on file at the submitting institution, preferably on the program's website/webpage. Those Program-Level Learning Outcomes will then be *mapped* to the courses in the PoS. Moreover, the Self-Study will include documentation of the identified KUs for the PoS and the *alignment* of the KUs to the relevant courses in the PoS. Figure 3, the CAE PoS Validation Conceptual Model, provides a graphical representation of the: (1d) Curriculum Map and Plan courses with associated documentation, the (1e) KU alignment courses, and (4) Continuous 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 indicated in the KU alignment, as all students should experience all courses indicated in the KU alignment. Additionally, for (1b) NICE Framework (a.k.a. NICE Cybersecurity Workforce 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-CD. 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)
f) Graduate Thesis/Dissertation/Equivalent Guidelines and Process (Masters and Doctoral programs only)

2. Students

a) Student enrollment/graduation in the PoS(s)
b) CAE-CD: Sample student certificate/notation on transcript/official letter
c) Students work products (papers, assignments, labs, etc.)
d) Students participation in extracurricular activities

3. Faculty Members

a) Cyber Program(s) of Study PoC
b) Full-time, part-time, and adjunct faculty members + Faculty qualifications (publications, research, industry involvement, certifications, etc.) related to PoS type
c) Faculty support of enrolled students
d) Process of Faculty Promotion/Reappointment (e.g. Faculty Policy Manual)

4. Continuous Improvement

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

DRAFT

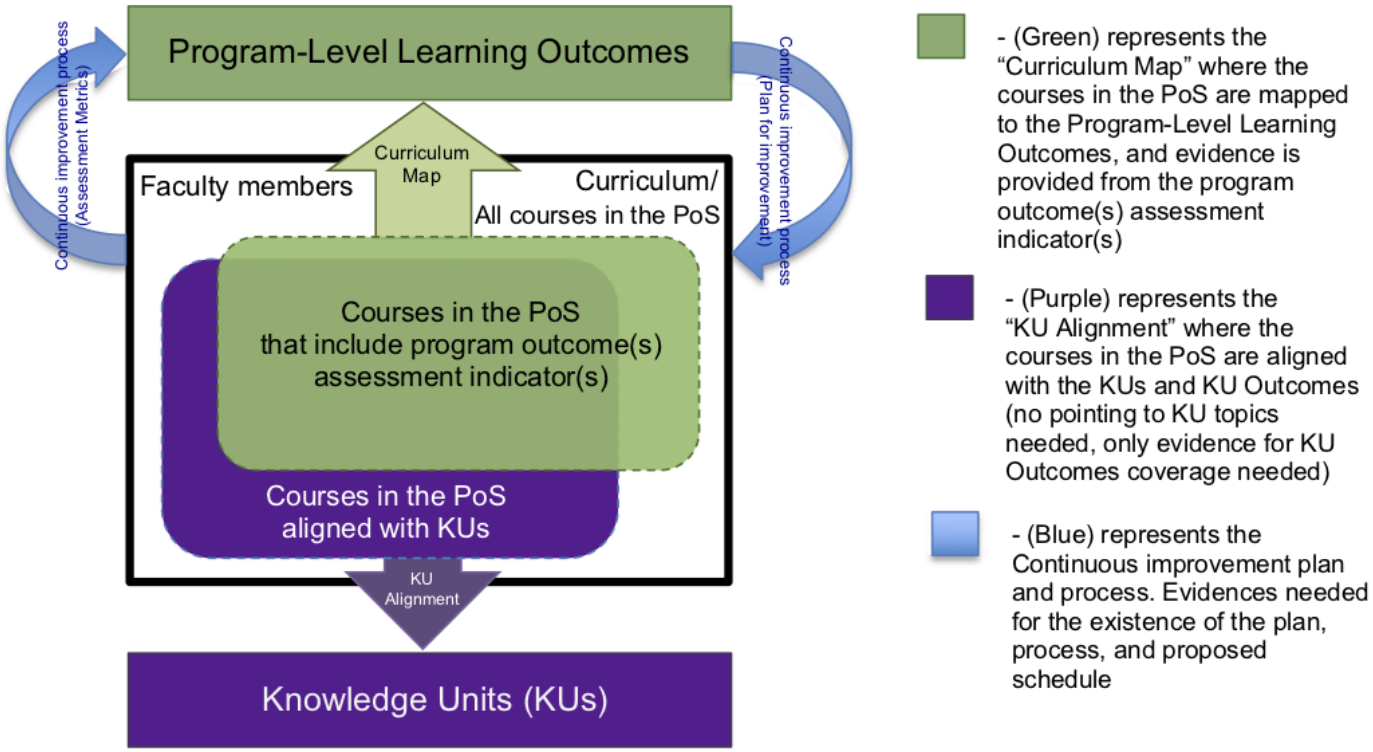

Figure 3. PoS Validation Conceptual Model

Institution Details

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

Requirements:

- Identify/confirm the official institution name
- Provide link to the homepage of the institution (not department)
- Provide the address of the institution

Additional Information for Grant Related Opportunities (Not guaranteed):

Academic institutions applying are highly encouraged to provide further evidences of eligibility for NSA grants for the benefit and ease of applying for grants. Doing so will allow NSA to identify potential CAE-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(s) of Study (PoS) Validation Requirements

1. PoS Curriculum

Academic program(s) at the institution will be validated as Program(s) of Study (PoS). The academic institution must show its curriculum path and show that students are enrolled and successfully complete the path and receive recognition. A single academic institution may have multiple PoSs validated, but only one is required to proceed to CAE Designation. All institutions applying for PoS validation must be regionally accredited.

PoS is defined sets of courses that are designed to develop Program-Level learning outcomes in the student population over time. It is possible to have multiple cybersecurity PoSs at an academic institution, in different departments, producing students with different knowledge and skills. It is also possible to have a PoS that can be achieved by multiple paths or sets of elective options. 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 validated PoS.

CAE-CD Designations have a requirement to align courses to CAE-C Knowledge Units (KUs) and provide Curriculum Map and Plan (See Figure 3). The Application Tool will simplify the KUs alignment as well as the Curriculum Map and Plan submission process. KUs are the link between the CAE-C program and the cybersecurity workforce, and is the means by which the PMO communicates to employers and potential students which PoS may most closely match their hiring requirements or study interests. Graduate programs (Masters and Doctoral) should provide evidence of institutional documentation for thesis, dissertation, graduate project course, and/or graduate experiential learning course.

a. The Cybersecurity PoS offered by the institution

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

Requirements (All needed):

- State the official name of the cybersecurity PoS (including: degree level, if applicable, minor, concentration, certificate). If validated, the PoS name will be displayed on a NCAE website list, thus, it must be the official name (Examples: AAS in Computer Technology with a Cybersecurity Certificate; BS in Cybersecurity; BS in Computer Science with Cybersecurity Minor; MS in Information Technology with concentration in Cybersecurity Management; Ph.D. in Cybersecurity Management).
- 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 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, CAE 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.

DRAFT

- 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 all courses 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 NICE Framework (a.k.a. NICE Cybersecurity Workforce 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 NICE Cybersecurity Workforce Framework category(ies) that the PoS is best aligned to (May check more than one).

c. Courses 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 (in PDF).
- For KU aligned courses that require applied labs exercises (i.e. hands-on labs that develop competencies) in the cyber domain, highlight it on the syllabus, and highlight in which unit/week it is required.
- 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 (in PDF).

d. Curriculum Map and Plan with Assessment Documentation

Program-Level Learning Outcomes are the basis for determining the effectiveness of a CAE-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 experience all courses indicated in the Curriculum Map and Plan.

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).

DRAFT

- 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 CAE-C program will rely upon the institutional accreditation for sufficiency of program construction and maintenance. Courses, or other academic elements, should be institutionally approved per the institutional requirements for accreditation and aligned to the KUs. The PoS content as demonstrated by KU alignment will be used to determine if the courses together as a whole constitute sufficient material in quantity and form. All CAE-CD programs need to cover the foundational, appropriate core, and required elective KUs per academic program type (Associate, Bachelors, Maters, or Doctoral) as indicated in Figure 4. No elective or optional courses should be included in the KU alignment, as all students should experience all courses indicated in the KU alignment. One course may align with one or more KU(s), however, a course should not be aligned to an excessive number of KUs given the challenge of so many KU Outcomes coverage with a single course. One KU may align to multiple courses, however, this is not recommended. KU alignment is only needed for courses that are identified for alignment with the KUs. Course learning outcomes will also be aligned (as a set) to the relevant KU(s), while the KU Outcomes will be shown (as a set) to provide guidance on the coverage (See Appendix 3 - Example 1e1). As part of the application, the academic institution will provide information on the academic year that each of the KU aligned course was last offered.

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 - Examples 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.
- For graduate programs (MS or Doctoral) that seek exemption from the three (3) Foundational KUs and five (5) Technical or Non-Technical Core KUs, provide evidence that students are admitted with the foundational and core knowledge.

CAE-CD PoS Validation KUs:

The core or other set of PoS courses that all students in the PoS attend are aligned to chosen KUs (See Figure 4. CAE-CD KU requirements below for each degree level).

Appendix 1 provides a list of **Required and Optional Knowledge Units for the CAE-CD Program**. The full list and details on each knowledge unit can be found at: https://www.iad.gov/nietp/Requirements.cfm. *Appendix 2* provides an overview of the **KU Alignment Requirements for CAE-CD**.

DRAFT

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

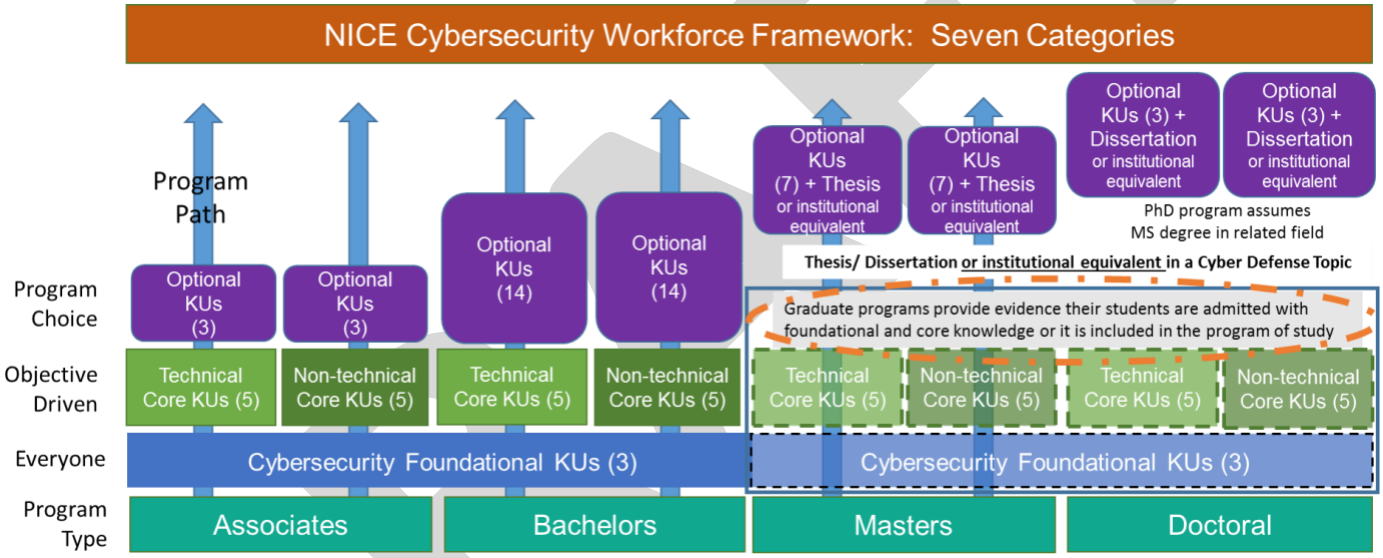

Figure 4. CAE-CD Knowledge Units Alignment Requirements

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

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

Masters degree programs may include traditional Master Thesis or equivalent such as: graduate project course, graduate experiential learning course, or graduate practicum with a preference for industry advisor interactions. Master Thesis/equivalency should include one or more dedicated term-long course(s) indicated as "Thesis", "Project", "Experiential Learning", or "Practicum" preferably towards the end of the student's PoS and should be supervised by a qualified faculty member. The student (or small group of up to two students) develops a final project and/or experiential learning as a paper and/or applied project that integrates best practices in the context of cybersecurity. Concepts and national cybersecurity standards underlying the student's project and/or experiential learning are articulated; the problem is clearly stated; measurable goals are specified; and strategies to implement the project and/or experiential learning goals are provided.

Doctoral degree programs may include Traditional Dissertation (Ph.D./D.Sc.) or equivalency such as professional doctorate applied research project. The Traditional Dissertation should show clear and

demonstrable focus on cybersecurity and should be supervised by a qualified faculty member. The work should represent at least two years effort by the student on the research. Professional Doctorate Equivalency should show clear and demonstrable focus on cybersecurity and should be supervised by a qualified faculty member. The work should represent at least one-year effort by the student on the applied research. The Traditional Dissertation and the Professional Doctorate Equivalency should include a formal scheduled defense.

Requirements (Masters/Doctoral):

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

2. <u>Students</u>

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

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

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

Requirements (All needed):

- Provide student enrollment in PoS for the last three years
- Provide official institutional letter for the enrollment/graduation (letter from Registrar or equivalent) (in PDF)
- Provide at least three (3) redacted student transcripts, dated within the last three years and clearly highlight the courses taken that are in the KUs alignment. All KU aligned courses must appear on the transcript.

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

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

Requirement:

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

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

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

Requirements (All needed):

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

DRAFT

d. Students Participation in Extracurricular Activities

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

Requirements (All needed):

- Provide evidence of three student participation in extracurricular activities within the last three 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, summer internship program, industry guest lectures, etc.
- Provide date and description for each evidence provided.

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 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, CAE 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 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 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 (all links and evidence information provided within a single PDF).

DRAFT

- Provide evidence for institutional process of faculty promotion/reappointment (e.g. Faculty Policy Manual) (in a single PDF)

4. Continuous Improvement

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 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 the Continuous Improvement Plan for the PoS (in PDF).

b. Continuous Improvement Process for the PoS

The *Continuous Improvement Process* commonly includes the four 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.

DRAFT

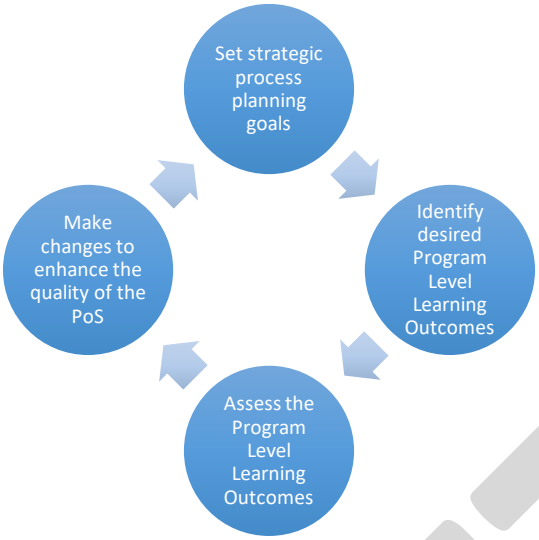

Figure 5. Continuous Improvement - Regular Evaluation Cycle

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).

DRAFT

PART II: CAE-CD APPLICATION – CAE-C DESIGNATION CRITERIA

Overview

The table below provides the required criteria needed for CAE-CD Designation. The CAE PMO is moving to ensure there is more accountable by ensuring all data is within an online CAE Application Tool to document the history/purity of the data for CAE-CD Designation.

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

1. Accreditation: The institution must be regionally accredited to hold any CAE-C designation.
2. Institution Commitment: A letter of intent and endorsement, signed by the Provost or higher, documenting that the institution is aware of the expectations and responsibilities associated with the CAE program including established "Center" for cybersecurity, identified CAE 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. Evidences 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 at the institution. A signed letter on official letterhead from the officer assigned with direct responsibility for institutional cybersecurity, attesting to the fact that the institution has a solid cybersecurity posture and plan in place, along with examples of cybersecurity plan implementations through awareness, training and tutorials, log in security banners, etc. will suffice.
4. Established "Center" for Cybersecurity: An officially established "Center" (either physical or virtual) for Cybersecurity providing program guidance and oversight, general cyber defense information, collaboration and outreach opportunities among students, faculty, other academic units/departments in the same institution, and other institutions, and a website that is dynamic, current and visible within the institution and the external community at large that also list the PoS Validated program(s). The "Center" must have an external board of advisors (maybe shared with other programs).
5. Affirmation of the CAE Core Values and Guiding Principles: Applicant institutions will affirm their commitment to the CAE Core Values as part of the Designation application, and expected to follow the Guiding Principles indicated on each of the three CAE 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. Cybersecurity Academic Integration: Demonstrate cybersecurity content is integrated into additional degree programs within the academic institution.
9. Outreach: The academic institution must demonstrate how cybersecurity practices are extended beyond the normal boundaries of the institution. Show how cybersecurity concepts developed at the academic institution are shared with others to improve the practice of cybersecurity in the community.
10. Transfer of Credit/Articulation Agreements: Provide evidence of Articulation/Transfer agreements with institutions offering a concentration or cybersecurity (or related field) degrees/areas of study/track or certificates (United States Military Academies are exempt). Examples include: statewide transfer agreements, articulation agreements, credit for prior learning, credit for military training, or membership in Transfer Evaluation Services (TES) with evidences of several transfer credits institutions in the geographic area.

CAE-CD Designation Criteria

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

1. Accreditation

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

DRAFT

Requirement:

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

2. Institution Commitment

The letter of intent and endorsement, signed by the Provost or Higher, demonstrating that the institution is aware of the expectations and responsibilities associated with the CAE-C program. The letter must express institutional commitment to excellence in the cybersecurity field and support of the program the institution is submitting for CAE-C designation, identify the CAE 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 CAE PMO, the CAE Community, and the CAE Regional Hubs (CRH); and active participate in the CAE Community and support of the CAE-Cybersecurity programs. This letter must be submitted early in the process to demonstrate that the institution supports the application, executive leadership acknowledges and supports the CAE 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 CAE-C program (in PDF, do not mail) that:
  - 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
  - Identify regional accreditation information.
  - Express institutional commitment to excellence in the cybersecurity field.
  - Identify and provide institutional support of an established "Center" for Cybersecurity within the institution.
  - Identify the CAE Point of Contact (POC) from the institution.
  - Identify the name of a designated CAE Institutional Accounts Administrator (A person who oversees the CAE accounts across the institution - one who is authorized to switch POCs, activate new users, etc.).
  - List the program(s) of study supporting the requested designation.
- Provide acknowledgement to follow the minimum participation expectations of a CAE-C:
  - Submission of an Annual Report with all required information.
  - Attendance at either (or both) the CAE Principal's Meeting and CAE Community Symposium each year.
  - Regular communication with the CAE 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 CAE-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. Evidences 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 at the institution. The institution must demonstrate that they have

DRAFT

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 separate examples of how the institution implements its cybersecurity plan through awareness, training and tutorials, log in security banners, user acknowledgements, online help and good security practice guides (e.g. Students, faculty and staff are required to take computer based training or online tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc.) (in six separate PDFs).

4. Established "Center" for Cybersecurity

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

Requirements (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 Validated PoS(s)
  - 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 CAE Core Values and Guiding Principles

CAE-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 CAE-C program. Applicant institutions will affirm their commitment to the CAE Core Values as part of

DRAFT

the *Designation* application, and are expected to follow the *Guiding Principles* indicated on each of the three Core Values (not to be submitted, affirmed only).

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 CAE-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 CAE and non-CAE institutions.
   - The academic institution has appropriate mechanisms to share resources, instructional material, faculty, and/or facilities between institutions, both CAE and non-CAE 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 CAE-C program. Having full-time permanent faculty members associated with the "Center" and PoS Validated program(s) 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 CAE-C program Core Values at the institution. Having these full-time permanent administration personnel, and POC (who may be a faculty member as well) identified in the application is part of assuring that the institution has the necessary resources, capacity, and processes for the cybersecurity program(s) to be successful.

DRAFT

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 established "Center" for Cybersecurity (Department chair, faculty lead, CAE 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 established "Center" for Cybersecurity POC and indicate year the individual joined the academic institution (in PDF).
- Identify the alternate POC for the 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 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 CAE-C program. Ongoing access to working professionals and practitioners during their time in a CAE-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 separate examples of professional development opportunities provided to faculty and students over the past three years. Evidence files can be fliers, posters, letters, attendance records, or other evidence of professional development for faculty and students (in six different PDFs).

8. Cybersecurity Academic Integration

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

Requirements (all needed):

- Identify the course and academic unit (department/college/etc.) at the institution where students from non-validated PoS (or non-PoS(s) applied for validation) are exposed to cyber concepts.

DRAFT

- Provide syllabi of three different courses where cyber modules clearly highlighted from other departments/colleges. Combine the syllabus, guidelines (i.e. what students are asked to do) of the work, and one sample student work into a single file for each of the three courses (Three separate PDFs).

9. Outreach

One of the core values of the CAE-C program is sharing of cyber defense expertise. The institution must demonstrate how cyber defense practices are extended beyond the normal boundaries of the institution. Outreach activities help show how cyber defense concepts developed at the institution are shared with others or how industry theory and practice are incorporated into curriculum. Moreover, outreach activities allow the cybersecurity program to engage with business and industry to provide pathways for graduates while maintaining an appropriate curriculum to place graduates into those jobs. Examples of outreach and collaboration include:

- Participation in CAE events such as: CAE Community Symposia, CAE Regional Hubs (CRH) workshops for candidate institutions, CAE Tech Talks/Forums used in classroom, collaboration on grants with CAE-C institutions.
- Faculty members collaborating with current CAE-C institutions on research, grants, course development, etc.
- Faculty and/or staff participating as CAE reviewers/mentors/advisors, etc.
- Faculty and/or staff participating on FBI affiliated InfraGard (https://InfraGard.org/) as members, and/or chapter board and/or sector chiefs, USSS Electronic Crime Task Forces, DHS Regional Domestic Task Forces, and/or other national, regional, state, and/or local cybersecurity working groups, task forces, and leadership positions.
- Faculty and/or staff sponsorship or oversight of cybersecurity events for the community at large. Events could include cyber awareness and education for local schools, adult education centers, senior centers, camps, first responders and the surrounding community. Examples of events could be, but are not limited to, computer "check-up" days, presentations on protecting personal information in cyber space, workshops for senior citizens on Internet safety, or preventing and recovering from a "virus" (senior centers, K-12, camps, etc.).
- Involvement with industry (internships for students, identifying needs of business partners for course content, job fairs, guest speakers, etc.).
- Institution partners with companies and other employers to identify cybersecurity needs of potential employers and encourage student internships.

Requirements (all needed):

- Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge within the last three years. Identify specific materials provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties' website, etc. is encouraged (in PDF).
- Provide evidence (three) that the applying institution has participated in CAE events such as: CAE Community Symposium, CRH workshops for candidate institutions, CAE Tech Talk/Forum used in classroom, collaboration on grants with CAE institutions (Three separate PDFs).
- Provide at least three evidences that faculty members from the applying institution has contributed to the CAE community such as: served as PoS Validation and/or CAE-C Designation mentors, reviewers, members of the CAE Working Groups, presented in CAE Community Symposiums, CRH workshops, CAE Tech Talk/Forum (Three separate PDFs).
- Provide evidence of faculty members collaborating with current CAE-C institutions on research, grants, course development, etc. (in PDF).
- Provide evidence of faculty members/employee sponsorship or oversight of students for Cyber events for the community at large. Events could include Cyber awareness and education for local schools, adult

education centers, senior centers, camps, first responder training and the surrounding community (in PDF).

- Provide evidence on how the institution works with employers and students to support placement for cyber related internships and jobs, such as via institutional Career Development Services (i.e. HandShake) and industry events on-campus (in PDF).
- Provide evidence of obtaining input on curriculum to meet industry needs (in PDF).

10. Transfer of Credit/Articulation Agreements

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

Requirement:

- Provide evidence that the institution awards credit in cybersecurity related courses and/or technical prerequisite courses from other academic institutions, community colleges, tech schools, etc. or through alternative means. Examples include but are not limited to: transfer agreements with community colleges, articulation agreements, statewide transfer agreements, articulation agreements, college in the high school, dual credit, running start, credit for prior learning, credit for military training or occupation, and/or membership in Transfer Evaluation Services (TES) (in PDF).

DRAFT

PART III: CAE-C POST-DESIGNATION REPORTING REQUIREMENTS

Overview

Academic institutions holding any CAE-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 CAE-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 CAE-C program. Items such as number of students, number of graduates, and other "metric" elements are used by the CAE-C Program Management Office (PMO) to document program effectiveness with a wide constituency. The needed elements are defined by the PMO and collected at application time and annually.

Expectations of All Designated Institutions

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

There is a continual need for specific metric elements associated with institution performance. Items such as number of students, number of graduates, and other "metric" elements are used by the PMO to document program effectiveness with a wide constituency. The needed elements will be defined by the PMO and collected at application time and annually. These elements will be delivered via entry into a web-based data collection system and are the responsibility of the institution to keep current.

If the required annual report of institutional metrics is not submitted on time each year, a message is automatically sent to the POC's supervisor or the appropriate Dean (See Table IV.1 for time-dependent additional consequences).

DRAFT

1 *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 CAE-C sponsored events. The institution's designation returns to good standing upon submission of the report.
• After 90 days	If the information is not submitted within 90 days of the deadline, the institution is ineligible for Grants or Scholarships issued by the PMO for the remainder of the calendar year, and the Institution is removed from the Designated list online; the President is notified of this action. The institution's designation returns to good standing upon submission of the report.
• After 120 days	If the information is not submitted within 120 days of the deadline, beyond the consequences noted in the 90 days mark, an ad hoc committee will be assigned to review the status of the program and report back to the PMO within 30 days. The committee will be authorized, at its discretion, to request documentation and to contact the POC(s), institutional administrators, or take other steps to review the current state of PoS Validation and/or CAE Designation compliance in order to ascertain facts relevant to the status of the program/center remaining in accordance with its most recent PoS Validation and/or 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 CAE (including logos and other CAE indicators) from all printed and electronic materials and to remove all references to CAE 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 CAE (including logos and other CAE indicators) from all printed and electronic materials and to remove all references to CAE status. The institution will be required to reapply for PoS Validation and/or CAE 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

DRAFT

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 CAE-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 Designated Program of Study(ies) (PoSs)

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

Strong continuous improvement plan and a process for regular implementation of the plan are key element 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 assessment items (i.e. the Program-Level Learning Outcome assessment indicator(s)) shall be chosen to measure each Program-Level Learning Outcome. These assessment indicator(s) will be graded at least once every three years (See Appendix 3 - Examples 1 and 2 for requirement 1d1: Curriculum Map and Plan). It is not necessary to assess all Program-Level Learning Outcomes every year, nor is it desirable as changes should be gradual and measurable. Improvement efforts should be spaced out so that some Program-Level Learning Outcomes are assessed every year. For each assessment indicator, the class assignment and associated rubric used to measure the Program-Level Learning Outcome shall be provided (See Appendix 3 - Examples for requirements 1d2 and 1d3).

As a normal part of the continuous 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.

DRAFT

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

Academic institutions holding any CAE-C designations (CAE-CD, CAE-CO, & CAE-R) must formally renew their PoS(s) Validation and CAE designation every five years.

1. A 5-Year Report of Institutional Metrics

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

2. A 5-Year Report on Continuous Improvement

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

DRAFT

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

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

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

The five technical **core** KUs are:

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

The five non-technical **core** KUs are:

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

Optional KUs (56 total) can be adopted by any program as needed to document their program of study. Additionally, opposing core KUs may be used as optional KUs (i.e. If technical core is chosen, then non-technical core may be used as optional KUs and if non-technical core is chosen, then technical core maybe used as optional KUs.). Optional KUs include:

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

https://www.iad.gov/nietp/Requirements.cfm

DRAFT

APPENDIX 2 – KU ALIGNMENT REQUIREMENTS FOR CAE-CD

<table>
<tr><th colspan="5"></th></tr>
<tr><td colspan="5">Program of Study (PoS) Validation - Knowledge Units (KUs) requirements per academic level; See Appendix 1 for a the CAE-CD list of KUs. All PoS align to the three Foundational KUs, and five Technical or five Non-Technical KUs. Each designation also has a requirement to align to Optional KUs. The number of Optional KUs is determined by the academic level of the program.</td></tr>
<tr><th>Designation</th><th>Optional KUs</th><th>Foundational KUs</th><th colspan="2">Core KUs (Choose technical OR non-technical)</th></tr>
<tr><td>CAE-CD, Associates</td><td>3</td><td rowspan="2">IT Systems Components
Cybersecurity Foundations
Cybersecurity Principles</td><td>Non-Technical</td><td>Cyber Threats
Policy, Legal, Ethics and Compliance
Security Program Management
Security Risk Analysis
Cybersecurity Planning and Management</td></tr>
<tr><td>CAE-CD, Bachelors</td><td>14</td><td>Technical</td><td>Basic Scripting and Programming
Basic Networking
Network Defense
Basic Cryptography
Operating Systems Concepts</td></tr>
<tr><td>CAE-CD, Masters</td><td>7</td><td colspan="3" rowspan="2">Graduate programs must demonstrate that students have received subject matter preparation equivalent to the foundational and core KUs or alignment to required KUs or include it in the program.</td></tr>
<tr><td>CAE-CD, Doctoral</td><td>3</td></tr>
</table>

DRAFT

APPENDIX 3 – EXAMPLES OF POS VALIDATION REQUIREMENTS

Example for requirement 1a: PoS Curriculum Sheet:

Information Assurance and Cybersecurity

MASTER OF SCIENCE

Curriculum | Total Credits: 30

PREREQUISITE COURSES

Applicants who do not have adequate academic backgrounds may be required to take one or more of the following 500-level graduate courses during the first two terms of the program. (Courses are 3 credits each.)

CISC	500	Java Programming Language
CISC	501	Computer Organization and Architecture
CISC	502	Mathematics in Computing
CISC	503	Data Structures and Algorithms

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

DEGREE PROGRAM COURSES

Required Courses (10 courses, 3 credits each)

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

DRAFT

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.

DRAFT

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.

DRAFT

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 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

DRAFT

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]

DRAFT

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

Program of Study 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. …	(CSF) Cybersecurity Foundations	1. Describe the fundamental concepts of the cybersecurity discipline and use to provide system security. 2. Describe potential system attacks and the actors that might perform them. 3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks. 4. Describe appropriate measures to be taken should a system compromise occur. 5. Properly use the Vocabulary associated with cybersecurity.
			(NDF) Network Defense	1. Describe the key concepts in network defense (defense in depth, minimizing exposure, etc.). 2. Explain how network defense tools (firewalls, IDS, etc.) are used to defend against attacks and mitigate vulnerabilities. 3. Analyze how security policies are implemented on systems to protect a network.

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

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

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

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

Cybersecurity Foundational KUs (3)

Non-technical Core KUs (5)

Optional KUs (3)

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

DRAFT

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

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

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

Cybersecurity Foundational KUs (3)

Technical Core KUs (5)

} Included in the PoS

Optional KUs (7)

Additional KUs (7)

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

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

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

DRAFT

APPLICATION PROCESS AND ADJUDICATION RUBRIC (APAR) - WORKING GROUP (WG)

Working Group Co-Chairs

Yair Levy, Nova Southeastern University

Eric Berkowitz, Roosevelt University

Cyber Operations (CO) Subgroup Co-Chairs

Faisal Kaleem, Metropolitan State University

Shankar Banik, Citadel

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

Alan Carter, Green River College

Bill Chu, University of North Carolina - Charlotte

Art Conklin, University of Houston

Jane Cothran, Trident Technical College

Jose R. de la Cruz, Polytechnic University of Puerto Rico

John Franco, University of Cincinnati

Erik Fretheim, Western Washington University

Ernie Friend, Florida State College at Jacksonville

Greg Gogolin, Ferris State University

Seth Hamman, Cedarville University

Mark Hufe, Wilmington 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

Michael Whitman, Kennesaw State University

The APAR-WG 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.

DRAFT