CAE-CO Designation Workshop

Hosted By: CNRC Candidates Program

Agenda

- Welcome
- Centers of Academic Excellence (CAE) Designations and Resources
- Getting Started
- Program of Study & CAE Application Process
- Part 1: Program of Study Validation
- Part 2: CAE Designation

The Centers of Academic Excellence (CAE) Designations and Resources

CAE Designations

- **Cyber Defense** (CAE-CD) designation is awarded to regionally accredited academic institutions offering cybersecurity degrees and/or certificates at the Associates, Bachelors and graduate levels.

- **The Cyber Research** (CAE-R) designation is awarded to DoD schools, PhD producing military academies, or regionally accredited, degree granting four-year institutions rated by the Carnegie Foundation Basic Classification system as either a Doctoral University – Highest Research Activity (R1), Doctoral University – Higher Research Activity (R2), or Doctoral University – Moderate Research Activity (R3).

- **The Cyber Operations** (CAE-CO) designation is awarded to regionally accredited academic institutions offering cybersecurity degrees that are deeply technical, inter-disciplinary, higher education programs firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

CAE Resources

CAE Community

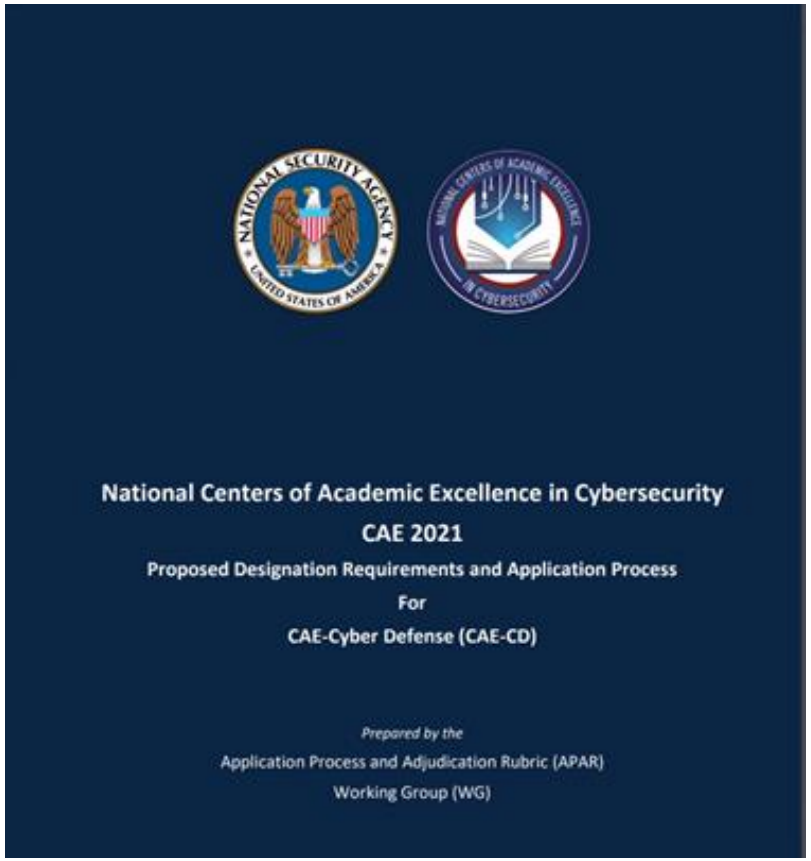
- www.caecommunity.org

Candidates Program National Center

- www.ncyte.net
- ncyte@whatcom.edu

NSA CAE Program Office

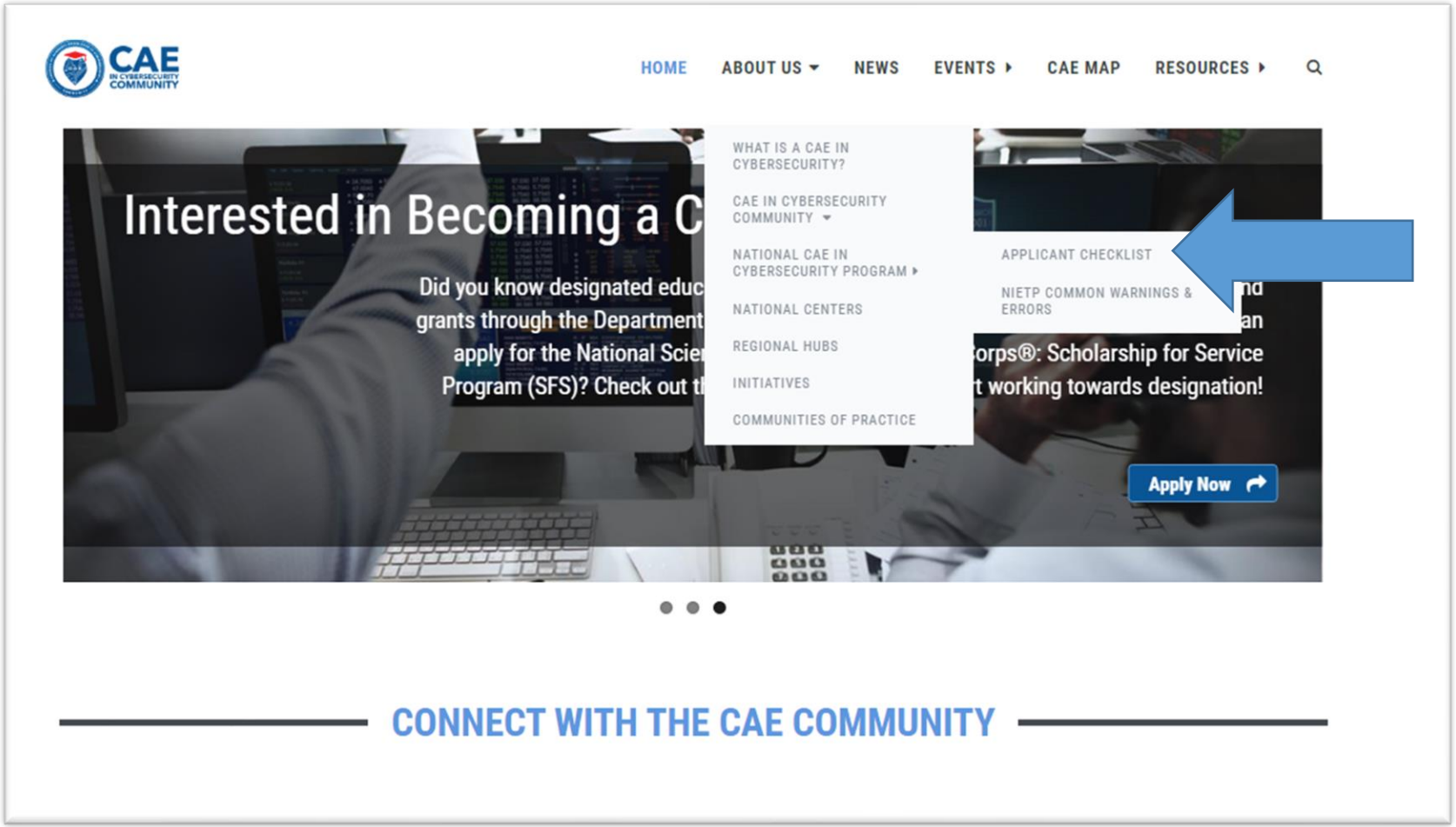
- https://public.cyber.mil/ncae-c
- caepmo@nsa.gov



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

Getting Started

CAE Checklist



www.caecommunity.org

Application Process

PoS/CAE Application Process

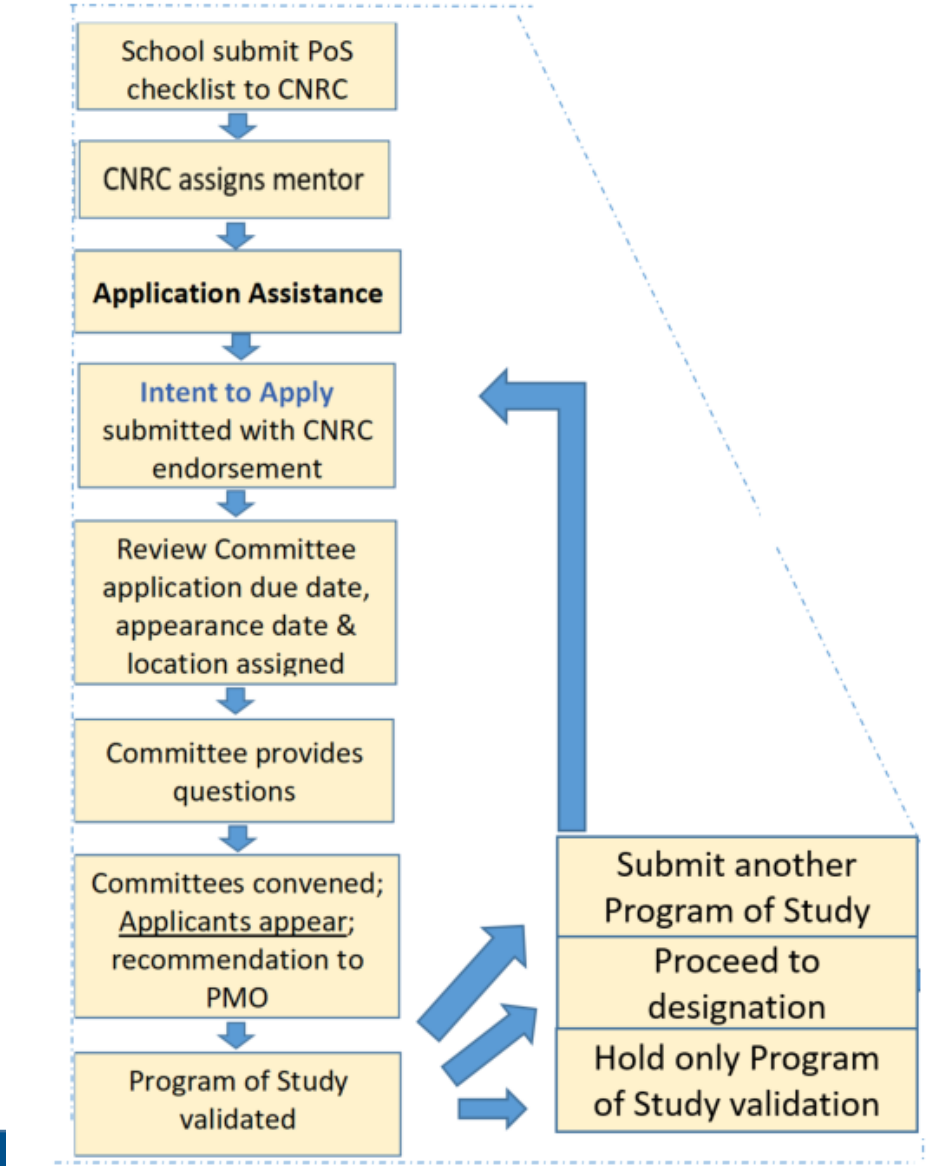
Part 1: Program of Study (PoS) Validation

- To apply for CAE, all institutions must have a validated program of study
- An institution may opt to have multiple programs of study validated before pursuing CAE designation
- Some Institutions will stop here

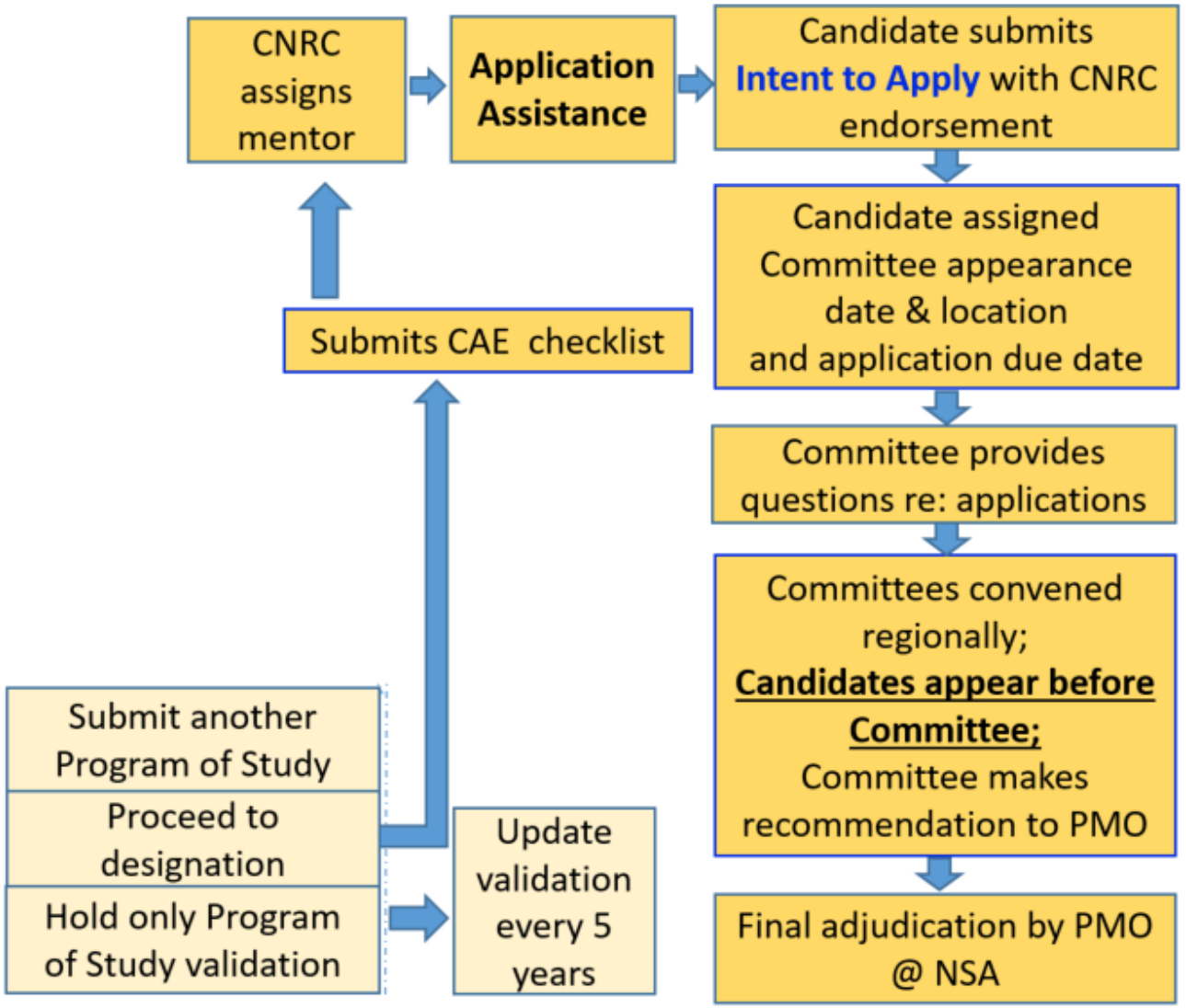
Part 2: CAE Designation

- One program of study needs to be validated before the institution can pursue the CAE designation

PoS/CAE Application Process



PoS/CAE Application Process



Assign Submission Cycle to PoS/CAE

Program of Study (PoS) Cycle	Access to Application	*Application Due	**Pre-submission Review (PSR) Feedback Deadline	Final Submission
PoS Cycle 1	10/15/2020	12/15/2020	1/1/2021	1/15/2021
PoS Cycle 2	11/17/2020	3/15/2021	4/1/2021	4/15/2021

CAE Cycle	Access to Application	*Application Due	**Pre-submission Review (PSR) Feedback Deadline	Final Submission
CAE Cycle 1	3/26/2021	4/9/2021	4/23/2021	5/7/2021
CAE Cycle 2	6/24/2021	7/8/2021	7/22/2021	8/5/2021

Application Due – Institutions **must** submit a completed application for pre-submission review (PSR) on this date. Partial applications will not be forwarded for review. The PSR is required before there will be a full review of the CAE application.

PSR Feedback Deadline – The pre-submission reviewer will provide feedback to the institution on or by this date.

Final Submission – The date an institution must submit their PoS/CAE application by 11:59pm (ET).

PoS/CAE Application User Roles & Responsibilities

Access Manager (Initial POC is the default):

- Manages access to institution applications
- Approves additional users
- Holds account administrator privileges

Point of Contact (POC):

- Primary contact for PoS/CAE application
- Full application privileges
- Responsible for annual report

Alternate Point of Contact:

- Secondary contact to POC

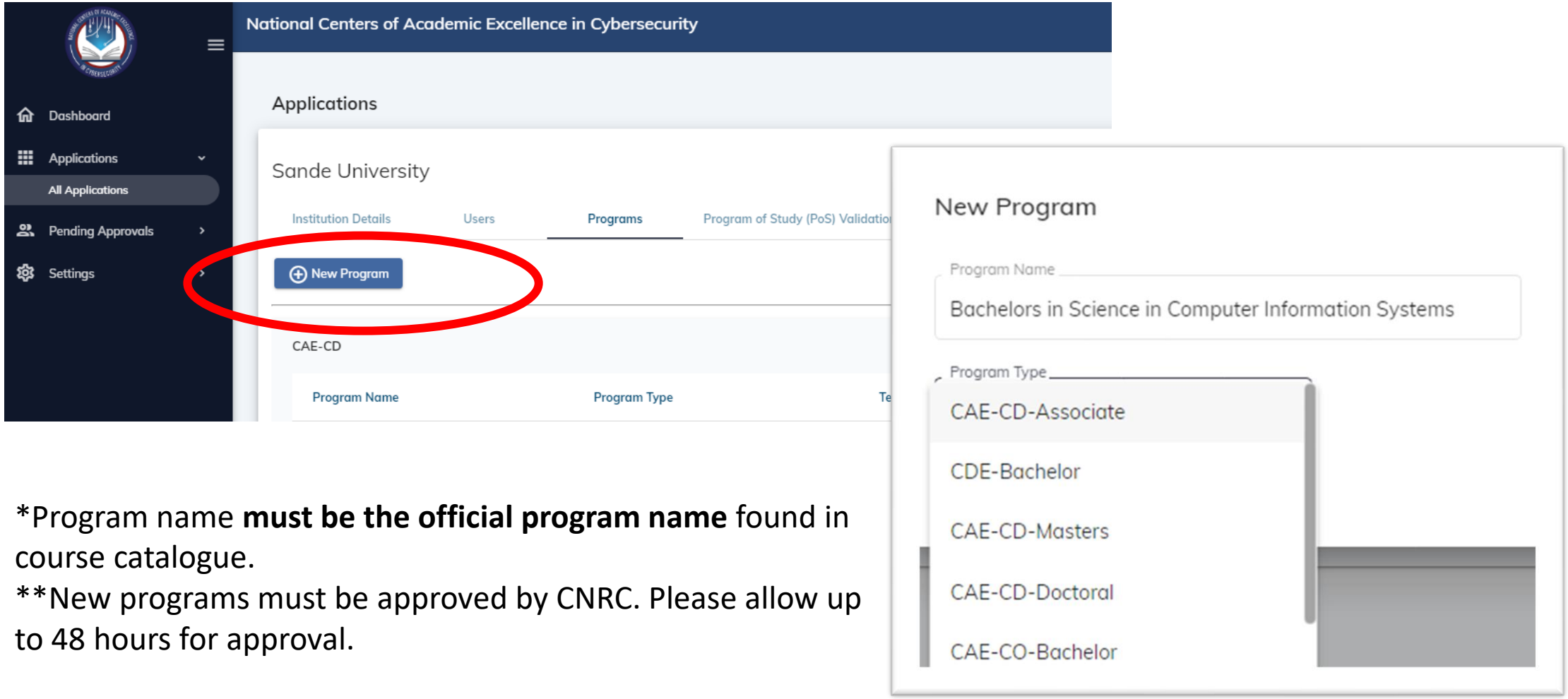
Data Entry (not required):

- Given data entry access
- Cannot submit application

How to Add Users in the Application

Step 1	The Alternate POC and data entry personnel must create a user account and will need to be approved by the POC/Access manager.
Step 2	POC/Access manager approves users under “Pending Approval”.
Step 3	POC/Access manager assigns user to the correct application.

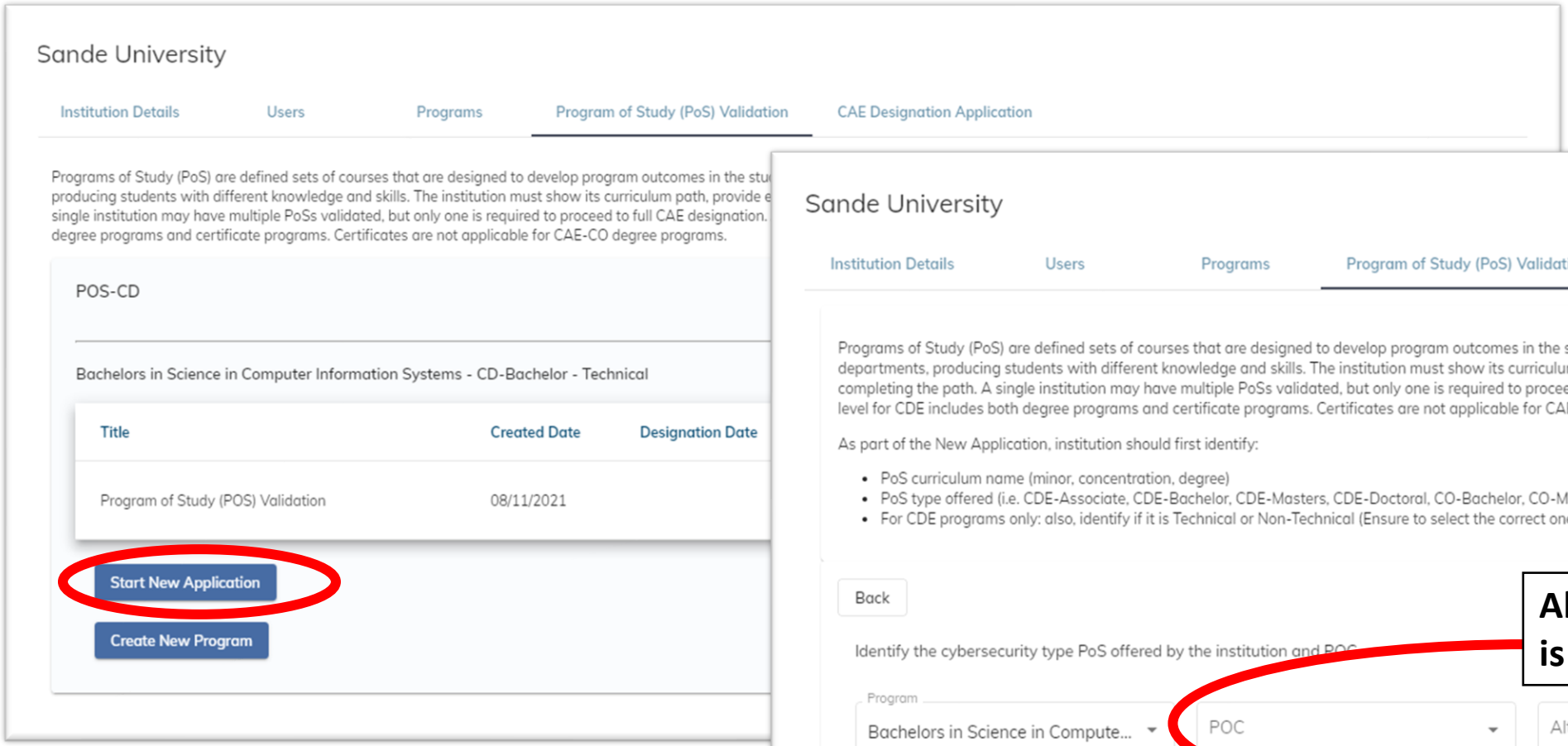
Official Program of Study Name & Designation Type

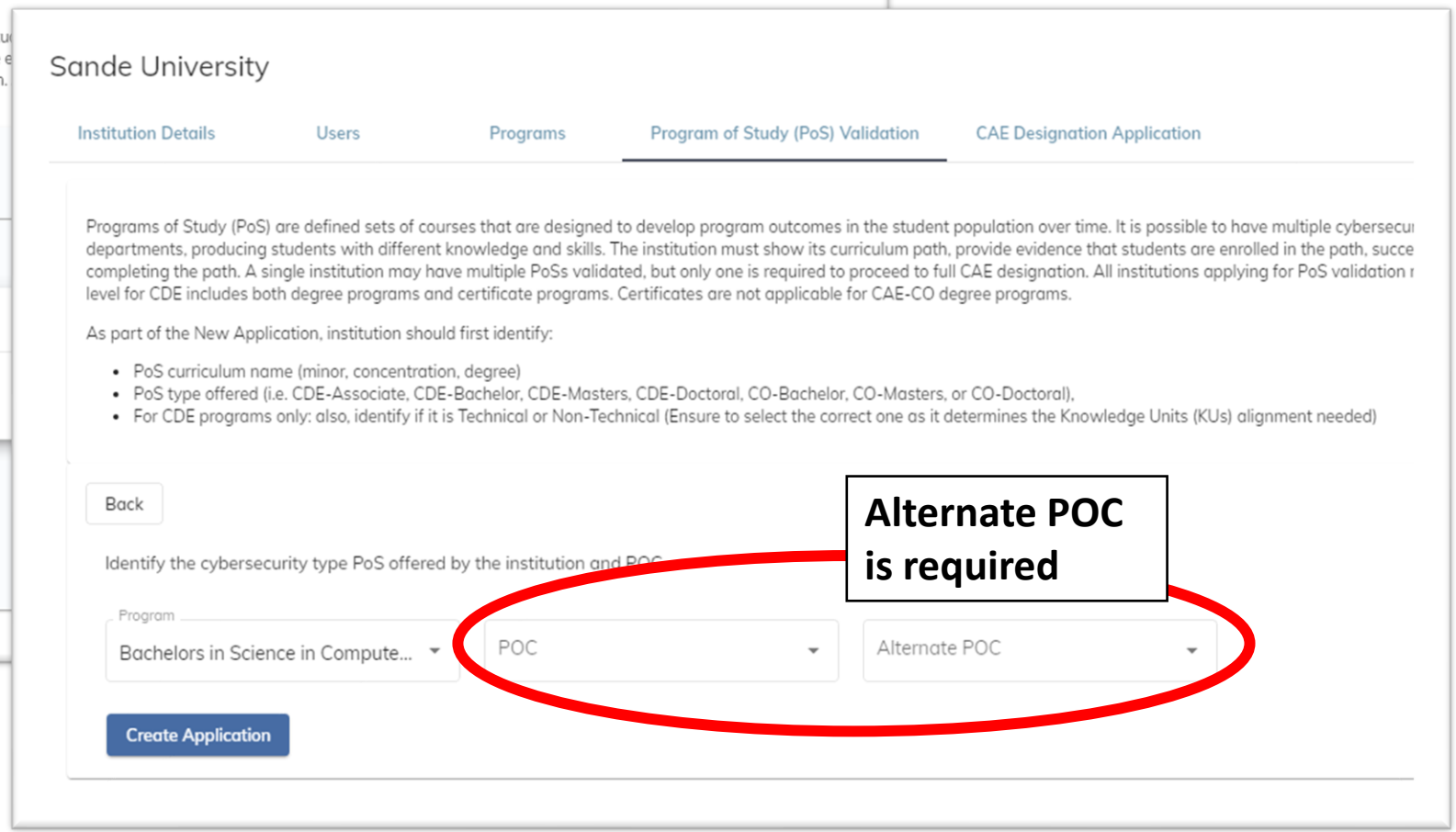


*Program name **must be the official program name** found in course catalogue.

**New programs must be approved by CNRC. Please allow up to 48 hours for approval.

Starting a New Application



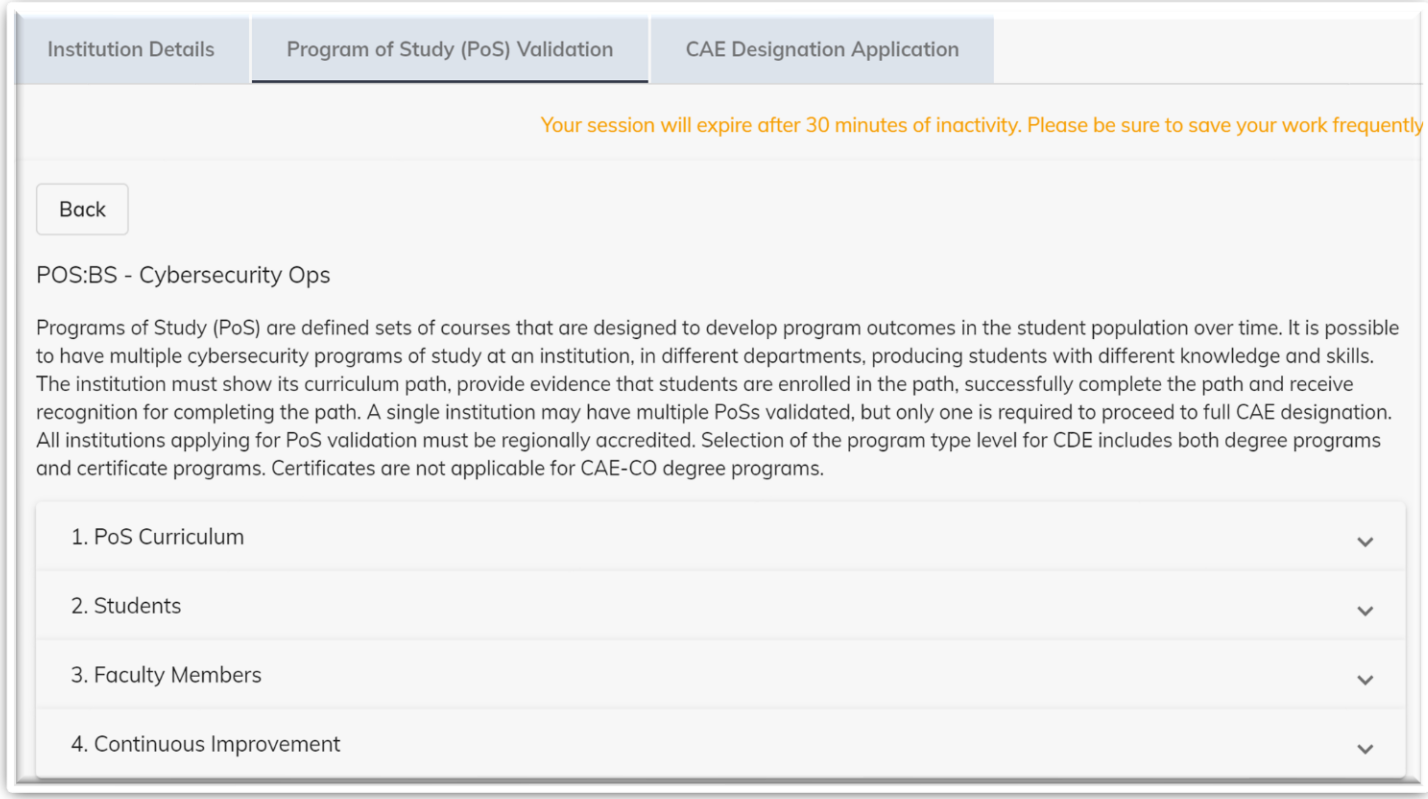


Part One: Program of Study Validation

Main Takeaways

- CO Application Process Changes (since circa 2019)
  - NSA PMO Merger – efficient, formal, process driven
  - Online not paper
  - KUs – learning outcomes are aligned instead of topics mapped
- While Completing the Application
  - Quality counts
  - Don’t make the reviewer think
  - Official university records
- Helpful Resources
  - NCyTE Website www.ncyte.net
  - Mentor

Part One: Program of Study Validation



Program of Study (PoS): Curriculum

Section 1a: The cybersecurity CAE-CO PoS offered by the institution

- Official PoS name **must match what is listed in the institutions course catalogue**.
- If application is approved, only the PoS identified is allowed to be marketed as validated.
- PoS curriculum must have been in existence for at least three (3) years **AND** have one (1) year of students who have completed the PoS curriculum by the time of final submission.
- Identify the Point-of-Contact (POC) and an alternate POC for the PoS (Department chair, faculty lead, CAE POC, etc.) including name, phone number, and e-mail address.

Program of Study (PoS): Curriculum

Section 1a: Only list courses

- Used to assess the Program-Level Learning Outcomes ***or,***
- Aligned to the Knowledge Units (KUs)

Section 1a: Courses must be

- Identifiable in current course catalog ***and,***
- Mandatory for students completing the PoS

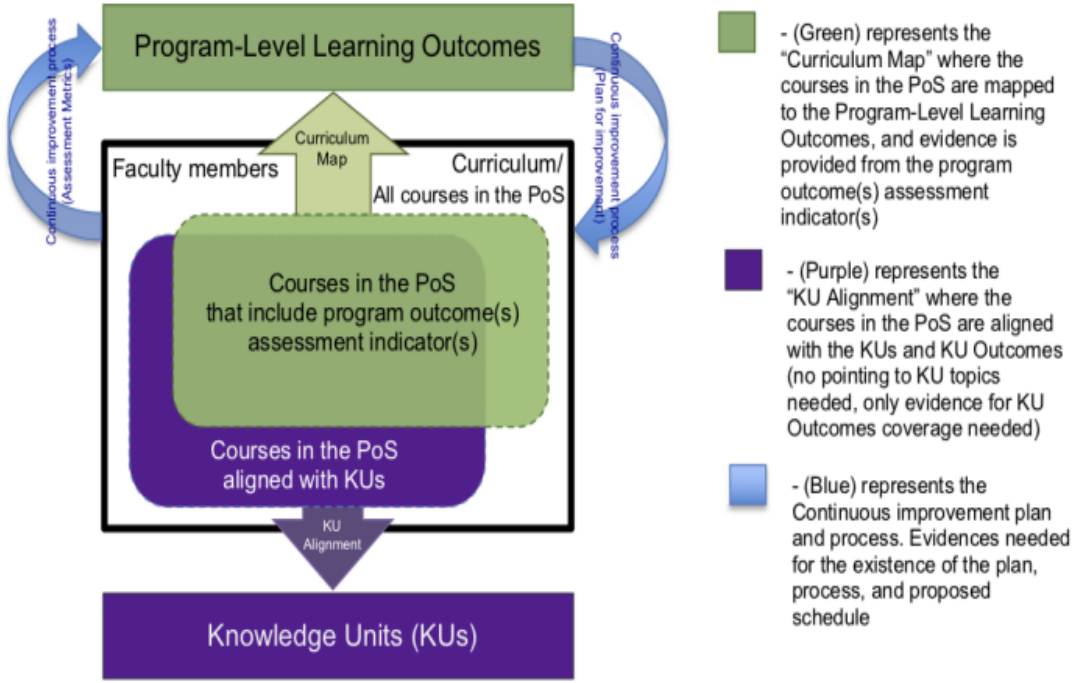


Figure 3. PoS Validation Conceptual Model

Program of Study (PoS): Curriculum

Section 1b: NICE Framework Crosswalk Alignment

- Provide the cybersecurity PoS crosswalk alignment with the NICE Cybersecurity Workforce Framework

Section 1c: Course Syllabi and Courses Requiring Applied Lab Exercises

- Provide a concise syllabus of each course in the KU alignment
- For KU aligned courses that require applied lab 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

Program of Study (PoS): Curriculum

Section 1d: Curriculum Map and Assessment Documentation

- Program-level learning outcomes measure the effectiveness of the selected program
- Outcomes must be on file at the institution
- Use the institutions current curriculum map and plan (don't update)

ABET:

- ABET Student Level Outcomes and Performance indicators = Program-level Learning Outcomes.

Program of Study (PoS): Curriculum

Section 1d: Curriculum Map and Assessment Documentation Requirements

- State the Program-Level Learning Outcomes of the PoS
- Documentation of the Program-Level Learning Outcomes
- Documentation of the Program-Level Learning Outcomes Curriculum Map and Plan
- For each Program-Level learning Outcome provide:
  - Documentation for the General information
  - Documentation of the Assessment of Indicators
  - Documentation of the Overall Assessment Information

Program of Study (PoS): Curriculum

Section 1e: KU Alignment

- Knowledge Units (KUs)
  - All CAE-CO programs need to cover the Mandatory and Optional Kus
  - No elective or optional courses should be included in the KU alignment for Mandatory KUs
  - 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.

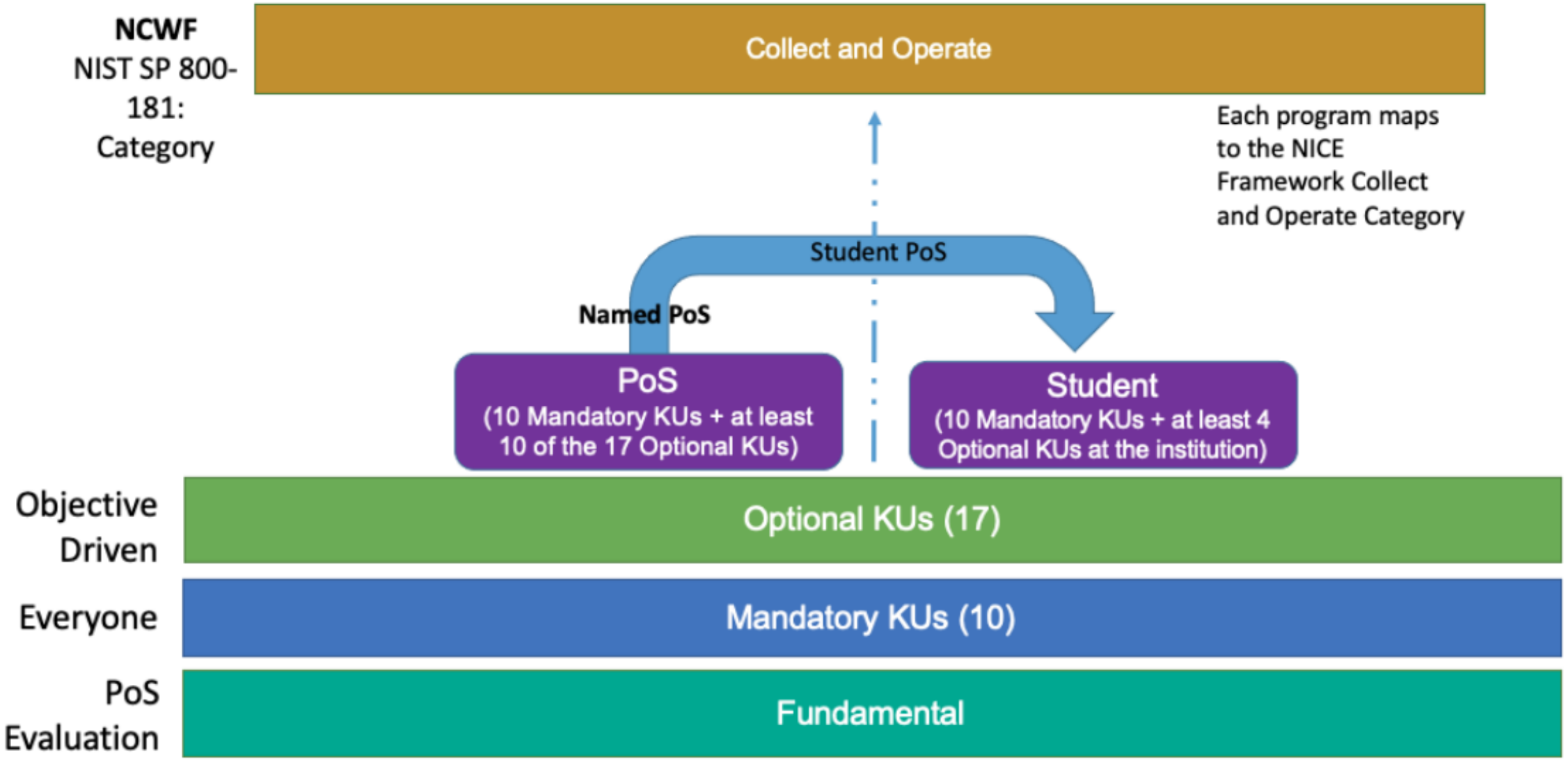


Figure 4. CAE-CO Knowledge Units Alignment Requirements

Curriculum Map and Plan (Example)

Program-Level Learning outcomes: Graduates should be able to…	ABC 140	ABC 145	ABC 106	ABC 110	ABC 116	ABC 205	ABC 214	ABC 215	ABC 216	ABC 226	ABC 227	ABC 228	ABC 229
1. Write programs in a variety of languages	I	A (2019-20)											
2. Identify threats and implement countermeasures to ensure network system security.				I			R	R	A (2023-24)				
3. Implement and troubleshoot a variety of network topologies and protocols.			I		R	R	R	R	R	R	R	R	A (2021-22)
4. Set up and maintain medium-size routed and switched networks.										I	R	R	A (2022-23)
5. Perform the basics of computer and network security.				I			R	R	A (2020-21)	R	R	R	R
6. Communicate professionally with customers and co-workers.						A (2018-19)	R	R					

* I, R, and A indicate the courses in which each Program-Level Learning Outcome is: introduced (I), reinforced (R), and formally assessed (A).

General Information for Program-Level learning Outcome (Example)

Date report submitted	11-18-2016 and 09-20-2018
Program faculty who contributed to this report	Jane Doe
Program-Level learning outcome	Perform the basics of computer and network security.
Course(s) that formally assess(es) this Program-level learning outcome (at its highest level, see curriculum map)	ABC 216 Industrial Control Systems Security
Number of students assessed for this program-level learning outcome	23
Quarter students were assessed (e.g., Winter 2020)	Winter 2020

Assessment of indicators for the program outcome (Example)

Indicators	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 214. 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 part of the project is basically a review of those skills, although they must set up a customized network to meet the criteria of the project.	Group Project	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

Overall Assessment of a Program-Level learning outcome (Example)

Overall, how well did the students perform on this program outcome?	**☐ below expected levels** **☐ at expected levels** **☐ above expected levels**
Analyze assessment of indicator results in section II: What does the information in section II 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	More lecture on Snort and writing snort rules in 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 2015.

Program of Study (PoS): Curriculum

Section 1e: Knowledge Units (KUs) Alignment

- The process of documenting how the KUs and KU outcomes are aligned to the relevant courses in the PoS

Requirements:

- Provide a narrative on the description of the PoS and explain the overall KU alignment to the PoS
- Provide the KU Alignment Summary Table for the PoS (example next slide)
- 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
- 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

KU Alignment Summary Tables

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

CAE-CO Program (Total 20 KUs min)																				
PoS Courses in	Mandatory KUs										Optional KUs (10 or more)									
KU Alignment	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	0?	0?	0?	0?	0?	0?	0?	0?	0?	0?
course 1																				
course 2																				
course 3																				
course 4																				
course 5																				
etc.																				

Program of Study (PoS): Student Information

Section 2a: Student Enrollment / Graduation in the PoS

- Provide student enrollment in PoS for the last three years
- Provide official institutional letter for the enrollment/graduation
  - Letter from Registrar or equivalent
- Provide at least three redacted student transcripts, dated within the last three years and clearly highlight the courses taken that meet the PoS
  - All courses with KU alignment and those identified in the curriculum map must appear on transcript

Program of Study (PoS): Student Information

Section 2b: Cyber Operations Recognized

Cyber operations must be explicitly recognized as a degree program or a focus area or a specialization or a concentration and students must m

Required:

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

Program of Study (PoS): Student Information

Section 2c: Student Work Products

- Provide samples of six students work products from six different assignments (six files total).
- Provide the guidelines (what student are asked to do)
- Remove student name prior to submission

Program of Study (PoS): Student Information

Section 2d: Student Participation in Extracurricular Activities

- Provide evidence of three students participation in extracurricular activities within the last three years
- Provide date and description of each activity
- Examples: local/regional/national cyber exercises and competitions, outreach to community, summer internship program, industry guest lectures

Program of Study (PoS): Student Information

Section 2e: Student Cybersecurity Research

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

- Provide samples of three students' cybersecurity research products (papers, assignments, projects, presentations, etc.) (three files total).
- Remove student name prior to submission
- Remove comments and grade
- Include guideline

Program of Study (PoS): Student Information

Section 2f: Cyber Operations Interdisciplinary Student Exposure

The goal of the CAE-CO program is to produce graduating students with a well-rounded educational foundation that enables them to better function in the world of specialized cyber operations.

- Identify the PoS courses that interdisciplinary components from other disciplines (i.e. policy, social, human factor, legal and ethical aspects of conducting cyber operations) have been integrated into the cyber operations PoS courses
- Provide three different student sample work from three different courses (one example from each 8 course) where interdisciplinary components from other disciplines have been integrated into the cyber 9 operations PoS courses.

Program of Study (PoS): Faculty

Sections 3a to 3d: Faculty Members

- The cybersecurity faculty should have appropriate experience associated with the PoS and courses they are assigned.
- A portion of faculty must be fulltime members teaching in the PoS, with the remainder being adjuncts or part-time

Requirements:

- Identify the Point-of-contact (POC) for the PoS and alternate POC
- Provide a CV for each faculty member (10 max)
- Provide evidence of participation or sponsorship of cybersecurity exercises and competitions within the last 3 years. Examples include: clubs, cyber defense exercises
- Provide evidence of institutional process for faculty promotion / reappointment

Program of Study (PoS): Continuous Improvement

Section 4: Continuous Improvement Plan

- A key element to ensure vitality and functionality over time is a strong continuous improvement plan, process, and regular evaluation schedule

Section 4a: Requirements

- 4a: Continuous improvement plan for the PoS
  - Strategic process planning goals for the PoS
  - The Program-Level Learning Outcomes for the PoS
  - Description of the assessments of the Program-Level Learning Outcomes
  - Proposed changes to enhance the quality of the PoS

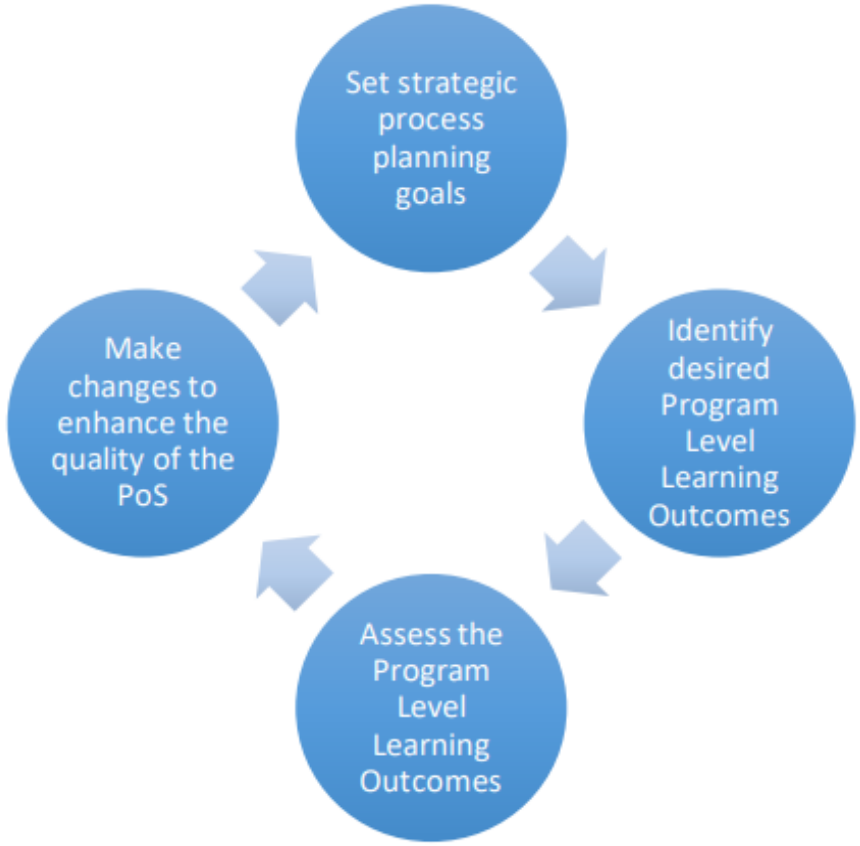
Program of Study (PoS): Continuous Improvement

Section 4b: Continuous Improvement Process

- Provide documentation of the Continuous Improvement Process with specific improvement efforts linked to assessments

Section 4c: Regular Evaluation Schedule

- Provide documentation of the Continuous Improvement - Regular Evaluation Schedule



Break

Workshop will resume in 10 minutes.

Part Two: CAE Designation

Section
1. Accreditation
2. Institution Commitment
3. Evidences of Sound Cybersecurity Posture and Plan
4. Established "Center" for Cybersecurity
5. Affirmation of the CAE Core Values and Guiding Principles
6. Sustainability
7. Professional Development
8. Commitment to Support the CAE-CO Program

CAE Designation

Section 1: Accreditation

- The Academic institution must be regionally accredited
- http://ope.ed.gov/accreditation/

Requirement

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

CAE Designation

Section 2: Institution Commitment

A 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.

CAE Designation

Section 3: Evidence of sound cybersecurity posture and plan

Institutions shall have a sound institutional cybersecurity posture and plan including a dedicated official to oversee its implementation to provide an overview of the institution's ability to protect critical information and systems processing that information at the institution.

CAE Designation

Section 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

- Center website (url) is visible within the institution and the external community at large and must be located on institution's website with an .edu address
- Center POC is noted on "Center" website
- Faculty members are listed
- Links to student Cybersecurity activities available to students at the institution and beyond

CAE Designation

Section 5: Affirmation of the CAE Core Values and Guiding Principles

- **Ethical Behavior**
  - The Institution must encourage and support ethical behavior by students, faculty, administrators, and professional staff
- **Share Core Values**
  - 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
- **Lead by Example**
  - The "Center" demonstrates a commitment to address, engage, and respond to current and emerging cybersecurity issues both in the classroom and in the institution itself

CAE Designation

Section 6: Sustainability

- 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.

CAE Designation

Section 7: Professional Development

- Ongoing access to working professionals and practitioners during their time in a CAE-C program is needed by both faculty and students 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.
- Requirement: Provide six separate examples of professional development opportunities provided to faculty and students over the past three years

CAE Designation

Section 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. Cybersecurity concepts must be integrated into additional degree programs within the institution **outside the PoS(s) applied for or previously validated**
- Three different syllabi with course name and cyber modules clearly highlighted

CAE Designation

Section 8: Commitment to Support CAE-CO Program

The CAE-CO applying institution must demonstrate commitment to the CAE-CO program.

Examples:

- Student participation in the CAE-Cyber Operations Summer Internship Program or advanced CO competitions
- Faculty participation in KU review and changes, CAE-CO related activities offered by the PMO, working groups, supporting program initiatives
- Faculty support in the form of acting as a mentor or application reviewer,
- Faculty briefing or teaching during the CAE-Cyber Operations Summer Internship Program, Tech Talks and/or CAE Forum webinars

CAE Designation

Section 8: Commitment to Support CAE-CO Program (continued)

Additional opportunities for new institutions

- **Events**
  - Submit a CAE Forum / CAE Techtalk
    www.caecommunity.org
- **Contributions**
  - Submit to CLARK.CENTER
    https://clark.center/home
  - The CAE Resource Directory (CARD)
    https://caeresource.directory/home

CLARK

CARD
The CAE Resource Directory

Post-Designation Reporting Requirements

- Continuous improvement plan & process
- Institutional metrics
- Newly designated institutions will attend orientation and designation ceremony
- Prepare an annual report
- Send a representative to an annual CAE community symposium and/or the annual POC meeting and/or regional CAE community meetings
- Maintain designated program
- Maintain correct contact information
- Report major PoS changes

Additional Resources

- Centers of Academic Excellence in Cyber Defense Resources
- https://public.cyber.mil/ncae-c/
- CAE Community website
- https://www.caecommunity.org/
- National Cybersecurity Training & Education Center
- https://www.ncyte.net/

Contact Information:

- CAE Candidates Program at Whatcom:
  - NCyTE@Whatcom.edu
- NSA CAE Program Office:
  - CAEPMO@nsa.gov

NCyTE CENTER

We want to hear from you!
Please complete our CAE Workshop Survey.

https://www.surveymonkey.com/r/9TBFPH3