Center of Academic Excellence (CAE) in Cyber Operations (CO) Designation

Program of Study / CAE Designation Summary

NSA's CAE in Cyber Operations (CAE-CO) program supports the President's National Initiative for Cybersecurity Education (NICE): Building a Digital Nation, and furthers the goal to broaden the pool of skilled workers capable of supporting a cyber-secure nation.

The CAE-CO program is a deeply technical, inter-disciplinary, higher education program firmly grounded in the computer science, computer engineering, and/or electrical engineering disciplines, with extensive opportunities for hands-on applications via labs and exercises.

The CAE-CO program complements the existing CAE in Cyber Defense (CAE-CD) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our Nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations.

By completing the CAE-CO checklist you are affirming your institution's readiness to apply for the Program of Study (PoS) validation and the Center of Academic Excellence (CAE) designation. Completing the checklist is the first step in this process and does not guarantee your institution's final approval for the PoS validation or CAE designation. This checklist is for new CO schools only and is not for currently designated CAE-CO schools seeking redesignation.

Institutions wishing to earn the **Center of Academic Excellence in Cyber Operations (CAE-CO) Designation** for a particular program of study will apply in two parts.

Part 1: Program of Study (PoS) Review: The process will begin with the submission of elements pertaining to the academic program of study, including curriculum, faculty profiles and qualifications, maturity of the program, and so on. Prospective CAE-CO Institutions must proceed to Part 2 after completing Part 1.

Part 2: CAE Designation: Once the program of study has been reviewed, the institution may pursue CAE designation. To be eligible for designation, the academic institutions must hold a current regional accreditation as outlined by the Department of Education (https://www.ed.gov/accreditation).

CAE-Cyber Operations (CAE-CO)

Program of Study (PoS) / Designation

Checklist

Centers of Academic Excellence (CAE) Information:

- Is your institution pursuing re-designation? Yes/No
  - If yes, please list the re-designating program name below:
    -
- Is your institution validating an additional program of study? Yes/No
  - If yes, please list all current PoS validations and CAE designations below:
    -
- Have you previously earned the Cyber Operations program of study validation / CAE designation at your institution? If you are unsure, refer to the CAE Map at https://caecommunity.org/cae-map Yes / No
  -
  - If yes, you must verify that you have contacted the current POC to inform of your intent to pursue validation and/or designation. The current POC will serve as your mentor. Have you communicated your intent to apply to the CAE designated POC? Yes / No
    -

College Information:

Institution Name:
Institution address:

- Name of *Regional Accreditation Agency(required)*:
- Name of chosen program of study (PoS):
- Department that houses the program of study:
- Program of Study type:
  - Doctoral:
  - Masters:
  - Bachelors
  - Other
  - Link to the webpage for the PoS:
  - Link to the online course catalog for the PoS:

- If the proposed PoS is ABET accredited, please list the accreditation type (e.g., Computer Science, Cybersecurity, etc.)
    - If the proposed PoS is resides within an ABET accredited program, please list the accreditation type (e.g., Computer Science, Cybersecurity, etc.)

Point of Contact (POC) Information:

Note: The POC must be a full-time **faculty member** of the institution directly involved with the representative academic program. This will be the person who will be contacted by the PMO and/or the National Centers for all NCAE-C program updates, grants and scholarship opportunities, upcoming events, and other administrative communications. This person is responsible for the Annual Report, Re-designation, and any other important milestones in the institution's NCAE-C participation.

- Title:
- First:
- Last:
- POC Phone:
- POC Email (must be .edu):

Alternate Point of Contact (POC) Information:

Note: The Alternate POC must be a **full-time employee** of the institution associated with the Designation and PoS.

- Title:
- First:
- Last:
- Alternate PoC Phone:
- Alternate PoC Email (must be .edu):

Please indicate 'Yes', 'No', or 'Unknown' to the questions below and submit the checklist; you will be contacted with information on how to continue.

Centers of Academic Excellence (CAE) in Cyber Operations (CO)			
Criteria Description	**Yes**	**No**	**Unknown**
Has your institution previously earned the CAE-CO designation?			
Have you attended a CAE-CO workshop in the past six (6) months?			
Have you been approved by your institutions administration to pursue the CAE-CO?			
Has your selected Program of Study been in existence for three (3) years with one (1) year of graduates?			
Have you reviewed the Program of Study (PoS) validation and CAE designation requirement documents? CAE-CO Document: https://public.cyber.mil/ncae-c/documents-library/			

PoS Knowledge Unit (KU) Requirements:

For an explanation of KU requirements refer to the CAE-CO Program Guidance document and the CAE-CO Knowledge Units document found on NCAE-C's web page https://public.cyber.mil/ncae-c/documents-library/.

List the courses in which the ten mandatory KUs are taught:

Mandatory KUs	Course(s)
M1: Cyber Policy, Law, and Ethics	
M2: Computer Science Foundations	
M3: Operating Systems	
M4: Computer Networks	
M5: Systems Programming	
M6: Cybersecurity Foundations	
M7: Applied Cryptography	
M8: Software Reverse Engineering	
M9: Defensive Cyber Operations	
M10: Offensive Cyber Operations	

List the four optional KUs taught in the program and the courses in which they are taught:

Four Optional KUs	Course

Please indicate 'Yes', 'No', or 'Unknown' to the questions below.

Program of Study (PoS) Requirements				
Criteria Name	**Description**	**Yes**	**No**	**Unknown**
1. Program of Study (PoS): Curriculum	Is your Cyber Operations program based within a computer science, electrical engineering or computer engineering department, or a degree program of equivalent technical depth, or a collaboration between two or more of these departments?			
	Does your PoS align with the CO Student Outcomes?			
	Are you familiar with your institution's accreditation process and program-level learning outcomes?			
	Does your PoS require a substantial amount of hands-on labs and programming assignments?			
	Are you familiar with curriculum maps?			
	Does your program of study teach the ten mandatory KUs?			
	Does your program of study teach at least four of the optional KUs?			
2. Students				
	Are you able to provide student research projects in cyber operations (student names redacted)?			
	Are you able to provide evidence that students participate in activities that contribute to growing and strengthening the cyber operations community and cyber security for the Nation?			

	Are you able to provide student transcripts (redacted) to demonstrate that students have completed the selected PoS at your institution?			
	Do all graduating students in the program of study complete the 10 Mandatory KUs?			
	Do all graduating students in the program of study complete at least 4 of the Optional KUs?			
	Students will be able to write computer network applications that employ standard and custom protocols.			
	Students will be able to write systems programs in C that leverage assembly language and operating system calls.			
	Students will be able to write software that performs cryptographic operations using standard libraries..			
	Students will be able to safely reverse engineer and document software of unknown origin and malware.			

	Students will be able to conduct enumeration and scanning of target networks.			
	Students will be able to write malware to exploit vulnerabilities.			

3. Program Faculty	Is there someone with overall responsibility for the selected PoS?			
	Do you have faculty involved in cyber operations education who are also active in research related to cyber operations?			
	Do you have the equivalent of at least two full-time faculty members teaching relevant cyber operations courses who are also active in relevant cyber operations research?			

CAE Designation Requirements				
Criteria Name	**Criteria Description**	**Yes**	**No**	**Unknown**
Institution Commitment	Is your institution able to provide evidence of their commitment to excellence in the cyber operations field?			
	For initial applying institutions, are you able to make a stated commitment to support the CAE-Cyber Operations program?			
	Does your Provost or higher support the efforts of earning the CAE-CO designation?			
Established "Center" for Cybersecurity	Does your institution have an officially established cyber center (physical or virtual)?			
	Does your cyber center have an external board of advisors?			
	Is your cyber center website visible within the institution and the external community?			
Institutional Security Plan	Are you able to provide evidence of your institution's information system security plan and policies?			
	Does your institution have an Information System Security Officer (ISSO) to oversee Security?			
	Does your institution provide cybersecurity awareness training, online help, and security best practice guides for students, faculty, and staff?			
Acknowledgement	I certify that the information is true and correct to the best of my knowledge: *Yes/No*			NA

*I certify that the information is true and correct to the best of my knowledge: *Yes/No*