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.

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

College Information:

- Institution Name:
- Name of *Regional Accreditation Agency*:
- Name of Program accreditation agency (optional)
    - Institution Street Address:
    - City, State, Zip:
- Name of chosen program of study (PoS):
- Department that houses the program of study:
- Program of Study type:
    - Doctoral:
    - Masters:
    - Bachelors:
    - other:

Point of Contact (POC) Information:

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

Secondary Point of Contact (POC) Information:

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

President/ Provost Information:

- Title:
- First

- Last:
- Phone:
- Email:

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 the NCAE-C web page https://public.cyber.mil/ncae-c/documents-library/.

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

- List the courses in which the ten optional KUs are taught:

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

Program of Study (PoS) Requirements				
Criteria Name	**Criteria Description**	**Yes**	**No**	**Unknown**

Program of Study (PoS) General Information	Is your academic institution regionally accredited?			
	Has your Institution previously earned the Centers of Academic Excellence (CAE) designation in Cyber Operations?			

	Have you attended a CAE workshop in the past 6 months?			
	Have you been approved by your institutions administration to pursue the CAE-CO designation?			
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?			
	Are you able to identify interdisciplinary components and/or courses required in the PoS?			
	Are you familiar			

	with your institutions accreditation process?			
	Are you familiar with program-level learning outcomes?			
	Are you familiar with curriculum maps?			
	Does your program of study teach the ten mandatory KUs?			
	Does your program of study teach at least ten of the optional KUs?			
2. Students	Has the selected PoS been in existence for three (3) years with one (1) year of graduates?			
	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?			
	Affirm all students graduating in this program are able to do each of the following or an assignment of equivalent complexity.			

	Can you affirm all students graduating in this program are able to do the following or of equivalent complexity?			
	Students will be able to write a functional, stand-alone assembly language program, such as a simple telnet client, with no help from external libraries.			
	Students will be able to use tools such as IdaPro and Ghidra to safely perform static and dynamic analysis of software (or malware) of potentially unknown origin, including obfuscated malware, to fully understand the software's functionality.			
	Students will be able to describe user associations and routing in a cellular/mobile			

	network, interaction of elements within the cellular/mobile core, and end-to-end delivery of a packet and/or signal and what happens with the hand-off at each step along the communications path. They will be able to explain differences in core architecture between different generations of cellular and mobile network technologies.			
	Students will understand how automata are used to describe computing machines and computation, and the notion that some things are computable and some are not. They will understand the connection between automata and computer languages and describe the			

	hierarchy of language from regular expression to context free.			

3. Program Faculty	Is there someone with overall responsibility for the selected PoS?			
	Do you have faculty involved in cyber operations education 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
1. 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 pursue of earning the CAE-CO designation?			
2. 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?			
4. Institutional Security Plan	Are you able to provide evidence of your institutions information system security plan and policies?			
	NOTE: For the final application, evidence of such a plan must be provided.			
	Does the 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?			

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