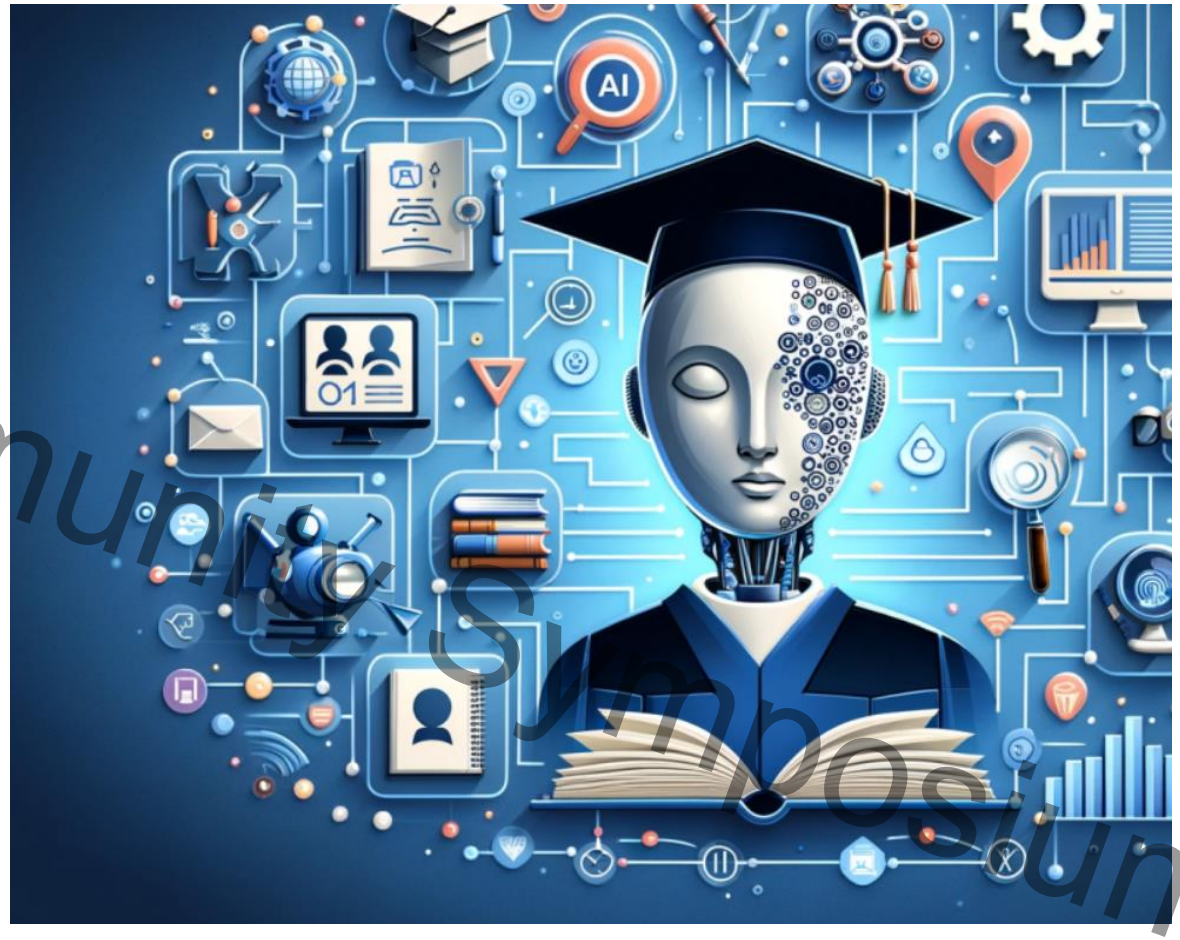
National Centers of Academic Excellence-Cybersecurity

CyberAI Programs of Study



Introductions

Dr. Victor Piotrowski- Senior Advisor for AI and Cyber, National Science Foundation

Angie Painter- CyberAI Program of Study Lead, NCAE-C PMO, National Security Agency

Stephen Troupe- Director of the CAE Candidates National Center (CCNC), Whatcom Community College

Dr. Sidd Kaza- Associate Provost for Research & Dean of Graduate Studies, Towson University, CyberAI CoP Lead

Dr. Blair Taylor- Director of the Center for Interdisciplinary and Innovation Cybersecurity, Towson University, CyberAI CoP Lead

NSF authorized to establish AI SFS program

Fulfilling National Science Foundation (NSF) request to establish a Program of Study in Artificial Intelligence in Cybersecurity for the NCAE-C program.

NSF has a mandate from congress per the 2022 CHIPS and Science Act to establish a scholarship-for-service program in AI, and to explore the advisability of establishing a CAE program for AI.

First step was to define Knowledge Units (KUs) for AI in cybersecurity and to run a pilot on a Program of Study (PoS) based on KU's for CAE Cyber Defense and CAE Cyber Operations designated institutions.

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University

CyberAI Program of Study (PoS)

In February 2024, the National Security Agency (NSA) National Centers of Academic Excellence in Cybersecurity (NCAE-C) program in collaboration with NSF, launched an initiative to outline the AI content cybersecurity academic programs need to teach their students.

- PoS Development:
  - Collaborative process between educators, government entities, and industry representatives
  - Labor-intensive and iterative process that can take years
- CyberAI PoS Challenges:
  - Timeline was ~6 months
  - The field of AI is evolving as quickly as the PoS was being developed

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University

2025 CAE Community Symposium

NSF/NSA

Cyber AI Programs

www.towson.edu/cyberai

Lead Authors

Banik, Shankar - The Citadel, CAE-CD

El-Sheikh, Eman - University of West Florida, CAE-CD

Flores, Paige - Towson University, CAE-CD, CAE-CO

Hamman, Seth - Cedarville University, CAE-CD, CAE-CO

Kaza, Sidd - Towson University, CAE-CD, CAE-CO

Levy, Yair - Nova Southeastern University, CAE-CD, CAE-R

Nestler, Vincent - California State University, San Bernardino, CAE-CD

Sajid, Md - Towson University, CAE-CD, CAE-CO

Samtani, Sagar - Indiana University, CAE-CD, CAE-R

Tague, Patrick - Carnegie Mellon University, CAE-CD, CAE-CO, CAE-R

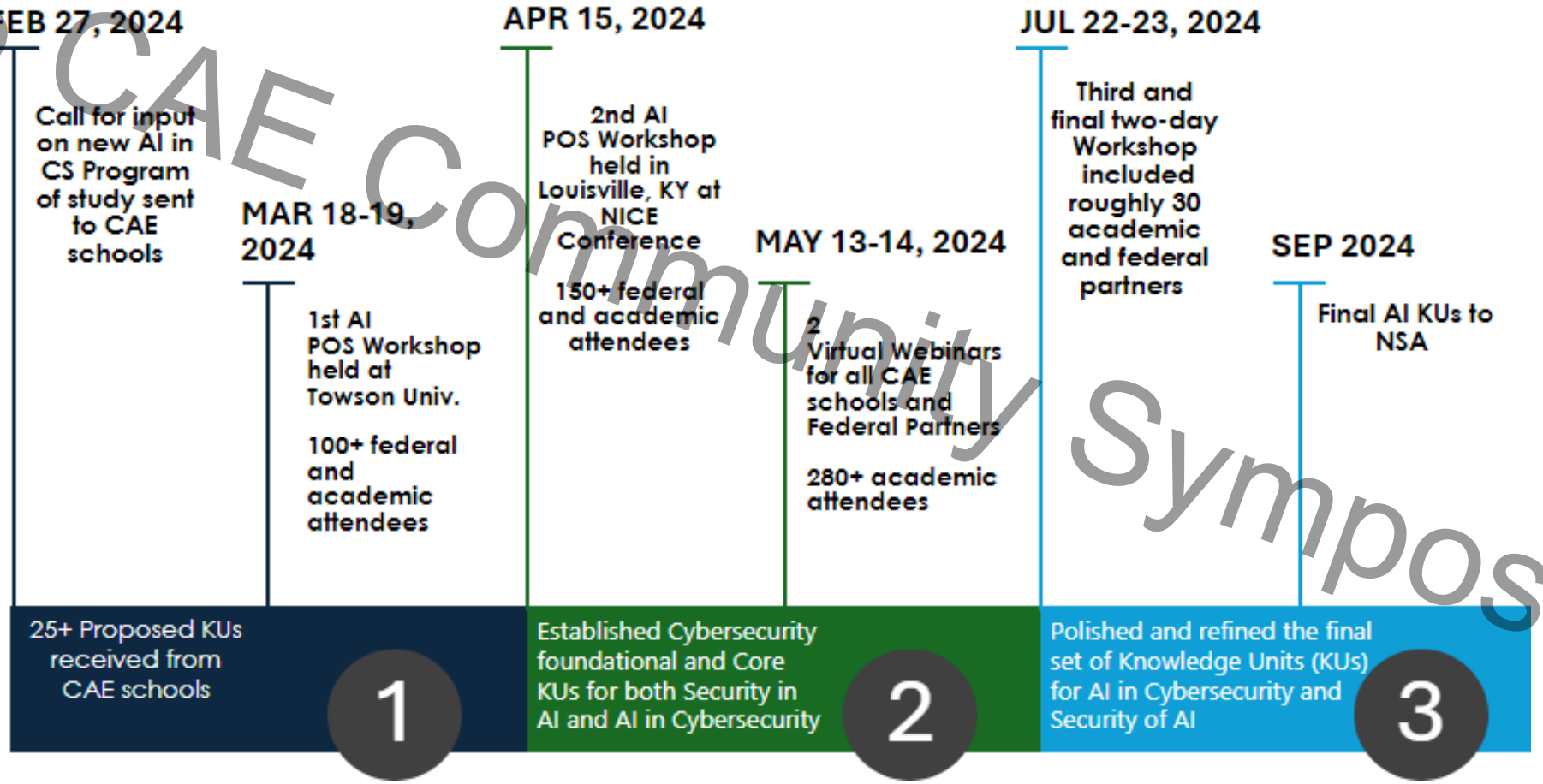
Taylor, Blair - Towson University, CAE-CD, CAE-CO

Wagner, Paul - University of Arizona, CAE-CD, CAE-CO, CAE-R

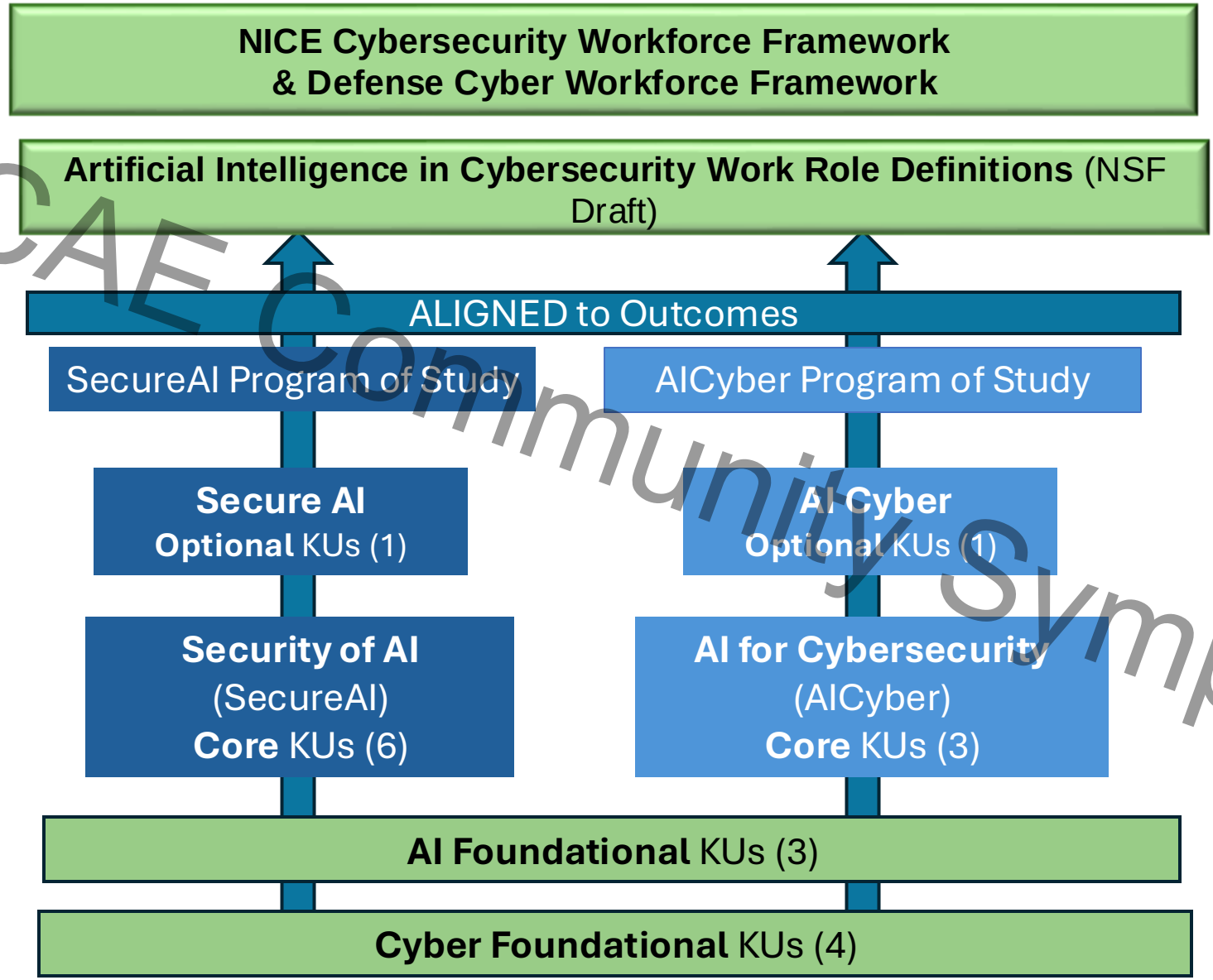
This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University

CyberAI Timeline

Goal: Build NCAE-C Program of Study for AI in Cybersecurity



CyberAI Knowledge Units



Outcome:
SecureAI
Program of Study

Must be CO or CD Designated

Program rigor will dictate which PoS students choose

Outcome:
AICyber
Program of Study

Must be CD or CO Designated

Will compliment CD or CO PoS – could be Minor or Electives

Security of AI (SecureAI) Program of Study

Cyber Foundational KUs (4)

- Cybersecurity Fundamentals
- IT Systems Components
- Basic Scripting and Programming
- Math Fundamentals

AI Foundational KUs (3)

- AI Governance, Laws & Ethics
- AI Fundamentals
- Machine Learning Fundamentals

SecureAI Core KUs (6)

- Computer Science Fundamentals (CO)
- Advanced Math for AI
- Securing the AI Lifecycle
- Machine Learning Algorithms
- Deep Learning
- Adversarial Learning

Optional KUs (1)

- Model Selection, Evaluation & Specification
- Risk Management of AI

towson.edu/cyberai (Stoneman)

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University

AI for Cybersecurity (AICyber) Program of Study

Cyber Foundational KUs (4)

- Cybersecurity Fundamentals
- IT Systems Components
- Basic Scripting and Programming
- Math Fundamentals

AI Foundational KUs (3)

- AI Governance, Laws & Ethics
- AI Fundamentals
- Machine Learning Fundamentals

AICyber Core KUs (3)

- Basic Networking (CAE-CD)
- Network Defense (CAE-CD)
- AI for Security Assessment

Optional KUs (1)

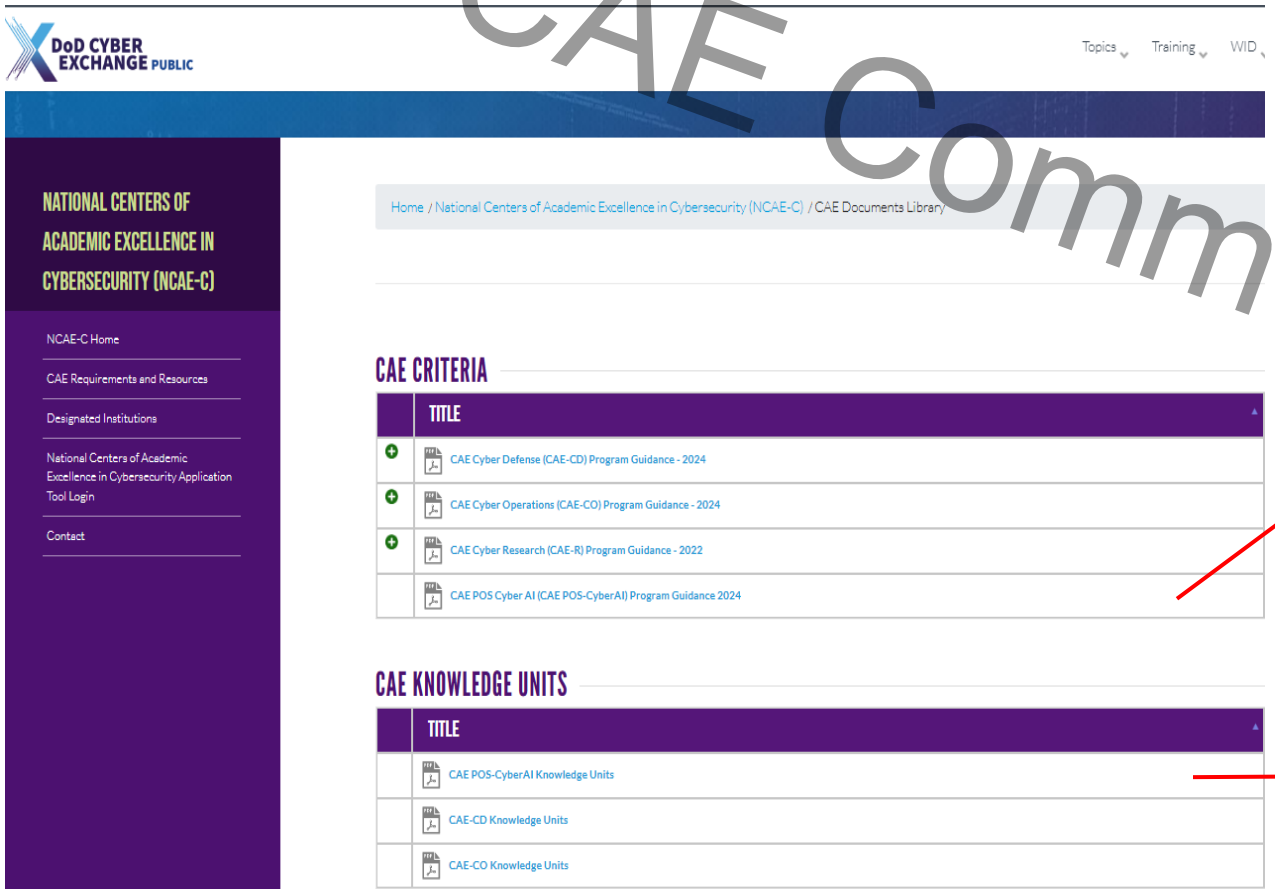
- Defensive Applications of AI
- Offensive Applications of AI

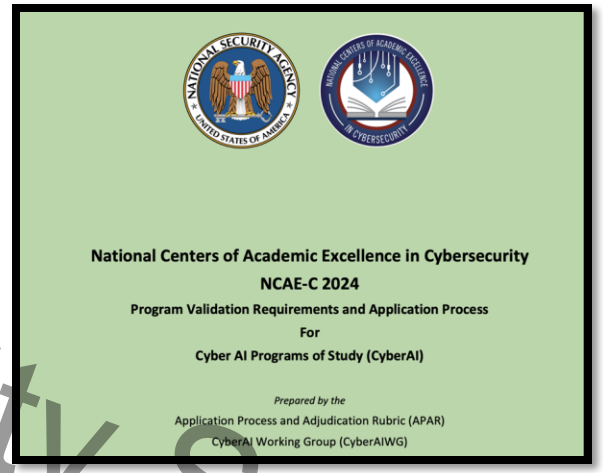
towson.edu/cyberai (Stoneman)

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University

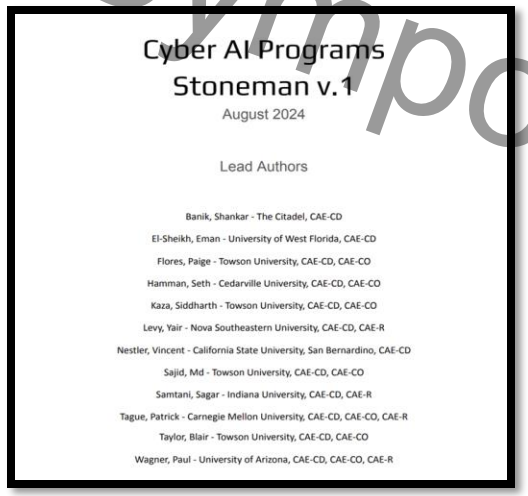
CyberAI Requirements Document and Knowledge Units found:

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




National Centers of Academic Excellence in Cybersecurity
NCAE-C 2024
Program Validation Requirements and Application Process
For
Cyber AI Programs of Study (CyberAI)

Prepared by the
Application Process and Adjudication Rubric (APAR)
CyberAI Working Group (CyberAIWG)


Cyber AI Programs
Stoneman v.1
August 2024

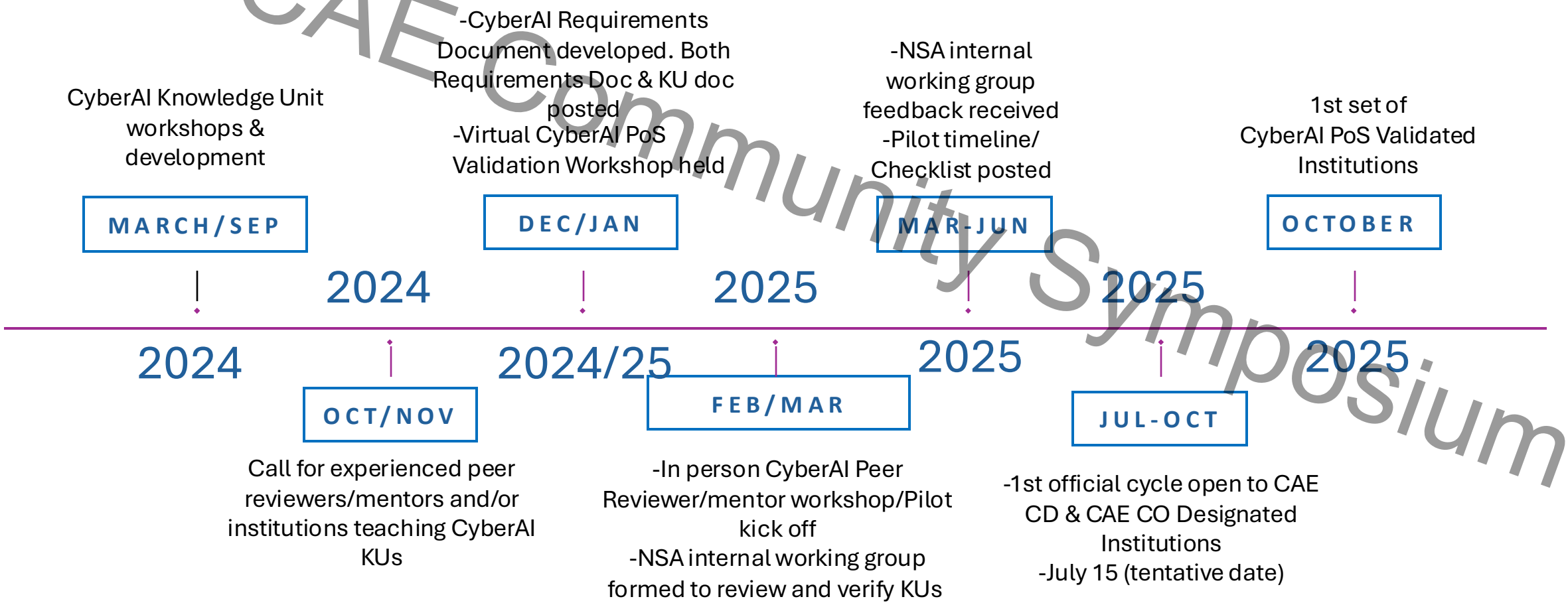
Lead Authors

Banik, Shankar - The Citadel, CAE-CD
El-Sheikh, Eman - University of West Florida, CAE-CD
Flores, Paige - Towson University, CAE-CD, CAE-CO
Hamman, Seth - Cedarville University, CAE-CD, CAE-CO
Kaza, Siddharth - Towson University, CAE-CD, CAE-CO
Levy, Yair - Nova Southeastern University, CAE-CD, CAE-R
Nestler, Vincent - California State University, San Bernardino, CAE-CD
Sajid, Md - Towson University, CAE-CD, CAE-CO
Samtani, Sagar - Indiana University, CAE-CD, CAE-R
Tague, Patrick - Carnegie Mellon University, CAE-CD, CAE-CO, CAE-R
Taylor, Blair - Towson University, CAE-CD, CAE-CO
Wagner, Paul - University of Arizona, CAE-CD, CAE-CO, CAE-R

Timeline

AI FOR CYBERSECURITY (AICYBER) PROGRAM OF STUDY

SECURITY OF AI (SECUREAI) PROGRAM OF STUDY



Pilot Timeline

Timeline:

- ✅ **In-person Workshop:** March 6-7, 2025
- ✅ **Pilot start:** March 7, 2025
- ⬛ **PSR deadline:** May 1, 2025
- ⬛ **PSR feedback review:** May 15, 2025
- ⬛ **Final peer review submission:** May 30, 2025
- ⬛ **AI Feedback meeting:** June 5, 2025
- ⬛ **Final adjustments to requirements document & tool:** June 30, 2025

📌 **First official Cycle begins July 15, 2025**

CAE Checklist

CAE-CD Program Eligibility and Summary

The CAE-CD Program is open to current regionally accredited:

- Four-year Colleges
- Graduate-level Universities
- Two-year Community Colleges
- Technical Schools
- State or Federally Endorsed Cybersecurity Training Centers
- U.S. Government Cybersecurity Training Centers

Start Applicant Checklist

Download CAE-CD Checklist

CAE-CO Program Eligibility and Summary

The CAE-CO Program is open to current regionally accredited:

- Four-year Colleges
- Graduate-level Universities
- Must be 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

Start Applicant Checklist

Download CAE-CO Checklist

CAE-R Program Eligibility and Summary

The CAE-R Program is open to current:

- Department of Defense (DoD) schools
- Ph.D. producing military academies
- Regionally accredited, degree granting four-year institutions rated by the Carnegie Foundation Basic Classification system as either:
  1. Doctoral University – Highest Research Activity (R1)
  2. Doctoral University – Higher Research Activity (R2) or
  3. Doctoral University – Moderate Research Activity (R3)

Start Applicant Checklist

Download CAE-R Checklist

CyberAI PoS Checklist COMING SOON…

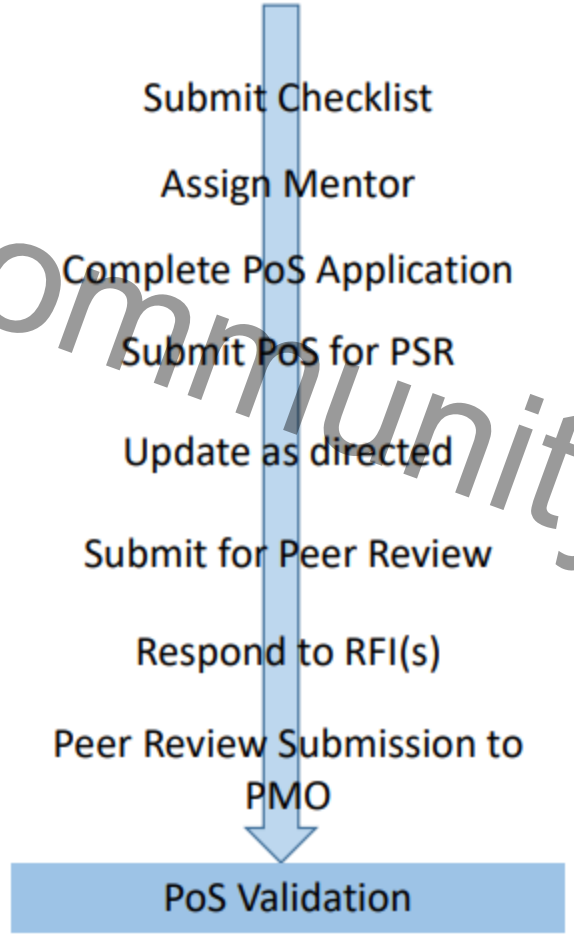
Must hold a CAE-CD or CAE-CO to Apply for CyberAI PoS Validation

*Once released, PMO will inform all CAE CD/CO Designated institutions

https://caecommunity.org/about-us/national-cae-cybersecurity-program/applicant-checklist

Application Process

Must hold a CAE-CD or CAE-CO to Apply for CyberAI



First Official Cycle

POS CYCLE*	ACCESS TO APPLICATION	APPLICATION DUE**	PSR FEEDBACK DEADLINE***	FINAL SUBMISSION
PoS Cycle 16	10/15/2023	12/15/2023	12/30/2023	1/15/2024
PoS Cycle 17	1/15/2024	3/15/2024	3/30/2024	4/15/2024
PoS Cycle 18	4/15/2024	6/15/2024	6/30/2024	7/15/2024
PoS Cycle 19	7/15/2024	9/15/2024	9/30/2024	10/15/2024
PoS Cycle 20	10/15/2024	12/15/2024	12/30/2024	1/15/2025
PoS Cycle 21	1/15/2025	3/15/2025	3/30/2025	4/15/2025
PoS Cycle 22	4/15/2025	6/15/2025	6/30/2025	7/15/2025
PoS Cycle 23	7/15/2025	9/15/2025	9/30/2025	10/15/2025
PoS Cycle 24	10/15/2025	12/15/2025	12/30/2025	1/15/2026
PoS Cycle 25	1/15/2026	3/15/2026	3/30/2026	4/15/2026

https://www.ncyte.net/academia/institutions/centers-of-academic-excellence/cae-cd-resources

Contact Information

CAE Program Office:

- Caepmo_uwe@uwe.nsa.gov
- Angie Painter Arpaint@uwe.nsa.gov

CCNC Director:

- Stephen Troupe STroupe@whatcom.edu

CCNC Project Managers:

- Emma Graves Egraves@whatcom.edu
- Michael Singletary MSingletary@whatcom.edu

PCNC Director:

- Stephen Miller SMiller@whatcom.edu

Checklist Coordinator:

- Joel Hutchins Joel.Hutchins@enmu.edu

CyberAI KU/Community of Practice:

- Dr. Sidd Kaza skaza@towson.edu
- Dr. Blair Taylor btaylor@towson.edu