National Centers of Academic Excellence IN CYBERSECURITY

INITIATIVE GUIDE 2021

Introduction

Program Management Organizations

Cybersecurity Education Initiatives

Appendix

Introduction

NCAE-C FY2020 Initiatives Points of Contact Quick Reference

Initiative Title	Lead Institution(s)	Point of Contact	Email
CAE National Center: CAE Community Technical, logistic support Portal of Resources Strategic initiatives	California State University, San Bernardino (CSUSB)	Dr. Tony Coulson	tcoulson@csusb.edu
CAE Community of Practice – CD NICE Challenge	Nova Southeastern University	Yair Levy	levyy@nova.edu
CAE Community of Practice – CO	Mississippi State University	Dr. Drew Hamilton	hamilton@cci.msstate.edu
CAE Community of Practice – R INSuRE	Northeastern University	Dr. Agnes Chan	Ag.Chan@northeastern.edu
	Stevens Institute of Technology	Dr. Susanne Wetzel	swetzel@stevens.edu
CAE-C Regional Hub Southeast	University of West Florida	Dr. Eman El-Sheikh	eelsheikh@uwf.edu
CAE-C Regional Hub Northeast	Capitol Technology University	Dr. William Butler	whbutler@captech.edu
CAE-C Regional Hub Southwest	San Antonio College	Kim Muschalek	kmuschalek@alamo.edu
CAE-C Regional Hub Northwest	University of Colorado Colorado Springs	Gretchen Bliss	gbliss@uccs.edu
CAE-C Regional Hub Midwest	Moraine Valley Community College	Dr. John Sands	sands@morainevalley.edu
CAE National Center: Candidates Program	Whatcom College	Corrinne Sande	csande@whatcom.ctc.edu
CAE National Center: Peer Review	Northern Virginia Community College	Dr. Margaret Leary	nvlearm@nvcc.edu
Consolidated CAE-C Professional Development Resources	Montreat College	Kelli Burgin	kelli.burgin@montreat.edu
Cybersecurity Education Diversity Initiative (CEDI)	Fordham University	Dr. Thaier Hayadneh	thayajneh@fordham.edu
	Excelsior College	Dr. Amelia Estwick	AEstwick@excelsior.edu

Initiative Title	Lead Institution(s)	Point of Contact	Email
Evidencing Competency	Norwich University	Dr. Karen Hinkle	hinkle@norwich.edu
Faculty Professional Development	University of Colorado Colorado Springs	Dr. Gurvirender Tejay	gtejay@uccs.edu
	Dakota State University	Dr. Wayne Pauli	wayne.pauli@dsu.edu
National NCAE-C Competitions Program	Mohawk Valley Community College	Jake Mihevc	jmihevc@mvcc.edu
	University of South Florida	Dr. Ron Sanders	rpsanders@usf.edu
NCAE-C K12 Pipeline	Moraine Valley Community College	Dr. John Sands	sands@morainevalley.edu
	The University of Alabama in Huntsville	Dr. Tommy Morris	tommy.morris@uah.edu
Senior Military Academy Cyber Institutes	Norwich University	Dr. Sharon Hamilton	shamilto@norwich.edu
Workforce Development Pilot Midwest	Purdue University Northwest	Dr. Michael Tu	Michael.Tu@pnw.edu
Workforce Development Pilot Southeast	University of Louisville	Dr. Sharon Kerrick	sharon.kerrick@louisville.edu
Workforce Development Pilot Southwest	University of West Florida, Center for Cybersecurity	Dr. Eman El-Sheikh	eelsheikh@uwf.edu

NCAE-C Program Office Contact Information

Phone: (410) 854-6206
Email: caepmo@nsa.gov
More Information: www.iad/gov/nietp

NCAE-C Program Office Introduction

This guide to the National Centers of Academic Excellence in Cybersecurity (NCAE-C) grants initiatives provides a summary of the programs and initiatives made possible by Congressional funding add-ons provided in FY2020. The NCAE-C program has long cultivated K12 outreach, faculty professional development, cybersecurity research, and other academic programs. For the first time this year, participating schools were asked to form coalitions and partnerships around specific initiative topics. As a result, there is an unprecedented excitement and energy in the CAE-C Community, undertaking challenging and innovative programs to support cybersecurity education across the nation. Federal partners and CAE-C academic institutions are invited to contact program managers and initiative leads provided in this document in the interest of collaboration and reductions of duplications of effort.

NSA is honored to partner with four primary federal organizations that are leaders in the cybersecurity education area.

Cybersecurity and Infrastructure Security Agency (CISA), part of the Department of Homeland Security) has long partnered with NSA to sponsor the NCAE-C program. CISA offers a wealth of resources and leadership to the cybersecurity education community, and national authorities in Homeland Security that complement NSA's national authorities to provide support and collaboration to the nation's academic institutions. Visit the National Initiative For Cybersecurity Careers and Studies (NICCS) at https://niccs.us-cert.gov/ for more information.

The Federal Bureau of Investigation (FBI) joined the NCAE-C partnership two years ago to sponsor the Cyber Operations program. FBI brings expertise and resources to the partnership in the form of instructors on a wide range of topics and professional experience and is active in the CAE-CO Summer Program.

The National Initiative for Cybersecurity Education (NICE), a Department of Commerce organization, has been a close partner since its inception. NICE has sponsored the annual CAE Community Symposium in concert with the annual NICE Conference, and the programs collaborate closely on the NICE Cybersecurity Workforce Framework (NCWF). The NCAE-C academic requirements map directly to the NCWF, and NCAE-C competency-based education initiatives tie directly to the NCWF work roles and NICE plans to add competencies to NCWF.

The National Science Foundation (NSF) cybersecurity education programs are closely aligned with the CAE-C program. NSF has funded several grants at CAE-C academic institutions that directly support the program; a mentoring initiative started by NSF provided the foundation for the NCAE-C Candidates Program, which mentors newly participating schools during their application preparation. Most of the institutions receiving CyberCorps® scholarships are designated in the NCAE-C program.

In addition to the initiatives described in this Guide, the NCAE-C program office issued two types of research grants in FY2020. Research grants were awarded to Minority Serving Institutions (MSIs) as part of Congressional funding specifically targeted to support diversity; grants were also awarded to schools holding the CAE-R designation.

The NCAE-C program collaborates with other Federal partners as the opportunities arise. Most recently, a group of CAE-C schools worked with the Department of Education on a three-year Career Technical Education project for high schools across the nation.

At the completion of the 2020 application cycle in November 2020, there are 335 designated NCAE-C institutions. Contact the NCAE-C program office by email at caepmo@nsa.gov, or get more information at www.iad/gov/nietp or www.caecommunity.org.

We sincerely appreciate the support from Congressional representatives, our Federal department and agency partners, and the commitment and expertise demonstrated by participating academic institutions.

Program Management Organizations

CAE in Cybersecurity Community National Center

The CAE in Cybersecurity (CAE-C) Community National Center grant is administered through California State University, San Bernardino (CSUSB). Focused on the development of a robust cybersecurity workforce, the CAE-C Community National Center will offer three primary functions to the 335+ CAE-C institutions and projects:

1. Provide technical and logistical support for CAE events, activities, and curriculum

2. Provide a portal of CAE resources for the community, geographic regions, and the Nation as a whole

3. Engage and facilitate strategic initiatives for the Nation in the areas of research, student and faculty development, diversity, and other workforce development activities

Components

The CAE-C Community National Center will directly fund and support five geographic areas known as CAE-C Regional Hubs (CRHs) to coordinate and expand cybersecurity workforce initiatives throughout the country. The CRHs are detailed as follows:

- Northeast Regional Hub: consortium of Capitol Technology University, Mohawk Valley Community College, and Towson University

- Southeast Regional Hub: consortium of the University of West Florida, University of South Florida–Cyber Florida, and Forsyth Technical Community College

- Midwest Regional Hub: Moraine Valley Community College

- Northwest Regional Hub: University of Colorado Colorado Springs

- Southwest Regional Hub: San Antonio College

The complexity of a cybersecurity workforce requires an ever-changing range of skills. The CAE-C Community National Center will also directly support three CAE-C Communities of Practice, focusing efforts on research (CAE-R), cyber defense (CAE-CD), and cyber operations (CAE-CO). Each of these workforce and educational areas require specific competencies and skills and the goal of these communities of practice is to engage industry, academia, and government to help set a strategic direction for academia. Two major elements of the communities of practice include the INSuRE (Information Security Research and Education) Project and the NICE Challenge Project. INSuRE focuses on student research teams working with technical directors from government and national labs on real-world cybersecurity research problems. The NICE Challenge

Project is a national educational cyber range designed around the NIST 800-181 cybersecurity workforce education framework. It is currently used by more than 450 colleges and universities.

The CAE-C Community National Center will partner in research, including a cybersecurity post-secondary education resource directory and feasibility study to create a high school Centers of Academic Excellence Program.

POC(s): Dr. Tony Coulson
Email: tcoulson@csusb.edu
More Information: www.caecommunity.org

CAE Candidates Program National Center (CNC)

The CAE Candidates National Center acts as the entry point for all colleges and universities that plan to apply for either Academic Validation or NCAE-C Designation. The CNC provides mentoring, resources, advice, and other support to colleges and universities that want to earn the NCAE designation, or to have their academic program validated as a first step in the process. Candidate institutions must have their mentor's endorsement to apply for designation. Because Whatcom College also plays a lead role in the National Science Foundation's (NSF) Advanced Technical Education (ATE) National Center, known as the National Cybersecurity Training & Education Center (NCyTE), applicants benefit from both NCAE-C program and NCyTE resources and expertise. The project's ultimate goal is to improve and expand cybersecurity education nationwide to meet the workforce needs of the nation.

Lead Institution: Whatcom Community College
POC(s): Corrinne Sande
Phone(s): (360) 383-3552
Email: csande@whatcom.edu
More Information: https://ncyte.net/cae-program, https://www.caecommunity.org/ogcnrccrrc/cnrc-candidates-program

CAE Peer Review National Center (CNC)

The CAE Peer Review National Center works with the NCAE-C Program Management Office to train reviewers and execute peer reviews of applications for Academic Endorsement and/or NCAE-C Designation. Northern Virginia Community College and Whatcom College collaborate to manage peer review panels based on readiness of Candidates to submit applications or Designated institutions to apply for re-designation.

Lead Institution: Northern Virginia Community College
POC(s): Margaret Leary
Phone(s): (703) 582-2720
Email: mleary@nvcc.edu
More Information: www.nvcc.edu/Cybersecurity

Cybersecurity Education Diversity Initiative (CEDI)

The co-chairs of CEDI understand the diff i culty of creating a full-f l edged cybersecurity program from scratch at MSIs. Each institution will adopt these courses at different speeds, and even programs that are rolled out rapidly might not be quick enough to enroll all interested students before they graduate. The best way to alleviate these concerns is by having sub-awardees develop credit transfer agreements with their chosen MSIs, so students can take courses already taught at the sub-awardee university and graduate from their current institution, while achieving a minor or certificate in cybersecurity. There will be no need for significant overhauls in the cybersecurity curriculum at the school, nor any reason to develop new courses — agreeing on a credit-transfer process will easily enhance the cybersecurity education at the MSI. One innovative transfer agreement is seen in Bluegrass Community and Technical College (BCTC), where they will offer college-level credit for high school students. Before joining the coalition, BCTC already had a great relationship with two high schools serving a predominantly African American neighborhood in Lexington, KY, and developed a rapport with Kentucky State University, the only MSI in Kentucky. Their credit transfer program will be a three-way agreement between themselves, Kentucky State University, and the high schools. If this is successful, high school students will get an early start on taking cybersecurity classes from the NCAE-designated Bluegrass Community & Technical College, and after completing a two-year program there, will move on to earn a bachelor's degree at Kentucky State University.

CEDI will share existing courses with MSIs, rather than developing new ones. Leadership at CEDI will oversee the creation of a Shared Knowledge Cybersecurity Education Initiatives Center, which will be the major library from which MSIs can pull the resources produced by the CEDI coalition. This facilitates collaboration from universities around the country and allows MSIs to easily download new courses, video lectures, and labs for their own programs. In addition to creating a CEDI-exclusive shared resource center, the PI will also pull courses from the CLARK library, so MSIs can integrate lessons that are created and currently taught at NCAE designated universities.

Sharing courses from existing cybersecurity programs is just half of the solution—students at MSIs will need professors with the cybersecurity skills to effectively teach these lessons. This can either be accomplished by creating bootcamps where faculty from MSIs can learn how to implement labs they will teach in courses, or by sending faculty from sub-awardee institutions to MSIs as guest lecturers or online instructors. These two options have unique benefits. By training faculty at MSIs to teach courses, the knowledge gained after the bootcamp is retained and kept inside the MSI for as long as the professor is there. This ensures a long-term impact at that institution.

Lead Institution: Fordham University
POC(s): Dr. Thaier Hayajneh
Email: thayajneh@fordham.edu
Co-Lead Institution: Excelsior College
POC(s): Dr. Amelia Estwick
Email: aestwick@excelsior.edu

Coalition Partners

1

Partner Institution: Polytechnic University of Puerto Rico
POC(s): Contact Initiative Leads

Initiative Description

The Center for Information Assurance for Research and Education and Polytechnic University in Puerto Rico (PUPR) will support cybersecurity education for faculty in both universities and community colleges, K12 educators, and students in graduate-level programs or servicemen/servicewomen. The center will support up to 15 people in completing a certificate, either for Secure IT Operation Management or Digital Evidence and Auditing. They will develop Capture the Flag (CTF) teams at other universities in Puerto Rico by hosting workshops at PUPR that provide training to students and faculty. Their proposal is an annual cybersecurity conference to promote cybersecurity education at local institutions in Puerto Rico.

2

Partner Institution: Metropolitan State University of Denver
POC(s): Contact Initiative Leads

Initiative Description

One of the goals of this sub-award is to encourage directors of cybersecurity programs at schools to reach out and ask for mentoring from NCAE-designated programs. The proposal to address this situation is creating a Mountain West Cybersecurity Consortium ,which will be a working group that CAE and non-CAE schools in the region can join. Another goal is to facilitate the creation of transfer agreements so students at 2-year institutions can transfer to 4-year institutions that have cybersecurity programs. Dr. London proposes to collaborate with the Colorado Department of Higher Education to collect census data from these schools to map the locations of publicly-funded institutions with cybersecurity programs and count the number of students enrolled in those programs.

.

3

Partner Institution: Bluegrass Community and Technical College
POC(s): Contact Initiative Leads

Initiative Description

This proposal seeks to expand the BCTC Informatics Academy to include cybersecurity courses to high schools and formulate a transfer agreement between BCTC and Kentucky State University. Their first task is to form a working group among faculty members, who coordinate the information technology courses as minority high schools and the faculty for Computer Science at Kentucky State University, to solicit involvement in the project. Next, they propose to expand the Informatics Academy course selection, to include cybersecurity lessons that will count toward college credit and double the number of enrollment spots in that program from 20 to 40. The final goal of the proposal is to design a 2+2 articulation agreement, so students completing an associate degree in Cybersecurity at BCTC can transfer to KSU and finish with a bachelor's degree.

4

Partner Institution: North Carolina Agricultural & Technical State University
POC(s): Initiative Leads

Initiative Description

NC A&T will share cybersecurity course materials with MSIs. In order to train educators to effectively teach their courses, NC A&T will host webinars and workshops, during which they will run through labs and learn good ways to integrate them into their own curriculum. For those institutions lacking computer facilities for labs, NC A&T will create virtual machines on their own servers. Students can also engage in the Capture the Flag events involving college, middle school, and high school students, which are normally hosted at the university.

5

Partner Institution: New Jersey City University
POC(s): Initiative Leads

The first goal is to provide consultation and course plans so HBCUs and MSIs can begin with introductory cybersecurity courses covering topics such as: automated information systems, security policies, and system operating environments. They have already identified four institutions with whom they will start the advising process: Essex County College, Mercer County Community College, Bergen Community College, and Hudson County Community College. The second goal is creating a beginner-level cybersecurity training workshop that will be taught at those four institutions by the PI and co-PI. After completing this workshop, participants will receive a certificate of attendance. Their third goal is creating a summer bootcamp, inviting 15 students from each of the colleges to practice hands-on lab exercises.

6

Partner Institution: University of North Florida
POC(s): Initiative Leads

Initiative Description

UNF is proposing four activities to develop a comprehensive cybersecurity partnership with Edward Waters College, a local MSI. The first goal is to establish a credit-transfer agreement with EWC, so that the course proposed by UNF will count toward a cybersecurity certificate. The PIs will assist EWC with creating a course schedule and the infrastructure for online teaching. A second goal is to share cybersecurity curriculum with faculty at EWC. There will be a five-day workshop hosted at UNF, during which faculty members can attend for a walk-through on cutting-edge, hands-on lab exercises, covering a wide range of technical topics in cybersecurity. The third goal is creating a pathway for students at the MSIs to participate in club meetings at UNF's student-led cybersecurity club. The fourth goal is to develop workshop for students, which will be jointly hosted by UNF and Florida State College.

7

Partner Institution: University of Tennessee at Chattanooga
POC(s): Initiative Leads

Initiative Description

The University of Tennessee at Chattanooga (UTC) proposes to offer online cybersecurity faculty development workshops for MSIs. The summer bootcamp, directed by the co-PI of their proposal, has nearly a 50% participation rate from women and minorities, and of the 22 organizations that have participated so far, seven are HBCUs. The proposal from UTC will provide a cloud-based cybersecurity training workshop three times a year for two years with a capacity of 20 instructors from MSIs for each workshop. Each workshop will span over a five-week period with five days total of instruction time, happening on the weekends. The PIs at UTC will cover subjects on Linux Scripting, Cloud Networking, Machine Learning, Network Security, and Applied Cryptography; many of these training materials were developed at UTC from NSF and NSA grants and shared through the CLARK library.

8

Partner Institution: University of North Texas
POC(s): Initiative Leads

Initiative Description

This proposal has a three-step pathway for cybersecurity education, leading to a potential NCAE program designation at MSIs. Firstly, they will inspire students and grow interest in Cybersecurity by hosting Capture the Flag and Digital Forensics Scavenger Hunt competitions at UNT. Their second goal is to build an internship readiness tool that automates the mapping of job descriptions to Knowledge Units that courses at UNT cover. This is an ambitious project, that if successful, will

allow instructors at universities to see how their courses prepare students for a specific job role, for example, according to the work role data set in the NICE Framework. The third goal is to develop bridge courses that will be offered to MSIs without a cyberserecurity program, so that students can either complete a certificate program or transfer to a four-year institution. UNT has identified four colleges in the Dallas County Community College District and is already discussing articulation agreements with them: El Centro College, Cedar Valley College, Del Mar College, and Odessa College.

7

POC(s): Initiative Leads
Partner Institution: Tennessee Tech University

Initiative Description

Tennessee Tech will provide five different services to the students and faculty of MSIs as a member of the CEDI Coalition. These are: Expanding hands-on skill opportunities for MSI students by developing and orchestrating 24-hour Capture the Flag (CTF) competitions where the students can remotely participate to gain technical skills in cyber; integrating security into computer science curriculum training for MSI faculty by providing faculty training workshops and free instructional materials to bring security topics and exercises into their classroom teaching; expanding awareness, knowledge, and skill training opportunities for MSI students by facilitating and programming their remote participation in two cybersecurity clubs and helping them to create and sustain such student organizations for their schools; NCAE designation guidance to MSI faculty by providing virtual advisement sessions to discuss considerations and issues related to applying for NCAE-C designations.

Other CEDI Partner Institutions

There are 40 faculty teaching in cybersecurity programs, who are also part of the MSI working group and they have all expressed interest in joining as consultants are independent contractors:

- American Public University System
- Athens State University
- Baker College
- Carnegie-Melon University
- Florida A&M University
- Harford Community College
- Henry Ford College
- Houston Community College
- Indiana University
- KY Community and Tech College System
- Lamar Institute of Technology
- LeMoyne-Owen College
- Lewis University
- Metropolitan State University of Denver
- National University
- New Jersey City University
- New York Institute of Technology
- New York University
- Norfolk State University
- North Carolina A&T State University
- Old Dominion University
- Polytechnic University of Puerto Rico
- Simmons College
- South Carolina State University
- St. Bonaventure University
- St. Cloud State University
- St. Petersburg College
- SUNY Rockland
- Talladega College
- Tennessee Tech University
- Tuskegee University
- University of Arizona
- University of Denver
- University of Maryland Global Campus
- University of Nevada Las Vegas
- University of Tennessee at Chattanooga
- University of Texas at El Paso
- University of Texas at San Antonio
- Webster University

CAE-C Competition Program

The CAE National Competition project aims to increase student and faculty engagement with cybersecurity competitions through an intuitive sequence of tools, tutorials, and activities that simplify and focus preparation activities within student clubs. The project will provide students with a positive initial experience with cybersecurity competition that leads them to further engagement within the cybersecurity competition landscape. A practice environment will be available in the spring of 2021, regional competitions will commence in the fall of 2021, and the finals will be held at the end of the spring 2022. CAE faculty and industry partners will be encouraged to submit content and challenges for the competitions to ensure the competitions reflect the broad scope of knowledge and subject matter expertise within the CAE Community.

Lead Institution: Mohawk Valley Community College
POC(s): Jake Mihevc
Phone(s): (315) 792-5653
Email: jmihevc@mvcc.edu
Co-Lead: University of South Florida-Cyber Florida
POC(s): Ron Sanders
Phone(s): (703) 819-4893
Email: rpsanders@usf.edu

Evidencing Competency Oversight

Norwich University will lead the Evidencing Competency Oversight Project, in support of the NCAE-C Program. In support of this effort are California State University, San Bernardino, Stevens Institute, and 32 faculty from 28 CAE-C institutions. The project is comprised of three simultaneous efforts:

- Regional Cybersecurity Exercises – Norwich will design, develop, and implement 10 cybersecurity exercises for CAEs located within the 10 FEMA Regions. These exercises will enhance students' skills and abilities in risk resiliency by providing an opportunity to exercise on a broad range of threats, while strengthening their knowledge about incident response plans and crisis communications.

- Security Situation Center for Evidencing Competency – The goal of the security situation center activity is to create a comprehensive resource for CAE-C institutions to replicate the model at their home institutions. The objectives are:

    - Identify CAE-C community members employing "live" environments for educational purpose, collect information on operations, architecture, and operating models

    - Define tools and training requirements for Work Roles

    - Map Work Roles to Tasks for each role and define appropriate "evidencing competency" demonstration

    - Assemble concept of operations document for CAE-C institutions to replicate Norwich Security Situation Center

    - Produce final report of results and future opportunities

- Evidencing Competency Working Group – The evidencing competency group has been in existence for two years. The working group has grown to approximately 60 individuals, mostly from academia, but includes some government and industry participants. It is broken into three sub-working groups with the following purposes:

- Sub-Working Group 1: Definitions and Documentation
- Sub-Working Group 2: Competency Development and Measurement Tools(s)
- Sub-Working Group 3: Cybersecurity Competitions as Competency Development and/or Evaluation Tools

The Evidencing Competency Working Group has agreed on the working definition of competency: Competency is the ability for students to complete tasks in the context of a work role. The definition is one that can be easily understood and implemented by faculty without the need to adopt new terminology or taxonomies. It is also a definition that can be easily understood and accepted by industry and hiring managers. Over the next two years the working group will follow a process to create and socialize a framework for evidencing competency that can be implemented through the NCAE-C program. The activities will also tie together a comprehensive review of the marketplace of cybersecurity measurement and tools and cyber competitions.

Lead Institution: Norwich University
POC(s): Dr. Sharon Hamilton
Phone(s): (802) 485-2411 (office); (717) 226-0237 (cell)
Email: shamilto@norwich.edu

1

Partner Institution: California State University, San Bernardino
POC(s): Dr. Vincent Nestler
Phone(s): (909) 537-5117
Email: vnestler@csusb.edu

Initiative Description
Sub-Working Group 1 will define the framework, definitions, and terminology for evidencing competency in CAE-C approved programs.

2

Partner Institution: Stevens Institute of Technology
POC(s): Dr. Susanne Wetz*el*
Phone(s): (201) 216-5610
Email: swetzel@stevens.edu

Initiative Description
Sub-Working Group 2 will explore cybersecurity skills assessment tools, develop the rubric to evaluate each tool, provide a list of the tools and the evaluation results for each, and share the working group's evaluation results with other NCAE-designated institutions.

3

Partner Institution: Expert consultant
POC(s): Dr. Daniel Manson (Professor Emeritus, Cal Poly Pomona)
Phone(s): (909) 455-2403
Email: dmanson@cpp.edu

Initiative Description
Sub-working Group 3 will identify and explore student cybersecurity competitions. It will identify established cybersecurity competitions that provide students with development of measurable competencies and document the competencies developed during competition.

Cybersecurity Faculty Development, Phase 2: Expanding Supply in Response to Demand – A National Focus

Dakota State University (DSU) and University of Colorado Colorado Springs (UCCS) as Lead Institutions in their respective projects have agreed to work together and coordinate grant-related activities: A unified Faculty Development program brand under the CAE-C Community banner, with 20 participating institutions.

Co-Lead Institution: Dakota State University
POC(s): Dr. Wayne E Pauli
Email: wayne.pauli@dsu.edu

Initiative Description

There is a critical shortage of cybersecurity professionals available to teach and perform faculty duties in cybersecurity. The institutional-directed projects have been designed with special attention to scaling nationwide. The objectives are:

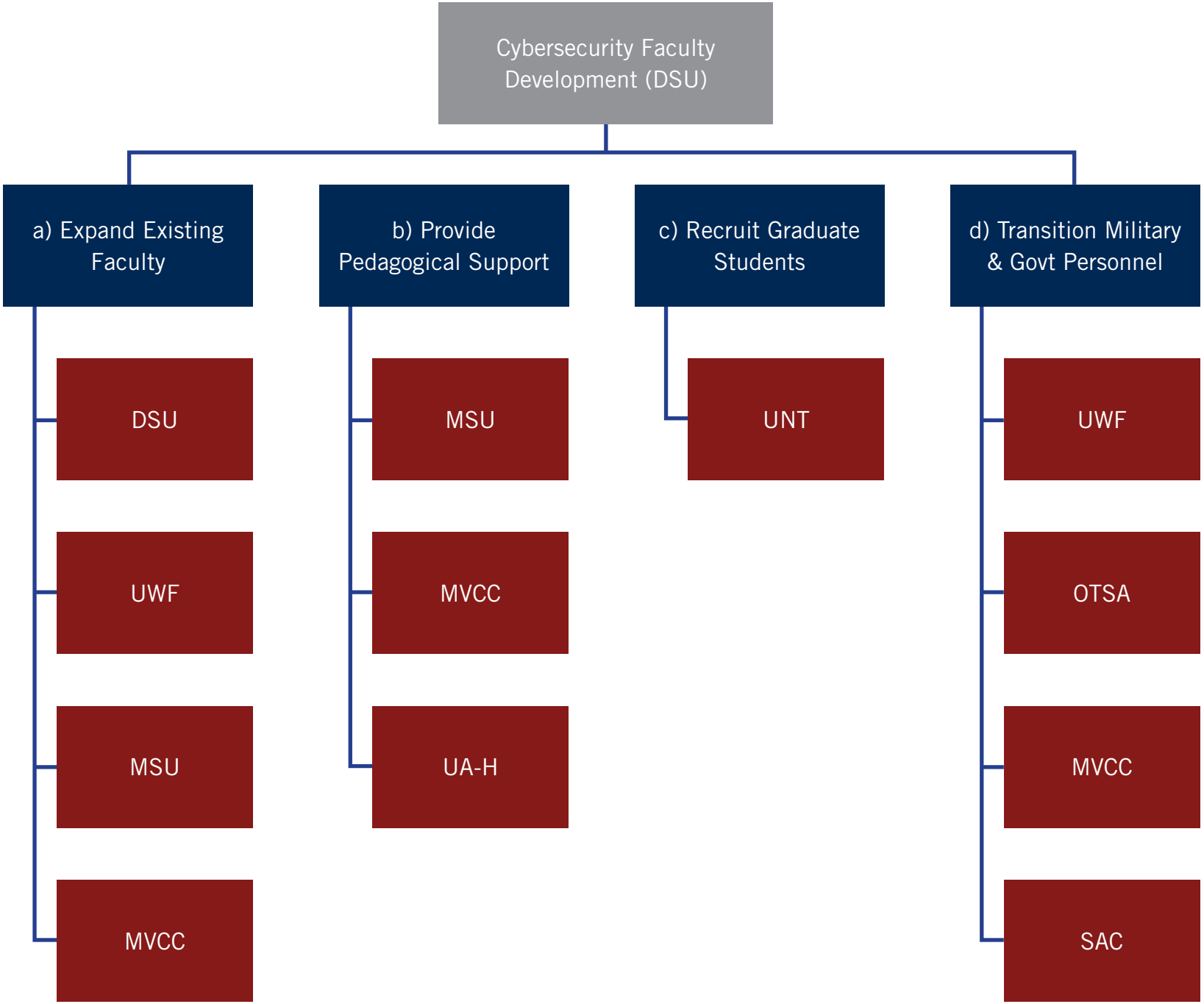
A. **Expanding the knowledge and teaching qualifications of existing faculty.** Programs will enable current cybersecurity faculty to expand on the programs already offered at designated and candidate CAE-C institutions.

B. **Recruiting and pedagogical preparation for professors of practice.** Faculty may propose a program engaging partnerships with government and industry employers, taking professionals in the field of cybersecurity, providing them with an understanding of pedagogy required in college education, and placing them in classrooms as adjunct or guest lecturers.

C. **Recruiting graduate students, particularly PhD candidates, to teach in cybersecurity.** Programs that engage graduate students to inspire and prepare them to teach in cybersecurity.

D. **Recruiting transitioning military and civil service personnel from government cybersecurity work roles.** Participants in either of these ventures will commit to teaching at an NCAE-designated or candidate institution for a specified period of time, based on investment.

Institution Name	POC Name	POC Email
Metropolitan State University – St Paul MN	Dr. Faisal Kaleem	Faisal.kaleem@metrostate.edu
University of West Florida – Pensacola FL	Dr. Tirthankar Ghosh	tghosh@uwf.edu
University of Texas at San Antonio – Texas	Dr. Glenn Dietrich	Glenn.dietrich@utsa.edu
Moraine Valley CC – Palos Hills IL	Dr. John Sands	sands@morainevalley.edu
San Antonio College – San Antonio TX	Kim Muschalek	kmuschalek@alamo.edu
Dakota State University – Madison SD	Dr. Kyle Cronin	Kyle.cronin@dsu.edu
University of North Texas – Denton TX	Dr. Ram Dantu	Ram.dantu@unt.edu
University of Alabama in Huntsville – AL	Dr. Tommy Morris	Tommy.morris@uah.edu


Cybersecurity Faculty Development (DSU)
a) Expand Existing Faculty
b) Provide Pedagogical Support
c) Recruit Graduate Students
d) Transition Military & Govt Personnel
DSU
UWF
MSU
MVCC
MSU
MVCC
UA-H
UNT
UWF
OTSA
MVCC
SAC

Coalition Partners

1

Partner Institution: Metropolitan State University (MSU)
St. Paul, MN
POC(s): Faisal Kaleem
Email: faisal.kaleem@metrostate.edu

Initiative Description
Minnesota Cyber Range and SOC Workshops – Provide a professional development opportunity for existing cybersecurity faculty from colleges and universities and expose them to the conceptual and practical details of Advanced Incident Response and Handling, leveraging MN Cyber Range and other open source platforms and tools.

Pedagogical Preparation for Industry Cyber Experts – To recruit interested cybersecurity subject matter expert from the industry leveraging the MN Cyber Institute's partner network and other organizations across the nation.

2

Partner Institution: University of West Florida (UWF)
Pensacola, FL
POC(s): Tirthankar Ghosh
Email: tghosh@uwf.edu

Initiative Description
Scenario-based Teaching Workshops – The University of West Florida (UWF) will deliver faculty development opportunities to train existing cybersecurity faculty in relevant, current technologies and tools using scenario-based learning. This will be accomplished by offering workshops to existing university and college faculty to prepare them for scenario-based teaching and integrating scenarios into their curricula.

Veteran Recruitment Program – The University of West Florida (UWF) plans on recruiting veterans interested in teaching to upskill them with relevant pedagogical and technical expertise. This will be completed by establishing a recruitment program to identify veterans with appropriate experience and expertise, to provide them with relevant pedagogical/technical knowledge and skills to teach in designated and candidate CAE-C institutions.

3

Partner Institution: University of Texas at San Antonio (UTSA)
San Antonio, TX
POC(s): Glenn Dietrich
Email: glenn.dietrich@utsa.edu

Initiative Description
Recruiting Transitioning Military and Civil Service Personnel – This project will recruit military and civilian personnel retiring from their current employment to have a career teaching cybersecurity in an academic institution. The project will also concentrate on current employees who want to work in academia on a part-time basis. Discussions with the major cybersecurity commands will be integral to the process. Advertisements will be laced in base/post newspapers, concerning the benefits and shortages in academia.

4

Partner Institution: Moraine Valley Community College (MVCC)
Palos Hills, IL
POC(s): John Sands
Email: sands@morainevalley.edu

Initiative Description
Industry Certification Train-the-Trainer Workshops – The National CSSIA Teaching and Learning Academy (Train-the-Trainer) will provide 10

workshops over the grant period. These workshops will serve 15-20 faculty members each. Each workshop will be aligned to recognized industry credentials, emerging technologies, and popular products. Courses will include CISSP, CISA, CEH, Security+, CCNA Security Operations, Palo Alto Security Fundamentals, and Linux Professional Institute. Other workshops might include VMware, EMC, and Meraki.

Pedagogical Support via the National Academy – The CSSIA team has a long and successful history of providing pedagogical support systems through the National Academy. Pedagogical support systems for each course includes instructional best practices, suggested content, and activities and assessment tools. Instructors also receive mentoring support once they complete CSSIA workshops. In addition, the CSSIA support model includes an online curriculum library with packaged content, rubrics and assessment tools, access to the virtual teaching and learning environment, and mentoring from the CSSIA train-the-trainer team members.

5

Partner Institution: San Antonio College (SAC) San Antonio, TX
POC(s): Kim Muschalek
Email: kmuschalek@alamo.edu

Initiative Description

SAC will prepare at least 25 existing cybersecurity faculty to obtain Department of Defense-recognized IT industry certifications — with a focus on "Security+" — to prepare them for leading their institution's NCAE designation. SAC will identify at least 10 veterans or active duty military members who are employed in cybersecurity roles in government agencies nationwide and who have an interest in teaching cybersecurity. Over the next two years, SAC will help transition at least five of these individuals (50%) to adjunct or tenured positions at current or prospective CAE schools across the U.S., by providing pedagogical assistance to prepare them for the classroom and by providing financial support and linkages to NCAE-designated university programs to ensure they have the proper credentials to teach postsecondary cybersecurity courses.

6

Partner Institution: Dakota State University (DSU) Madison, SD
POC(s): Kyle Cronin
Email: kyle.cronin@dsu.edu

Initiative Description

Workshops will have five separate topics for attendees to select from, based on the survey results from the community. Each workshop will have five separate topics, hosting 30 CAE faculty each, totaling 150 participants per workshop. Each workshop will be organized into 12 in-person contact hours, organized over two or three days, depending on the location and venue. Two instructional staff will lead each group of 30 participants through the exercise and provide content they can directly import into their current classrooms. Participants will be provided with lessons, lecture notes, hands-on exercises, and be given a hands-on tutorial on how to setup and execute each lesson.

7

Partner Institution: University of North Texas (UNT) Denton, TX
POC(s): Ram Dantu
Email: ram.dantu@unt.edu

Initiative Description

Recruitment of graduate students toward expanding faculty numbers in Cyber–UNT plans to address a wide variety of thirteen novel activities to deal with the critical shortage of cybersecurity professionals in academia in the areas of preparing Professors of Practice and training of PhD students. There will be a sequence of mentoring and training readiness activities for industry professionals and PhD students aimed at producing

well-qualified faculty capable of not only teaching, but inspiring and engaging the next generation of cybersecurity professionals.

8

Partner Institution: University of Alabama in Huntsville (UAH)
Huntsville, AL
POC(s): Tommy Morris
Email: tommy.morris@uah.edu

Initiative Description
Concurrently Teaching Faculty and Students SCADA Security with Massive Online Academy – This proposal offers to teach for credit online SCADA cybersecurity classes to audiences of students and faculty at UAH and university partners. Class enrollment across all participating universities will be capped at 500 participants.

Co-Lead Institution: University of Colorado Colorado Springs
POC(s): Dr. Gurvirender Tejay
Phone(s): (719) 255-3186
Email: gtejay@uccs.edu

Initiative Description
UCCS will serve as the lead institution for a consortium of educational institutions delivering a comprehensive, programmatic approach to cybersecurity faculty development. We will provide cybersecurity education and training to over 1,700 participants for faculty roles, including existing faculty, professors of practice, doctoral candidates, and transitioning military and civil services personnel. Our partnership of academic institutions includes 10 prominent participants in cybersecurity instruction, to include community colleges up to major research universities. The program will offer certificates in narrow cybersecurity topics, masters and doctoral degrees in cybersecurity and cybersecurity management, boot camps in cybersecurity technology, and courses and pedagogy to fill specific knowledge gaps. Grant funds provide free instructions for some programs and scholarship assistance for the deeper programs.

A. **Expanding the knowledge and teaching qualifications of existing faculty (Train 1,335 faculty; 100 institutions for degrees)**

For existing faculty with a terminal degree, we will offer free cybersecurity teaching workshops and hybrid courses. In collaboration with our partner institutions, we plan to collectively recruit and train 1,335 existing faculty through cybersecurity teaching workshops, hybrid courses, bootcamps on tools/techniques, industry certifications, and program development workshops. Additionally, we are partnering with Cybersecurity Management Council to engage 100 institutions, helping them develop cybersecurity management degree programs. We will provide a program toolkit, course toolkits, pedagogical resources, online resources on certifications, and mentorship to 300 faculty.

B. **Recruiting and pedagogical preparation for professors of practice (Train 200 participants)**

The UCCS-proposed program is focused on recruiting industry experts to participate in a Professors of Practice program and will engage partnerships with government and industry employers. We plan to recruit and train 200 Professors of Practice. Taking current professionals in the field of cybersecurity, providing them with an understanding of pedagogy required in college education, and placing them in classrooms as full-time, adjunct faculty or guest lecturers can significantly increase the development and expansion of current cybersecurity programs in current and future CAE institutions.

UCCS plans to recruit industry cybersecurity experts with existing

credentials and/or a graduate degrees, and train them on pedagogy, curriculum development, and soft skill classroom dynamics. In addition to completing the education in pedagogical practices, the participants in this program will be offered a teaching practicum through the myriad of strategic partners in this faculty development grant, including universities and community colleges across the nation with specialties covering the depth and breadth of cybersecurity topics that fit their industry experience.

C. **Recruiting graduate students and PhD candidates to teach in cybersecurity (Train 250 students)**

We will train 250 graduate students and PhD candidates and provide cybersecurity scholarship opportunities, career guidance, and placement programs. The graduate and doctoral students will have access to pedagogical training to become effective educators and help them prepare for future careers in higher education teaching. The students can supplement their education by taking online graduate certificate programs listed in Table 1. Upon successful completion, the students will be prepared to teach cybersecurity courses at colleges and universities. The grant will provide up to a $5,000 scholarship award per student to pursue graduate certificates.

Institution	Graduate Certificate	Transfer Certificate credits to graduate degree	Pathway to PhD program
University of Colorado Colorado Springs	Network System Security	Yes	Yes
	Cybersecurity Management	Yes	Yes
Florida International University	Digital Forensics	Yes	Yes
University of New Mexico	Information Assurance	Yes	Yes
University of Cincinnati	Data-Driven Cybersecurity	Yes	Yes
University at Albany, SUNY	Information Security	Yes	Yes
Arizona State University	Emergency Management	Yes	No
National Cyberwatch Center	IT Foundations	No	No

Cybersecurity Capstone Field Trip. These 'live case study' educational field trips will allow students to experience the cybersecurity practice from a government, defense, or private sector vantage point. We will focus on Washington, D.C./Northern Virginia and Colorado Springs (Colorado) cybersecurity-focused ecosystems. These field trips offer a glimpse into the cybersecurity practitioners' day-to-day activities. Students will explore cybersecurity practices, career opportunities, visits to agencies, and interaction with subject matter experts.

Virtual Cybersecurity Teachers Program. This program will prepare graduate/doctoral students as teachers for online courses and place them to serve as teachers in high schools and community colleges. The proposed program will bring practical experience to the graduate programs, adding to the availability of qualified faculty in community college cybersecurity programs.

Cybersecurity Placement Program. This program will provide guidance on developing a successful application package, resources, webinars and mentorship to potential applicants.

Career Guidance. We plan to develop a Cybersecurity Educator career pathway to provide information on job roles, salary, required qualifications, and application process. We will provide information on various faculty roles at universities, colleges, community colleges, and high schools.

Cybersecurity Scholarships for Advanced Studies. The students interested in graduate or doctoral programs in cybersecurity may consider the CyberCorps® Scholarship for Service (SFS) program offered at our coalition institutions: UCCS, UNM, FIU, and ASU. This program provides scholarships for up to three years of support for cybersecurity undergraduate and graduate (MS or PhD) education.

D. **Recruiting transitioning military and civil service personnel from government cybersecurity work roles (Train 267 personnel)**

The military members with qualifications for adjunct or tenured positions will be provided with pedagogical training to become effective educators and help them prepare for future careers in higher education teaching. This program aims not only to obtain cybersecurity certifications for the military personnel interested in teaching in community colleges, but also gets them the needed depth of knowledge in educational pedagogical training to be able to teach at any level of cybersecurity educational program. The program will provide access to degree programs at CAE-C institutions, cybersecurity scholarship opportunities, pedagogical training and career guidance. Each coalition partner institution has committed to utilizing existing resources and programs at their institutions to recruit transitioning military and civil service personnel from government cybersecurity work roles.

"MOS Pathways." Designed to award credits based on military occupation, not based on specific training an individual received in the military. This can serve as an innovative approach to attract and recruit transitioning military personnel for cybersecurity faculty development. The military occupations are mapped to specific courses that also correspond in general to industry certifications.

Support Services. UCCS strives to provide transition assistance in the form of financial, social, and academic support for all Veterans, military service members and their families. These services include counseling referral, education benefits counseling, and transition/deployment assistance. Veterans, military service members, and their families will also have access to workshops on money matters, wellness resources including mental health screening, traumatic brain injury screening, and health and trauma clinic. Additionally, the participants will have access to Books for Battle Buddies program, Adaptive Leadership Certificate, and Boots to Suits program to gain a better understanding of civil work environments and reintegration into the workforce.

1

Partner Institution: Florida International University
POC(s): Contact Lead Institution

Initiative Description

The Digital Forensic program consists of two free workshops, four Digital Forensics courses and accompanying bootcamps to build fundamental knowledge and exposure to industry standard tools and techniques. The courses are to assist cybersecurity faculty in gaining expertise in the area of digital forensics, as a means to expand their capability in the area, leading toward expanded teaching and research. These four courses cover, to a great extent, the core topics necessary in formalizing a digital forensics program.

2

Partner Institution: University of New Mexico
POC(s): Contact Lead Institution

Initiative Description

We will provide two free online cybersecurity teaching courses and two hybrid bootcamps for faculty career development. In addition, we will provide scholarship support to graduate students, doctoral students, and military personnel without cybersecurity credentials to pursue Information Assurance Graduate Certificate. We plan to train 20 students during the grant period. Program details will be carefully tailored for transitioning military and civil service personnel and published in local newspapers, university journals, school website, and social media. On-campus ROTC unit will also be contacted for recruiting qualified candidates for enrolling in this program.

3

Partner Institution: Arizona State University
POC(s): Contact Lead Institution

Initiative Description

Arizona State University contributes to this initiative by offering faculty development and professional development opportunities in the specific area of emergency management and homeland security by examining their intersection with cybersecurity issues. Arizona State will lead two faculty development workshops covering the intersection of cybersecurity and emergency management in the United States and cybersecurity policy and management issues, as related to homeland security in the United States. Faculty participants in this initiative will also have access to two free courses in these same content areas. Finally, students will receive scholarship awards to enroll in a 15-credit hour graduate certificate in emergency management at Arizona State University; students with a military service affiliation transitioning to other careers will be a focus of recruitment for the emergency management certificate. Overall, this contribution is focused on supporting national needs to improve subject area knowledge, skills, and abilities for those who serve communities by preparing for, and responding to, cyber-related and other hazards risks.

4

Partner Institution: University at Albany, State University of New York (UAlbany)
POC(s): Contact Lead Institution

Initiative Description

UAlbany will be focused on training faculty and students in cybersecurity. As part of the project, UAlbany will develop curriculum for two separate courses (Digital Forensics and Information Security Risk and Policies). Each of the courses will be packaged with teaching materials, including, presentations, videos, assignments, and assessments. The courses will be taught for faculty looking to gain expertise in the areas and

there will be workshops to help transition course materials to faculty. Additionally, 30 students will be given $5,000 scholarships to complete their certificate program with a pathway towards an MS and PhD degree. The recruitment of students will be done through our recruitment channels at the university, as well as through our coalition partnership. Our goal is to have 20 percent transitioning armed forces personnel in the students recruited.

5

Partner Institution: University of Cincinnati
POC(s): Contact Lead Institution

Initiative Description

The proposed project is to create a series of connected education programs to recruit and train a diverse population, ranging from existing faculty, PhD students, military personnel and government IT professionals to teach cybersecurity curricula from entry-level technical courses to graduate-level, research-oriented courses. Two graduate certificates will be created to target instructors with different needs. First, an 18-credit-hour Graduate Certificate for Teachers and Instructors (GCTI) will prepare students to teach entry-level cybersecurity courses, such as system administration, network security, programming, and databases. The certificate is in Competence Based Education (CBE) format, consisting of 12 technical competencies, each equivalent to one graduate credit hour, and six teaching preparation competencies, through which students work with UC faculty members on a one-on-one basis to practice teaching in formal classroom settings. The second certificate is a Data Driven Cybersecurity (DDC) graduate certifi cate, consisting of four cybersecurity courses in UC's Master of Science in IT (MSIT) program. A DDC certificate will allow students to be specialized in Cybersecurity Data Analytics, which is the major theme at UC.

To further expand the impact of the project, UC will host two online courses through the project period to train faculty on selected DDC topics.

Participants of the workshop will learn how to collect and analyze a wide range of cybersecurity data from log files to malware binaries, using cutting edge programming or commercial software tools. The topics will be delivered in a MOOC modular format with fully developed lecture and demo videos, slide decks, assessment materials, and instructor manuals to facilitate participants quickly adopting and deploying these contents into their classes. Two one-week summer intensive bootcamps will be hosted online to accommodate learners with constraint time of study. The project is expected to train 110 participants nationwide.

6

Partner Institution: Robert Morris University
POC(s): Contact Lead Institution

Initiative Description

This initiative involves designing and teaching the workshop Pedagogy and Technology for Cybersecurity Teaching. This workshop will prepare cybersecurity professionals to teach and perform faculty duties in cybersecurity at the level of post-secondary education, with an emphasis in three areas: integration of technology, development and evaluation of cyber curriculum, and educational leadership. Participants will model a variety of active learning strategies (e.g., cooperative learning, case study, interactive lecturing, discussion, critical thinking, and role-playing) and will immerse themselves in thoughtful discussions addressing educational theory and practice.

7

Partner Institution: Whatcom Community College
POC(s): Contact Lead Institution

Initiative Description

We plan to provide faculty development workshops for colleges and universities that want to start a cybersecurity program or enhance an existing program with cybersecurity-related content. The workshops are for institutions that do not currently have a program that would qualify for "program validation" under the NCAE 2020 application. Workshop topics include program outcomes, the NICE Framework, CAE knowledge units, and obtaining funding.

This project also addresses mapping military occupation specialties (MOS) to credit at colleges and universities. Whatcom proposes expanding its MOS Pathways program to include universities. The MOS pathways program enables institutions to match military occupations to specific technical courses and provides a seamless way to award credit for prior learning to military veterans based on military occupation.

8

Partner Institution: Moraine Valley Community College
POC(s): Contact Lead Institution

Initiative Description

MVCC will provide faculty development workshops aligned to highly recognized industry credentials and emerging technologies. Course would include CISSP, CISA, CEH, Security+, CCNA Security Operations, Palo Alto Security Fundamentals, and Linux Professional Institute. Each course includes instructional best practices, suggested content and activities, and assessment tools. Participants will also be provided with industry certification exam preparation materials. These workshops provide institutions with the ability to increase and improve faculty knowledge, skills, and abilities. These workshops also provide an opportunity for faculty to earn industry-recognized cybersecurity credentials. Instructors are provided mentoring support after attending workshops. The support model includes an online curriculum library with packaged content, rubrics and assessment tools, access to the virtual teaching and learning environment, and mentoring.

9

Partner Institution: National CyberWatch Center
POC(s): Contact Lead Institution

Initiative Description

Educators represent an often overlooked but critical constituency missing from national discussions on cybersecurity workforce shortages. Higher education institutions need access to qualified instructors, as well as effective models for both building cybersecurity instructor capability and increasing their knowledge and skills beyond traditional faculty development offerings. Building on its 15 years of curriculum development expertise, faculty professional development offerings, and technical innovations in the delivery of both face-to-face and online hands-on cybersecurity courses and workshops, the National CyberWatch Center proposes the following: Conduct Train-the-Trainer workshops, employing a fully online delivery model. The workshop topics will provide the necessary IT foundation upon which existing faculty, traditional doctoral students, and transitioning military personnel can leverage to further increase their capability maturity in future cybersecurity course/workshop offerings delivered by other UCCS grant partners.

CAE K12 Pipeline Program: Regions Investing in the Next Generation (RING)

RING is a combined effort of two coalitions. The University of Alabama in Huntsville (UAH) and Moraine Valley Community College (MVCC), along with other partner universities and organizations, have combined efforts to establish a CAE K12 Pipeline. This effort will provide an online cybersecurity fundamentals course, which will target rural, under-resourced school systems; home school students; and schools without an established cybersecurity program.

The two coalitions have common marketing and administrative functions and administration that allows a universal insight into both efforts. This includes:

1. Shared project name with delineated responsibilities for each effort
2. Shared "Contact Us" account for email, phone, and social media housed at the national hub
3. Shared graphics designers for uniform look
4. Shared web page housed on the national hub's website
5. Common course application and registration through the national hub's website

While both teams will have distinct roles, they present a unified presence to schools, students, and partners. The UAH coalition leads curriculum development, instructs the online course for a national audience, and leads the student organization/honor society. The MVCC coalition leads development of four stage career pathways, virtual challenges, career planning, business partnerships, and competitions under the honor society.

Co-Lead Institution(s): The University of Alabama in Huntsville (UAH) and Moraine Valley Community College (MVCC)
POC(s): Dr. Tommy Morris
Email: tommy.morris@uah.edu

The project objective is to create and implement an online cybersecurity learning experience for high school students, where students will have the opportunity to earn high school credit, participate in extracurricular opportunities, and benefit from business partnerships. College credit may be obtained through select CAE-C institutions. The target audience is K12 students and schools, especially rural, under-resourced school systems, home school students, and schools without an established cybersecurity program.

RING is designed to give the high school learner the best online cybersecurity learning experience. With games and hands-on labs, this high school cybersecurity fundamentals class provides an age-appropriate curriculum. Developed by cybersecurity curriculum experts around the nation's only high school Cybersecurity Curriculum Guidelines (CCG), the program is inclusive, designed to be accessible to special populations. This program offers a clear education-career pathway, aligning CAE-C university degree options with work roles in the form of a fun, virtual experience. RING's student organization and honor society tie students to the cybersecurity community, while offering opportunities for students to complete service projects and conduct focused research. These opportunities will include after-school and extracurricular learning, which loops in a national business partnership.

RING is designed to remove the barriers to learning. By partnering with existing, accredited online K12 schools, students can easily earn high school credit for their learning, and qualifying low-income students will receive loaner laptops and Internet service, allowing students from home schools, rural schools, and technology-deprived schools an equal opportunity to learn. Additionally, students will have the option to earn credit that will transfer to institutions in the consortium, as well as other CAE-C institutions opting into the program.

Members of the UAH coalition include Coastline Community College, Dakota State University, Dark Enterprises, Pace University, and Purdue University Northwest. The UAH coalition leads curriculum development, instructs the online course for a national audience, and leads the student organization/honor society.

MVCC leads the second coalition of the partners, comprising of Brookdale Community College, Forsyth Technical Community College, California State Polytechnic University Pomona, Eastern New Mexico University Ruidoso, and Florida State College at Jacksonville. The MVCC coalition leads development of four-stage career pathways, virtual challenges, career planning, business partnerships, and competitions under the honor society.

UAH Coalition Partners

1

Partner Institution: Coastline Community College
POC(s): Dr. Tobi West
Email: twest20@coastline.edu

Initiative Description
Coastline Community College, the southwest partner, leverages their online instructional expertise to review online delivery methods and accessibility for the curriculum. They contribute the use of their NDG NETLAB+ virtual lab equipment for use in the instruction of the curriculum. Additionally, they utilize their relationships with CTE offices to assist with recruitment and credit transfer agreements.

2

Partner Institution: Dakota State University (DSU)
POC(s): Dr. Wayne Pauli
Email: wayne.pauli@dsu.edu

Initiative Description
DSU serves as the northwest region partner. As a leader in K12 education, they enhance the project by advising effective delivery methods, as well as providing feedback as to the curriculum's suitability and age-appropriateness. They also participate in credit transfer agreements.

3

Partner Organization: Dark Enterprises
POC(s): Melissa Dark
Email: melissa.dark@darkenterprisesinc.com

Initiative Description
Dark Enterprises develops and reviews formative assessments for the curriculum.

4

Partner Institution: Pace University
POC(s): Li-Chiou Chen
Email: lchen@pace.edu

Initiative Description
Pace University is the northeast region partner. Pace University examines the technical content of the curriculum and utilizes their existing pipeline to distribute the course. They also participate in credit transfer agreements.

5

Partner Institution: Purdue University Northwest
POC(s): Michael Tu
Email: Michael.Tu@pnw.edu

Initiative Description
Purdue University Northwest is the midwest region partner. They develop virtual games tied to the curriculum. These games reinforce concepts learned and provide a means of formative assessment. Additionally, they participate in credit transfer agreements.

6

K12 Partner Organizations: Alabama Connections Academy, Niswonger Online, and the National Rural Education Association

Initiative Description
Alabama Connections Academy and Niswonger Online host the curriculum for students, recruit students, and help with high school course accreditation. They also facilitate collaborations with school counselors and negotiate adoption by other K12 entities. The National Rural Education Association assists with recruitment efforts.

Moraine Valley Community College Coalition Partners:

1

Partner Institution: Brookdale Community College
POC(s): Michael Qaissaunee
Email: mqaissaunee@brookdalecc.edu

Initiative Description
Brookdale Community College, utilizing its success in building e-learning materials, leads development efforts in building the Cybersecurity Career Awareness Experience.

2

Partner Institution: Forsyth Technical Community College
POC(s): Dr. Deanne Wesley
Email: dwesley@forsythtech.edu

Initiative Description
Forsyth Technical Community College leads the effort to create, distribute and manage the National Directory of Cybersecurity K12 Pipeline Programs. This will include the organization of an annual college fair.

3

Partner Institution: California State Polytechnic University, Pomona (Cal Poly Pomona)
POC(s): Dr. Dan Manson
Email: dmanson@cpp.edu

Initiative Description
Cal Poly Pomona supports the national after school and extracurricular learning program. It will also track enrollment and participation of these events.

4

Partner Institution: Eastern New Mexico University - Ruidoso Branch Community College
POC(s): Dr. Stephen Miller
Email: Stephen.miller@enmu.edu

Initiative Description
Eastern New Mexico University Ruidoso, along with Florida State College at Jacksonville, lead the National Business Partnership Program. They will coordinate industry resources to provide students access to additional learning resources, products, and services.

5

Partner Institution: Florida State College at Jacksonville
POC(s): Ernest Friend
Email: ernest.friend@fscj.edu

Initiative Description
Florida State College at Jacksonville, along with Eastern New Mexico University-Ruidoso, lead the National Business Partnership Program. They will coordinate industry resources to provide students access to additional learning resources, products, and services.

Consolidated CAE-C Professional Development Resources (Ethics & Professionalism for Students)

Consolidated CAE-C Professional Development Resources, which are to provides students with insight into careers in cybersecurity, professional behavior and ethics, and other soft skills in demand in the workplace. Available to all students in a CAE-C-designated program to assist with exposure to cyber career paths and soft skill development. The audience for these materials will be CAE-C schools and students.

A. Cybersecurity Ethics Book and Curricula

Assemble an advisory group of experts from various industries to guide the book's content. The following major topics will be addressed:

1. **Create a Cybersecurity Oath.** This oath will be similar to the Hippocratic Oath in the medical field and serve as a guideline for ethical behavior for cyber professionals. When one considers the history of Western civilization, leaders through the ages have addressed the challenges of their time with solutions that often have a moral component. Medicine has the Hippocratic Oath. Law has legal ethics. Military engagement has Just War Theory, manifest in the Geneva Conventions. There are currently no broadly accepted moral guidelines in the world of cybersecurity. The creation of moral guidelines and demonstrated practice for cybersecurity is one of the pressing needs of our time.

2. **Ethics as a Requirement.** Explore ways to expand ethics within the academic curriculum and convince industry that ethics should be paramount in their sponsored training curricula. Ethics must be embedded into cybersecurity curriculum.

3. **Case Studies.** The book would examine relevant case studies (e.g. Edward Snowden, Eric Marques, Cameron Ortis) to develop road maps for government, industry, and academia in the importance of professionalism, ethics, and character in cybersecurity education, training, and operations. These case studies will be examined by subject matter experts from various fields, who will provide interdisciplinary input to help inform multiple audiences.

4. **Exploration of Classical and Modern Ethical Frameworks.** A multitude of foundations will be explored, from Aristotlian thought to Thomas Aquinas and others. Where we explore non-secular ethics, we would aim to wrap those philosophies together with similar secular ethics and create a universalized foundation that can be properly applied to cybersecurity.

5. **Exploration and Application of Just War Theory into Cybersecurity.** Adding to the exploration of ethical frameworks on the defensive side of cybersecurity, a narrative for the offensive side of cybersecurity would be created through exploration of the history of Just War Theory, with the goal of modernizing that theory to address the digital battlefield. The digital version of the Geneva Convention is something that is sorely needed as the theater of cyber war rapidly expands and evolves. In this exploration, we will look at documents such as the Tallinn Manual and review what other countries are doing to combat advanced persistent threats and peer and near-peer adversaries.

Cybersecurity Ethics Book Advisory Group:

- John Gallagher, Chief Operating Officer, Institute for Global Engagement
- Col. George Youstra, Command Chaplain, United States Special Operations Command
- Ed Skoudis, Co-founder, Counter Hack and SANS Faculty Fellow
- L. Crosland Stuart, Literary Agent and Project Development Specialist, Legacy, LLC
- Sandy Shugart, President, Valencia Community College (CAE-C)

Curriculum Development:

- Professor Jim Tippey, M.S., M.Div., CISSP, C|EH, Assistant Professor of Cybersecurity, Montreat College
- Mark Wells, Ph.D., Professor of Ethics/Philosophy, Faculty Ethicist, Montreat College

B. Professionalism and Soft Skills Curriculum Development & Pilot Program

The curricula for the pilot program have been developed around the following four key strategies:

1. **Identity development** is the strategy that builds upon students' experiences, strengths, and self-awareness to develop answers to questions such as "Who am I?" "What is my purpose?" and "How can I be authentic?" Students are introduced to assessments, such as the Clifton StrengthsFinder and Myers-Briggs Type Indicator (MBTI) to

deepen their self-understanding and insight as to how their unique set of strengths and other characteristics can be applied to their chosen work.

2. **Impacting experience** is the strategy that makes available opportunities to all students, such as internships, job shadowing, and service learning to help students put into practice what they have learned about a particular area of interest. In the process, impacting experiences help affirm that their chosen major and career will bring satisfaction, a sense of purpose, and the accomplishment of personal goals. Students are encouraged to use these experiences in campus involvements, such as student leadership, athletics, and service as opportunities to further develop skills desired by employers, such as problem-solving, collaboration, teamwork, and communication.

3. **Influential relationship** is the strategy that builds upon students' aspirations and goals through connections with others that help increase knowledge about careers and fields, develop networks and external relationships, and build social capital based on authentic relationships. Career counselors, mentors, sponsors, alumni, and others can provide guidance, ask intentional questions, give practical advice, and share their own journey and narrative of discerning a sense of purpose and calling. Academic advisors can provide guidance that will help students engage in curricular and co-curricular experiences most likely to develop employable skills.

4. **Readiness** is the strategy that equips students to reflect on their experiences, helps them hone their portfolio and interviewing skills, and gives them an employment search roadmap for identifying organizations and positions of interest.

The pilot program will emphasize the importance of experiential learning and the resulting development of abilities and characteristics desired by employers across disciplines. These skills include those identified by the National Association of Colleges and Employers (NACE), and are in alignment with outcomes of a liberal arts education such as critical thinking, problem-solving, collaboration, and interpersonal skills. Influential relationships, such as academic and co-curricular advising, mentoring and career readiness strategies, the use of ePortfolios, and a video assessment platform, will also be incorporated. Tools to support these strategies will be developed, including a step-by-step guide for students to build a portfolio and a comprehensive two- or four-year academic plan, with recommended career planning milestones and purposeful activities, which would be shared with CAE institutions. The activities outlined in the guide would help students identify how their experiences are helping them develop and utilize skills for improved employability. Through this guide, they would be led to engage in experiences, reflect on them, capture and curate examples of what they have learned and accomplished, and articulate their learning and its application to future experiences, such as employment.

Co-Chairs of the Professionalism and Soft Skills Curriculum Development & Pilot Program subcommittee:

- Marie Wisner, Ph.D., Associate Dean for Calling and Career, Montreat College Thrive Center

- Greg Sayadian, MS, Assistant Professor of Cybersecurity, Montreat College

C. **Cybersecurity Career Videos**

This deliverable set will leverage input from across our capable team. We

will define eight to ten entry-level cybersecurity roles that are prevalent or are emerging in the market today. These roles will be those achievable with a college degree and mature apprenticeship programs within approximately three years of graduation. This includes roles such as:

- Information Security Analyst
- Systems Administrator
- Network Analyst/Engineer
- Incident Handler/Response Analyst
- Penetration Tester
- Vulnerability Analyst
- Cybersecurity Assessment Analyst
- SOC Analyst I
- Security Auditor

We will then identify individuals currently working in these jobs and ask them to take part in videos to be added to a career video library. Due to travel and other potential factors, the videos will often need to be created remotely. To ensure minimum quality standards and efficiency, we will define a proper consistent environment for professionally curated videos (e.g., dress, background, colors, quiet, lighting, camera height and angles). We will also provide a set of questions (outlined below) and coaching as to how to be crisp and clear in their responses, and to be engaging for the audience. We will also conduct live practice sessions to value a participant's time.

Chair Career Pathways Team:

- Adam Bricker, Executive Director/Co-founder, Carolina Cyber Center at Montreat College

D. **Directory of Materials and Creation of Additional Materials**

Montreat will publish an online, continuously modifiable directory (not repository) of resources already in use by the CAE-C community. Principals from each CAE-C institution will be able to submit listings for their own materials in the appropriate categories. Each listing would include the title of the resource, followed by the provider institution, description, delivery format, contact information, and a URL. The principals from each institution will be able to modify or remove their directory listings. Montreat will review listings before they are published.

A tentative list of categories for this directory includes: Critical Thinking/Problem-Solving, Teamwork/Collaboration, Professionalism / Work Ethic, Oral/Written Communication, Leadership, Global/Multicultural Fluency, Ethical Judgment/Decision-Making, and Career Paths/Management.

After populating the directory with the list of materials currently in use by the CAE-C Community, Montreat College faculty, together with faculty from the below colleges and universities, will perform a gap analysis of available materials, identify additional materials that need to be developed, and develop them based on funding availability.

- Alexandria Technical & Community College
- Fayetteville Technical Community College (CAE-C)
- Eastern New Mexico University - Ruidoso Branch Community College (CAE-C)
- Johnson C. Smith University
- University of Houston, College of Technology (CAE-C)
- University of Detroit Mercy (CAE-C)

Student workers using a digital management platform will format, tag, and catalog digital resources. Once materials are completed, faculty will share, using CLARK.center and CAE forums.

Chair Directory of Materials and Creation of Additional Materials:

John Bannister, PhD, Instructional Designer, Johnson C. Smith University

Team Members:

- Kelli Burgin, MS CIS, CISSP, Assistant Professor of Cybersecurity, Montreat College
- Chris Herring, Department Chair, Systems Security & Analysis, Fayetteville Technical Community College
- Denise Kinsey, PhD, CISSP, CCISO, Assistant Professor, Department of Information & Logistics Technology, University of Houston, College of Technology
- Anne Kohnke, PhD, Associate Professor of Cybersecurity, The University of Detroit Mercy
- Vickie (Valerie) McLain, Cybersecurity Instructor, Alexandria Technical & Community College
- Stephen Miller, Professor and Director Cybersecurity Center of Excellence, Eastern New Mexico University–Ruidoso Branch Community College.

E. Dissemination of Curricula and Other Materials

Each of the four deliverable sets defined above are designed to be disseminated to the CAE-C community. To maximize dissemination, however, we will also design and run on-site or virtual workshops, as conditions allow. The goal of the workshops will be to enhance collaboration, conduct group review of materials, and "train the trainers," so that the CAE-C community can take ownership and leverage the materials defined. We will provide awareness presentations at three cybersecurity conferences, such as the CAE Symposium, CAE ELF, CISEE, or Community College Cybersecurity Conference. We will present up to five one- to two-day workshops to train the trainer at CAE hubs. We will also make presentations available through the CAE Forum Webinars.

Co-Chairs of the Dissemination subcommittee:

- John Bannister, Ph.D., Instructional Designer, Johnson C. Smith University
- Kelli Burgin, MS CIS, CISSP, Assistant Professor of Cybersecurity, Montreat College

The six principal personnel who will be responsible for the key deliverables comprise over 85 years of practical industry IT and cybersecurity experience, over 50 years of higher education experience, and offer a demonstrated commitment to advancing the development of cybersecurity professionals in industry and academia. We are honored to have this opportunity to serve the CAE-C community.

POC(s): Kelli Burgin
Phone(s): (828) 669-8012 Ext. 3456, (712) 304-0730
Email: kelli.burgin@montreat.edu

Senior Military College[1] (SMC) Cyber Institutes

The Department of Defense faces a competitive environment for the recruitment and retention of world-class cyber talent. DoD requires a deliberate pathway to enable talent development in cyber and cyber-related competencies to meet Department workforce needs for near term and future emerging cyber challenges. Development of talent is a critical component of DOD success in maintaining ahead of adversaries and defending the U.S. and its national interests. The DoD Cyber Institutes at the SMCs will have five lines of effort.

LOE 1: Develop SMC DoD Cyber Institutes

- Staff Hiring x SMC 2 FTEs and 6 x Military (*)
- Academic programs
- Expand programs to meet U.S. Cyber Command skills gaps
- Research programs

LOE 2a: Expand and Sustain Cyber Experiential Programs (Internal)

- InSURE and Hack for Defense Semester programs – Technical, Policy, and others Challenge problems
- Degree capstones and projects linked to U.S. Cyber Command requirements
- Expansion of Security Operations Centers/Security Situation Centers

LOE 2b: Expand and Sustain Cyber Experiential Programs (External)

- Cadet Leader Develop Program expansion
- U.S. Cyber Command Internships and Apprenticeships/ SMC Technical and Leadership programs
- Expeditionary Corps programs at U.S. Cyber Command, DISA, and CSC

[*] Senior military colleges (SMC) offer military Reserve Officers' Training Corps (ROTC) programs under 10 USC 2111a(f). The school must establish a corps of cadets in which all students wear military uniforms, and the corps of cadets live in a military environment constantly, not just during the school day, and students are subject to military discipline. The SMC must have as an objective the development of character through military training and the regulation of cadet conduct according to principles of military discipline (a cadet code of conduct). The SMC must maintain military standards similar to those of the federal service academies. Cadets at an SMC are authorized to take the ROTC program all four years, but taking a commission upon graduation remains optional, unlike other colleges where ROTC cadets are required to sign a contract to take commission before entering their final two years. Five of the six SMCs in the US are designated CAE-C schools, and the fifth participates in Candidates.

LOE 3: Recruit, Train, and Deploy RC SMC Deputy Directors

LOE 4: Extend Persistent Cyber Training Environment to SMCs

LOE 5: Build Governance and Assessment Framework/Processes

- Government Governance
- SMC Governance
- Joint Governance
- Assessment reporting and demonstrations

This initiative addresses a Department of Defense requirement, and will be executed in partnership between the NCAE-C Program Office, Office of Secretary of Defense R&E, and U.S. Cyber Command. The objectives for the Cyber Institutes and those of the NCAE-C Evidencing Competency Working Group are closely aligned and achievements of one will support the other.

Lead Institution: Norwich University
POC(s): Dr. Sharon Hamilton
Email: shamilto@norwich.edu

Workforce Development Pilots

National CAE-C Cybersecurity Workforce Development Program (University of Louisville)

The Cybersecurity Pathways Coalition (CPC) will develop and pilot a certificate-based workforce-development program, focusing on cybersecurity for the healthcare industry. This Healthcare Cybersecurity Pathways program will be implemented in the academic year. The "Healthcare Cybersecurity Certificate" will be awarded to applicants upon completion of a series of instructor-led online cybersecurity courses, incorporating technology industry badges and experiences focused on healthcare systems. Participants will demonstrate accomplishments in competency levels, experiential learning, and career readiness assessments. The program will include proprietary materials (owned by IBM, Microsoft, Cisco, AWS, Google, etc.).

The CPC will create a pathway leading to a Healthcare Cybersecurity Certificate with participants earning both the Certificate and several technology badges. Cybersecurity education is typically industry-agnostic or concentrated in specific industries such as tech, banking, finance, and manufacturing.

Lead Institution: University of Louisville
POC(s): Dr. Sharon Kerrick
Email: sharon.kerrick@louisville.edu

Coalition Partners

1

Partner Institution: University of Arkansas at Little Rock
POC(s): Dr. Mariofanna Milanova
Email: mgmilanova@ualr.edu

Initiative Description
The University of Arkansas at Little Rock (UALR) will work on the development of cybersecurity education curriculum, utilizing topics on cutting edge technologies, all relating to healthcare cybersecurity. UALR military veteran connections are through the Director of Military Affairs for the Arkansas Economic Development Commission, Little Rock

Air Force Base 223rd Cyberspace Operations Squadron, and the Army National Guard Professional Education Center at Camp Robinson.

2

Partner Institution: University of North Florida
POC(s): Dr. Bridgett Rahim-Williams
Email: bridgett.rahimwilliams@unf.edu

Initiative Description
The Coalition's program development and execution will incorporate University of North Florida's (UNF) regional council of cybersecurity professionals from these UNF partner groups: Mayo Clinic, Florida Blue, Deutsche Bank, FIS, CSX, and Crowley Maritime, technology companies (e.g., IBM and Microsoft), government (e.g., F.L. Dept of Law Enforcement, Jacksonville Sheriff's Office, and Office of Naval Intelligence), and academics. UNF is experienced in cybersecurity program curriculum and will be in lead roles to organize content and experiential learning components into the three levels of the purposed pilot program. Their partners of the PAX Technology Cybersecurity Lab and industry healthcare system experts will also teach/guest lecturer. UNF has expertise in intrusion detection, forensics, disaster recovery, and preparedness.

3

Partner Institution: Owensboro Community & Technical and Bluegrass Community & Technical colleges
POC(s): Dr. Kris Williams and Dr. Erin Tipton

Initiative Description
Kentucky Community and Technical Colleges CAE's (Owensboro and Bluegrass) offer robust courses in cybersecurity and have extensive technical knowledge, as well as course development expertise. They are valuable to our team because of this expertise, as well as the constituents they serve are typically workforce development types of audiences, so they understand the practical hands-on approaches that will be critical for us to incorporate in this certificate.

National CAE-C Cybersecurity Workforce Development Program (Purdue University Northwest)

Purdue University Northwest (PNW) in collaboration with Ivy Tech Community College, University of North Carolina at Charlotte (UNCC), and University of Tennessee at Chattanooga (UTC), will establish a Cybersecurity Workforce Development Consortium and develop a pilot AI-Cybersecurity certification-based national training program following USDOL apprentice training model for transitioning military, first responders, and other adult trainees. The main objectives for the pilot training program include the following:

1. Develop AI and Cybersecurity course curriculum with online access.
2. Recruit over 425 adult learners primarily transitioning military and first responders.
3. Offer three training tracks in cybersecurity administration, digital forensics, and artificial intelligence, each with six 8-week online courses. Upon completion of the courses, trainees are expected to take exams from certification vendors to earn certifications.
4. The training programs are offered online and are free of charge to all participants.

5. Tracks include certification training in CompTIA A+, CompTIA Linux+, CompTIA Security+, Cisco CyberOps Associate, EC Council CEH, EC Council CHFI, AWS Machine Learning, and Certified AI Practitioner.

Establishing a Workforce Development Consortium for a Pilot AI-Cybersecurity Certificate-Based National Training Program

Lead Institution: Purdue University Northwest
POC(s): Michael Tu
Phone(s): (219) 989-2634 (Office), (219) 670-6674 (Cell)
Email: Michael.Tu@pnw.edu
More Information: https://www.pnw.edu/cybersecurity/

Initiative Description

The consortium will create a pilot certificate-based apprentice training program to train a large number of transitioning military, first responders, and other adult trainees to enter into the IT and cybersecurity industry. The following three goals will be established for the training program.

1. Recruit 425 training participants, primarily from transitioning military and first responders.

2. Develop open accessible hands-on-based AI-Cybersecurity course curriculum with flexibilities for trainees to choose a training track that fits their educational background and career needs. The curriculum is expected to be mapped to existing courses which will allow pathways to be created for trainees to pursue degree programs at the participating institutions.
3. Offer AI-Cybersecurity training with online delivery that can accommodate the large number of target trainees' work schedules and locations. Through the program, training participants will be prepared with foundational skills and competencies in cybersecurity, industry-recognized and US DoD-endorsed certifications at three competency levels in various categories (DoD, 2020).

A total of three training tracks, Cybersecurity-System Administration (CS_ SA), Cybersecurity-Artificial Intelligence (CS_AI), Cybersecurity-Digital Forensics (CS_DF), will be offered through the program. All the tracks are composed of three core courses, that are common to all the tracks and are required courses and three elective courses that are unique for each individual track. Each course is offered with 45 instructional hours in 10 weeks with the last two weeks for certification preparation and examination. It is expected that each course will be offered at least two times and each training participant will receive at least three certifications.

Tracks	3 Required Core Courses	The 3 Elective Courses that are required for the Track
CS_SA	CompTIA A+ CISCO Cyber Ops Security+	Linux+, Cloud System Administration, CEH (Certified Ethical Hacker)
CS_DF		Computer Forensics-ACE, Mobile Forensics, CHFI
CS_AI		Python Essentials, IoTs Security, Machine Learning for Cybersecurity

In Year 1 (2020-2021), AI-Cybersecurity training course curriculum will be developed, online platform will be ready, qualified instructors will be hired and trained, training participants will be recruited, academically preparedness will be evaluated and enrolled into training courses.

In Year 2 (2021-2022), a total of five training sessions (10 weeks long for each session) will be offered online in evenings and on weekends. Training participants will be assessed with certification readiness and will be supported to take certification exams. The consortium will establish partnerships with industry and government agencies and will provide placement services to training participants.

partnerships with industry and government agencies and will provide placement services to training participants.

Coalition Partners

1

Partner Institution: Ivy Tech Community College
POC(s): Matthew Cloud (Associate Director) Lake County Campus
Phone(s): (219) 981-1111 x5369 (Office), (817) 690-2684 (Cell)
Email: mcloud3@ivytech.edu
POC(s): Rami Maximus Salahieh (PI) Valparaiso Campus
Phone(s): (219) 464-8514 x3079, (219) 201-2925 (Cell)
Email: rsalahieh@ivytech.edu

Initiative Description

Ivy Tech will be responsible for developing course curriculum (three courses) of the AI-Cybersecurity training program, recruiting training participants, offering the three tracks of training program, and providing placement service to training participants. Besides this, Ivy Tech will lead the consortium on instructor hiring, instructor professional development training, industry/government agency partnership development, CyberRange lab management, and technical support technicians for students on labs.

2

Partner Institution: University of North Carolina at Charlotte (UNCC)
POC(s): Fareena Saqib (PI)
Phone(s): (704) 687-8098 (Office), (505) 377-1198 (Cell)
Email: fsaqib@uncc.edu
POC(s): Shagufta Y Raja (Co-PI)
Phone(s): (704) 687-8728 (Office), (704) 649-6425 (Cell)

Initiative Description

UNCC will be responsible for developing course curriculum (one course) of the AI-Cybersecurity training program, recruiting training participants, offering one track of training program, and providing placement service to training participants.

3

Partner Institution: University of Tennessee at Chattanooga (UTC)
POC(s): Mengjun Xie (site PI)
Phone(s): Mengjun Xie: (423) 425-5863 (Office), (501) 259-4659 (Cell)
Email: mengjun-xie@utc.edu
POC(s): Daniel Pack (site Co-PI)
Phone(s): Daniel Pack: (423) 425-2256
Email: Daniel-Pack@utc.edu

Initiative Description

UTC will be responsible for developing course curriculum (one course) of the AI-Cybersecurity training program, recruiting training participants, offering one track of training program, and providing placement service to training participants.

National CAE-C Cybersecurity Workforce Development Program (University of West Florida)

The University of West Florida will lead a coalition of 10 CAE-C institutions to establish a nationally scalable and sustainable certificate-based cybersecurity workforce development program. The overall goal is to establish a best practice, nationally scalable and sustainable certificate-based program with verifiable credentialing to more rapidly expand the cybersecurity workforce as follows: (a) increase the number of qualified, skilled professionals; (b) support their transition to cybersecurity work roles in critical infrastructure sectors, with

initial emphasis on transitioning military and first responders for the defense industrial base, financial services, and energy Critical Infrastructure sectors; and (c) provide CAE-C institutions access to curricular resources through the NCAE Resources Directory. In addition to overall program leadership and coordination, UWF will also target transitionaing military and first responders with their Cybersecurity Workforce Development Program.

POC(s): Dr. Eman El-Sheikh
Phone: (850) 426-4995
Email: eelsheikh@uwf.edu
More Information: uwf.edu/cae

Coalition Partners

1

Partner Institution: University of South Florida – Cyber Florida
POC(s): Dr. Ron Sanders

Initiative Description
The University of South Florida – Cyber Florida will target military and veterans with their New Skills for a New Flight Program. The goal is to prepare and place transitioning military and first responders into cybersecurity work roles. Cyber Florida will co-lead efforts focused on employer and industry engagement and partnerships.

2

Partner Institution: University of Houston
POC(s): Dr. Art Conklin

Initiative Description
The University of Houston will co-lead efforts focused on the development of best-practice workforce development and curricular models.

3

Partner Institution: Augusta University
POC(s): Dr. Michael Nowatkowski

Initiative Description
Augusta University will target transitioning military with their Cyber Workforce Transition Program. They will recruit transitioning military members with bachelor's degrees to participate in the program and earn the Cyber Defender certificate in order to enhance student preparation and employability for cybersecurity jobs.

4

Partner Institution: Dakota State University
POC(s): Dr. Wayne Pauli

Initiative Description
The Dakota State University will target transitioning military and first responders with their Digital Forensics and Open Source Intelligence (OSINT) Training for First Responders and Transitioning Military Program. The learner-centric competency-focused education will train students on evidence identification, acquisition, preservation and investigative processes for traditional hard disk drives, emerging IoT devices, cloud accounts, and online communication.

5

Partner Institution: Eastern New Mexico University – Ruidoso Branch Community College
POC(s): Stephen Miller

Initiative Description
Eastern New Mexico University – Ruidoso Branch Community College will target transitioning military and first responders, and Native American populations with their Computer and Network Cybersecurity Certificate Program. In year one, they will offer the Computer and Network Security Certificate integrated with an Apprenticeship certificate program, leveraging expertise in Risk Management and DHS CSET Tool. In year two, they will expand the program and align with the coalition workforce and curricular models.

6

Partner Institution: Florida International University
POC(s): Randy Pestana

Initiative Description
Florida International University will target transitioning military and first responders with their Veterans and First Responders Cyber Threat Intelligence (VFR-CTI) Fellowship Program. By the end of the one-year fellowship program, a cohort of veterans and first responders will have received conditional job offers, internships, or apprenticeship opportunities that will have them contributing to the cybersecurity workforce.

7

Partner Institution: Metropolitan State University
POC(s): Dr. Faisal Kaleem

Initiative Description
Metropolitan State University will target transitioning military, first responders and other underrepresented minorities with their Intensive Cybersecurity Program for our Nation's Heroes. The program will implement an accelerated cybersecurity training program to prepare and place transitioning military veterans, first responders, and other underrepresented minorities into cybersecurity work roles.

8

Partner Institution: San Antonio College
POC(s): Kim Muschalek

Initiative Description
San Antonio College (SAC) will target transitioning military, existing first responders, SAC Finance and Criminal Justice majors with their Cyber Workforce Development Program. The goal is to increase the number of transitioning military veterans, existing first responders, and Criminal Justice, and Finanance degree earners who are prepared to defend our nation's security and prosperity via cybersecurity-related positions in San Antonio, Texas, and beyond.

9

Partner Institution: University of Texas at San Antonio
POC(s): Dr. Glenn Dietrich

Initiative Description
The University of Texas at San Antonio will target transitioning military personnel with their Workforce Development for Transitioning Military Program. The goal is to increase the number of certifications and job placements among both groups and increase the number of organizations that hire students.

Appendix

Participating Academic Institutions

Proposed Activities	Coalition
CAE Community National Center (CNC)	
Lead collaboration among the designated institutions, inclusive of Candidates, in accordance with program office policy. Provide administrative support to the Community (webinars, platform licenses, web pages). Manage of CAE-C travel, directory of event facilities, planning and management of events, support for competency development to include NICE Challenge, other tools, and student documentation software	**California State University, San Bernardino**, San Bernardino, CA
Sub-Task: CAE Regional Hubs	
Northwest Regional Hub Lead	**University of Colorado Colorado Springs**, Colorado Springs, CO
NW Regional Partner	**US Air Force Academy**, Colorado Springs, CO
NW Regional Partner	**Arapahoe Community College**, Littleton, CO
NW Regional Partner	**Pikes Peak Community College**, Colorado Springs, CO
NW Regional Partner	**University of Colorado**, Denver, CO
NW Regional Partner	**Northern Idaho College**, Coeur d'Alene, ID
NW Regional Partner	**North Dakota State University**, Fargo, ND
NW Regional Partner	**Montana State University**, Bozeman, MT
NW Regional Partner	**Portland Community College**, Portland, OR
NW Regional Partner	**Dakota State University**, Madison, SD
NW Regional Partner	**Brigham Young University**, Provo, UT

Proposed Activities	Coalition
NW Regional Partner	**University of Washington**, Seattle, WA
NW Regional Partner	**City University of Seattle**, Seattle, WA
NW Regional Partner	**Whatcom Community College**, Bellingham, WA
Southwest Regional Hub	**San Antonio Community College**, San Antonio, TX
SW Regional Partner	**Bossier Parish Community College**, Bossier City, LA
SW Regional Partner	**The University of Texas at San Antonio**, San Antonio, TX
SW Regional Partner	**National University**, San Diego, CA
SW Regional Partner	**University of Arizona**, Tucson, AZ
SW Regional Partner	**Eastern New Mexico University**, Ruidoso, NM
SW Regional Partner	**University of Arkansas**, Fayetteville, AR
SW Regional Partner	**The University of Hawaii Maui College**, Kahului, HI
Midwest Regional Hub	**Moraine Valley Community College**, Palos Hills, IL
MW Regional Partner	**Davenport University**, Grand Rapids, MI
MW Regional Partner	**John A. Logan College**, Carterville, IL
MW Regional Partner	**Purdue University NW**, Hammond, IN
MW Regional Partner	**Johnson County Community College**, Park KA
MW Regional Partner	**Owensboro Community & Tech College**, Owensboro, KY
MW Regional Partner	**Sinclair Community College**, Dayton, OH
MW Regional Partner	**Madison College**, Madison, WI
MW Regional Partner	**Metropolitan State University**, St Paul, MN
Northeast Regional Hub	**Capitol Technical University**, Laurel, MD
NE Regional Partner	**Mohawk Valley Community College**, Utica, NY
NE Regional Partner	**Towson University**, Baltimore, MD

Proposed Activities	Coalition
Southeast Regional Hub	**University of West Florida**, Pensacola, FL
SE Regional Partner	**University of Alabama in Huntsville**, Huntsville, AL
SE Regional Partner	**Valencia College**, Orlando, FL
SE Regional Partner	**Augusta University**, Augusta, GA
SE Regional Partner	**Bluegrass Community & Technical College**, Lexington, KY
SE Regional Partner	**Mississippi State University**, Starkville, MS
SE Regional Partner	**University of North Carolina**, Charlotte, NC
SE Regional Partner	**Polytechnic University of Puerto Rico**, San Juan, PR
SE Regional Partner	**The Citadel**, Charleston, SC
SE Regional Partner	**Tennessee Tech University**, Cookeville, TN

Sub-Task: Communities of Practice

Community of Practice Cyber Defense	**Nova Southeastern University**, Fort Lauderdale, FL
Community of Practice Research (Support INSuRE)	**Northeastern University**, Boston, MA
	Stevens Institute of Technology, Hoboken, NJ
Community of Practice Cyber Operations	**Mississippi State University**, Starkville, MS

Sub-Task: Resource Directory and Feasibility Study

Education resource directory	**Center for Cybersecurity Education & Innovation (CCEI)**, Savage, MD
Study on feasibility of high school CAEs	

Proposed Activities	Coalition
Sub-Task: Knowledge Units	
Develop NCAE-C Knowledge Unit Community Recommendations	**University of Houston**, Houston, TX
Sub-Task: Publishing	
Graphics, publishing, & printing	**Moraine Valley Community College**, Palos Hills, IL
Candidates Program National Center	
Manage NCAE-C Application Tool, evaluate Applicants/assign & manage mentor; Provide pre-submission review; Endorse readiness for designation Collaborate with Peer Review CNC & Develop Application Review Rubric	Lead: **Whatcom Community College**, Bellingham, WA **Northern Virginia Community College**, Alexandria, VA for peer review
Initiative: CAE-C Competition Program	
Introduction Level Infrastructure	Lead 1: **Mohawk Valley CC**, Utica, NY Lead 2: **University of South Florida**, Tampa, FL
Collaboration with Evidencing Competency WG	
Collaboration with Program Office and other Federal Partners	
Initiative: Consolidated CAE-C Professional Development Resources	
Provide students with insight into careers in cybersecurity, professional behavior and ethics, and other soft skills in demand in the workplace.	Lead: **Montreat College**, Montreat, NC

Proposed Activities	Coalition
Initiative: Cybersecurity Diversity Education Initiative (CEDI)	
CAE-C Coalition supporting development of programs at Minority Serving Institutions (Historically Black Colleges and Universities – HBCUs; Primarily Black Institutions – PBIs; Hispanic Serving Institutions – HSIs; Tribal Colleges and Universities – TCUs; Asian American and Pacific Islander Serving Institutions – AAPISIs)	Co-Leads: **Fordham University**, New York, NY and **Excelsior College**, Albany, NY Coalition Members: **Bluegrass Community & Technical**, Lexington, KY **Metropolitan State University of Denver**, Denver, CO **New Jersey City University**, Jersey City, NJ **North Carolina A&T**, Greensboro, NC **Polytechnic University of Puerto Rico**, San Juan, PR **Tennessee Tech University**, Cookeville, TN **University of North Florida**, Jacksonville, FL **University of North Texas**, Denton, TX **University of Tennessee at Chattanooga**, Chattanooga, TN

Proposed Activities

Capacity building for MSIs. A group of partner NCAE-designated institutions have committed to providing faculty time to mentor and assist new schools, to provide range time, curriculum, lab designs, and other resources to build cybersecurity education programs at CEDI institutions.

Coalition

American Public University System
Athens State University
Baker College
Carnegie-Melon University
Excelsior College
Florida A&M University
Harford Community College
Henry Ford College
Houston Community College
Indiana University
Kentucky Community and Technical College System
Lamar Institute of Technology
LeMoyne-Owen College
Lewis University
Metropolitan State University of Denver
National University
New Jersey City University
New York Institute of Technology
New York University
Norfolk State University
North Carolina A&T State University
Old Dominion University
Polytechnic University of Puerto Rico
St. Bonaventure University
St. Cloud State University
St. Petersburg College
Simmons College
South Carolina State University
SUNY Rockland
Talladega College
Tuskegee University
University of Arizona
University of Denver
University of Maryland Global Campus
University of Nevada Las Vegas
University of Tennessee at Chattanooga
University of Texas at El Paso
University of Texas at San Antonio
Webster University

Proposed Activities	Coalition
Initiative: Cybersecurity Faculty Development: Expand pool of CS educators available to CAEs	
Current Faculty Development 1 – Workshops (five topics) each year based on community requirements; train 100 participants each 2 – Prepare 25 cybersecurity faculty for DoD-recognized IT industry certifications 3 – Online for-credit SCADA classes for 500 participants 4 – Workshops to prepare faculty for scenario-based teaching and integration of scenarios into their curricula 5 – Workshops on Advanced Incident Response and Handling; leverages Minnesota Cyber Range and other open source platforms 6 – Faculty participate in Security Operation Center (SOC) cybersecurity incidents through Blue Team scenarios on Minnesota Cyber Range 7 – 10 workshops, 15-20 faculty each, aligned to industry credentials (CISSP, CISA, CEH, Security+, CCNA Security Operations, Palo Alto Security Fundamentals and Linux Professional Institute, VMware, EMC, and Meraki Pedagogical Support for Professors of Practice 1 – Recruit cybersecurity subject matter experts (SMEs) from industry leveraging Minnesota Cyber Institute's partner network 2 – Provide SMEs with necessary pedagogical background, tools and resources 3 – Assign participating SMEs as adjunct faculty at CAEs 4 – CSSIA National Academy will make pedagogical support systems for courses, including instructional best practices, content, activities and assessment tools. 5 – Mentoring support once instructors complete CSSIA workshops 6 – Online curriculum library with rubrics and assessment tools Transition Military and Government Personnel 1 – Recruit veterans interested in teaching to upskill them with pedagogical and technical expertise; assist with placement at CAE-Cs 2 – Provide faculty mentors for participating veterans 3 – Train 10 transitioning military members with pedagogical assistance, financial support, and placement at CAE-C institutions. 4 – Recruit 5-10 local veterans to retrain into education	Lead 1: **Dakota State University**, Madison, SD **Metropolitan State University**, St Paul, MN **University of West Florida**, Pensacola, FL **Moraine Valley Community College**, Palos Hills, IL **San Antonio College**, San Antonio, TX **Tennessee Tech University**, Cookeville, TN **University of North Texas**, Denton, TX **University of Alabama in Huntsville**, Huntsville, AL

Proposed Activities	Coalition
1 – Recruit and train 1,335 existing faculty through cybersecurity teaching workshops, hybrid courses, boot camps on tools/techniques, industry certifications, and program development workshops. Engage 100 institutions and provide support to three faculty members from each institution helping, them develop cybersecurity management degree programs. 2 – Recruit and train 200 Professors of Practice. UCCS plans to recruit industry cybersecurity experts with existing credentials and/or a Master of Science degree and train them on pedagogy, curriculum development, and soft skill classroom dynamics. Two target populations: (1) those that continue to work in industry that could adjunct outside work hours; and (2) those retiring from industry, military, or civil services who with this training can take on a full-time position teaching cybersecurity. 3 – Recruit 250 graduate students, particularly PhD candidates, to teach in cybersecurity; develop a recruitment program for graduate students and PhD candidates focused on providing cybersecurity scholarship opportunities, career guidance, and placement program. The eight graduate certificate options available to grant participants are discussed in the subsequent sub-section.	Lead 2: **University of Colorado Colorado Springs**, Colorado Springs, CO **Florida International University**, Miami, FL **University of Cincinnati**, Cincinnati, OH **University at Albany**, Albany, NY **University of New Mexico**, Albuquerque, NM **Arizona State University**, Tempe, AZ **US Air Force Academy**, Colorado Springs, CO **Whatcom Community College**, Bellingham, WA **Robert Morris University**, Pittsburgh, PA **National Cyber Watch Center**, Largo, MD

Initiative: Evidencing Competency Oversight: Establish CAE-C Competency Program

Design & implement a regional exercise program engaging state and local government, industry, and military Projects to advance competency Integration of sub-working group deliverables, definitions and documentation, tools, and competitions for competency development/measurement	Lead: **Norwich University**, Northfield, VT Sub-WG1: Dr. Vinnie Nestler Sub-WG2: Dr. Susanne Wetzel Sub-WG3: Dr. Dan Manson

Initiative: National K12 Pipeline

Target audience: While the pipeline program should be open to all middle and high school students in the United States, target students are youth in rural and under-resourced school systems, home schooled students, and those attending schools without a cybersecurity program.

• Building a fully engaging Cybersecurity Career Awareness Experience: Gamification to demonstrate cybersecurity careers • Establishing an after school and extracurricular learning program • Coordinating a National Business Partnership Program • National standardization • Articulation agreements/dual credit	Lead 1: **Moraine Valley Community College**, Palos Hills, IL **Brookdale Community College**, Lincroft, NJ **Forsyth Community College**, Winston-Salem, NC **Eastern New Mexico University-Ruidoso Branch Community College**, Ruidoso, NM **Florida State College at Jacksonville**, Jacksonville, FL

Proposed Activities	Coalition
• Developing an open source online cybersecurity foundations curriculum • Recruitment strategies	Lead 2: **University of Alabama in Huntsville**, Huntsville, AL **Coastline Community College**, Fountain Valley, CA **Dakota State University**, Madison, SD **Pace University**, New York, NY **Purdue University Northwest**, Hammond, IN **Dark Enterprises** **Alabama Connections Academy Niswonger Online**

Initiative: Workforce Development Pilot, Certificate, Curriculum and Research Coalitions

Workforce Certificate Programs: • Target groups are primarily transitioning military or first responders • Each pilot will focus on a specific sector and engage with industry • Curriculum development: list in Resource Directory and optional Clark • Topics: AI, quantum computing, cybersecurity and threat hunting, robotics automation analysis	
The overall goal is to establish a best practice, nationally scalable and sustainable certificate-based program with verifiable credentialing to more rapidly expand the cybersecurity workforce as follows: (a) increase the number of qualified, skilled professionals; (b) support their transition to cybersecurity work roles in critical infrastructure sectors, with initial emphasis on transitioning military and first responders for the defense industrial base, financial services, and energy Critical Infrastructure sectors; and (c) provide CAE-C institutions access to curricular resources through the NCAE Resources Directory. In addition to overall program leadership and coordination, UWF will also target transitioning military and first responders with their Cybersecurity Workforce Development Program.	Lead: **University of West Florida**, Pensacola, FL **University of South Florida**, Cyber Florida, Tampa, FL **University of Houston**, Houston, TX **Augusta University**, Augusta, FL **Dakota State University**, Madison, SD **Eastern New Mexico University-Ruidoso Branch Community College**, Ruidoso, NM **Florida International University**, Miami, FL **Metropolitan State University**, Denver, CO **San Antonio College**, San Antonio, TX **University of Texas at San Antonio**, San Antonio, TX
The Cybersecurity Pathways Coalition (CPC) will develop and pilot a certificate-based workforce-development program, focusing on cybersecurity for the healthcare industry. This program will be implemented in the academic year, commencing in Fall 2021. This "Healthcare Cybersecurity Certificate" will be awarded to applicants upon completion of a series of instructor-led online cybersecurity courses incorporating technology industry badges and experiences focused on healthcare systems.	Lead: **University of Louisville**, Louisville, KY **University of Arkansas at Little Rock**, Little Rock, AR **University of North Florida**, Jacksonville, FL **Bluegrass Community and Technical College**, Lexington, KY **Owensboro Community and Technical College**, Owensboro, KY

Proposed Activities

The consortium proposes to create a pilot certificate-based apprentice training program to train a large number of transitioning military, first responders, and other adult trainees to enter into the IT and cybersecurity industry. The consortium's three goals are:
1) Recruit 425 training participants, primarily from transitioning military and first responders.
2) Develop open accessible hands-on-based AI-Cybersecurity course curriculum with flexibilities for trainees to choose a training track that fits their educational background and career needs.
3) Offer AI-Cybersecurity training with online delivery that can accommodate the large number of target trainees' work schedules and locations.
Industry sector focus: Energy

Coalition

Lead: **Purdue University Northwestern**, Hammond, IN
Ivy Tech Community College (ITCC), Indianapolis, IN
University of North Carolina at Charlotte (UNCC), Charlotte, NC
University of Tennessee at Chattanooga (UTC), Chattanooga, TN

FY20-22 NCAE-C Research Grants

Twenty-eight academic institutions received cybersecurity research grants with FY2020 Congressional add-on funding. Several of these schools received funding in recognition of their status as a Minority Serving Institution, based on Congressional guidance. MSI status is included below.

Institution	State
Columbus State University	GA
Dakota State University	SD
Florida Atlantic University	FL
Indiana University of Pennsylvania	PA
Mississippi State University*	MS
Northeastern University	MA
Stevens Institute of Technology	NJ
Tennessee Tech University	TN
University of Alabama in Huntsville	AL
University of Arkansas	AR
University of Delaware	DE
University of Missouri	MO
University of New Haven	CT
University of North Texas	TX
University of South Carolina	SC
University of Tennessee at Chattanooga	TN
University of Wisconsin-Stout	WI

Institution	State	MSI Status
Florida International University	FL	HSI
Howard University	MD	HBCU
LeMoyne-Owen College	TN	HBCU
Morgan State University	MD	HBCU
North Carolina A&T University	NC	HBCU
Polytechnic University of Puerto Rico	PR	HSI
Stillman College	AL	HBCU
Tuskegee University	AL	HBCU
University of California (Irvine)	CA	AANAPISI & HSI
University of Texas at San Antonio	TX	HSI
University of Washington	WA	AANAPISI

In the higher education system of the United States, minority-serving institutions (MSIs) make up a category of colleges and universities based on either historical origin or enrollment criteria. MSIs occupy a unique place in the nation, serving primarily low-income students, first generation students, and students of color.

Unlike MSIs defined by demographics, HBCUs (and Tribal Colleges) began in response to a history of inequality and lack of access for people of color to majority institutions. See the Department of the Interior website for more information: https://www.doi.gov/pmb/eeo/doi-minority-serving-institutions-program.

- Historically Black Colleges and Universities (HBCU) – include 91 four-year and 17 two-year institutions of higher education established prior to 1964, for the primary purpose of educating African-Americans. A majority of the 102 HBCUs are located in the Southeastern states, the District of Columbia, and the Virgin Islands. HBCUs comprise 3 percent of America's institutions of higher education, yet enroll 16 percent of all African-American students, and award 24 percent of all baccalaureate degrees earned by African-Americans.

- Predominantly Black Institutions (PBI) – institutions that do not meet the definition of HBCU, but at least 50 percent of undergraduates receive Title IV assistance and 40 percent of student population is African American.

- Hispanic-Serving Institutions (HSI) – at least 50 percent of undergraduates receive Title IV needs-based assistance and Hispanic students constitute at least 25 percent of the student population.

- Asian American- and Native American Pacific Islander-Serving Institutions (AANAPISI) – at least 50 percent of undergraduates receive Title IV needs-based assistance and at least 10 percent of the student population is Asian American or Native American Pacific Islander.

* Mississippi State University leads a coalition including four MSI institutions for this research project.


NCS
NATIONAL
CRYPTOLOGIC
SCHOOL