The **Initiatives Guide** 2022

National Centers of Academic Excellence IN CYBERSECURITY

WWW.CAECOMMUNITY.ORG

Table of Contents

NCAE-C INITIATIVES POC QUICK REFERENCE LIST

Initiative	Lead Institution	Point of Contact	Email Address
CAE-C Community	California State University, San Bernardino	Tony Coulson	tcoulson@csusb.edu
CAE-C Community **Southwest Regional Hub**	San Antonio College	Kim Muschalek	kmuschalek@alamo.edu
CAE-C Community **Northwest Regional Hub**	University of Colorado Colorado Springs	Dr. Gretchen Bliss	gbliss@uccs.edu
CAE-C Community **Southeast Regional Hub**	University of West Florida	Eman El-Sheikh	eelsheikh@uwf.edu
CAE-C Community **Midwest Regional Hub**	Moraine Valley Community College	Stanley Kostka	kostkas@morainevalley.edu
CAE-C Community **Northeast Regional Hub**	Capitol Tech University	Dr. Bill Butler	whbutler@captechu.edu
CAE-C Community **CAE-CD Community of Practice**	Nova Southeastern University Detroit Mercy University	Dr. Yair Levy Dr. Ann Kohnke	levyy@nova.edu
CAE-C Community **CAE-CO Community of Practice**	Texas A&M University Cedarville University	Dr. Drew Hamilton Dr. Seth Hamman	hamilton@cci.msstate.edu shamman@cedarwille.edu
CAE-C Community **CAE-R Community of Practice**	Stevens Institute of Technology Northeastern University	Dr. Susanne Wetzel Dr. Agnes Chan	swetzel@stevens.edu, ag.chan@northeastern.edu
Candidates/Peer Review	Whatcom Community College	Corrinne Sande	csande@whatcom.edu
KU Management	University of Houston	Art Conklin	waconklin@uh.edu
Curriculum Task Force	Towson University	Sidd Kaza	skaza@towson.edu
Faculty Development	Dakota State University	Josh Pauli	josh.pauli@dsu.edu
Faculty Development **CAE-C in Cybersecurity Education Innovation**	University of Colorado Colorado Springs	Gurvirender Tejay	gtejay@uccs.edu
Workforce Development	University of Louisville	Dr. Sharon Kerrick	sharon.kerrick@louisville.edu
Workforce Development	University of West Florida	Dr. Eman El-Sheikh	eelsheikh@uwf.edu
Workforce Development	Purdue University Northwest	Dr. Michael Tu	Michael.Tu@pnw.edu
Community Development **Inland Empire Cybersecurity Initiative**	California State University, San Bernardino	Tony Coulson	tcoulson@csusb.edu
Community Development **The 502 Project**	University of South Florida	Nathan Fisk	fisk@usf.edu
Community Development **Initiatives to Contribute to a Culture of Cybersecurity**	University of Texas at San Antonio	Gregory White	greg.white@utsa.edu
Community Development **NW Region Cybersecurity Risk Management and Roadmapping**	Portland State University	Birol Yesilada	yesilada@pdx.edu

NCAE-C INITIATIVES POC QUICK REFERENCE LIST

Initiative	Lead Institution	Point of Contact	Email Address
Community Development **Virginia Cyber Navigator Internship Program**	University of Virginia	Jack W. Davidson	jwd@virginia.edu
Community Development **Regional Coalition for Critical Infrastructure**	Iowa State University	Doug Jacobson	dougj@iastate.edu
Community Development **NC Partnership for Cybersecurity Excellence**	North Carolina State University	Laurie Williams	lawilli3@ncsu.edu
Community Development **Improving Indiana's Local Cybersecurity Infrastructure**	Purdue University	Mat Trampski	mtrampski@purdue.edu
Community Development **Cybersecurity Education for Critical Infrastructure Protection**	University of Memphis	Dipankar Dasgupta	dasgupta@memphis.edu
NCAE Cyber Games	Mohawk Valley Community College	Jake Mihevc	jmihevc@mvcc.edu
Evidencing Competency Oversight	Norwich University	Karen Hinkle Dr. Sharon Hamilton	khinkle@norwich.edu shamilto@norwich.edu
Student Professional Development	Montreat College	Kelli Burgin	kelli.burgin@montreat.edu
K-12 **RING**	University of Alabama in Huntsville	Tommy Morris	tommy.morris@uah.edu
K-12 **RING Capacity Expansion**	University of Alabama in Huntsville	Jesse R. Hairston	jesse.hairston@uah.edu
K-12 **RING Out-Of-School Activities**	Moraine Valley Community College	John Sands	sands@morainevalley.edu
K-12 **RING Curriculum Expansion**	Brookdale Community Colelge	Michael Qaissaunee	mqaissaunee@brookdalecc.edu
K-12 - Teachers **Cybersecurity High School Innovations**	City University of Seattle	Morgan Zantua	zantuamorgan@cityu.edu
K-12 - Teachers **The National Cybersecurity Teaching Academy**	DePaul University	Dr. Filipo Sharevski	fsharevs@cdm.depaul.edu
K-12 - Teachers **The National Cybersecurity Teaching Academy**	University of Arkansas at Little Rock	Philip Huff	pdhuff@ualr.edu
K-12 - Teachers **The National Cybersecurity Teaching Academy**	University of Louisville	Adel Elmaghraby	adel.elmaghraby@louisville.edu
K-12 - State Outreach **Cybersecurity Education Innovation 2021**	Moraine Valley Community College	Charles Bales	bales@morainevalley.edu
K-12 - State Outreach **Regional Hubs Collaboration with States' DOEs for the NW Region**	University of Washington Bothell	Dr. Marc Dupuis	marcjd@uw.edu
CEDI	Fordham University	Dr. Thaier Hayajneh Dr. Amelia Estwick	thayajneh@fordham.edu aecedi@fordham.edu

INTRODUCTION

National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, managed by the National Security Agency (NSA), designates cybersecurity educational programs as Centers of Academic Excellence in Cybersecurity. Colleges and universities may apply for this designation by meeting rigorous standards of quality within their cyber defense, cyber operations, or cyber research programs. Those academic institutions that hold a designation from the NCAE-C program all belong to the Centers of Academic Excellence in Cybersecurity Community (CAE-C Community).

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, CISA partners with the NSA to sponsor the NCAE-C program. CISA offers a wealth of resources and leadership to the cybersecurity education community. Visit the National Initiative for Cybersecurity Careers and Studies (NICCS) at niccs.us-cert.gov for more information.

- **The Federal Bureau of Investigation (FBI) -** FBI joined the NCAE-C partnership in 2019 to co-sponsor the Cyber Operations program. FBI Instructors provide resources and expertise 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, NICE has been a close partner since its inception. NICE sponsors the annual CAE-C Community Symposium in concert with the annual NICE Conference. The programs collaborate closely on the NICE Cybersecurity Workforce Framework (NCWF). The NCAE-C academic requirements directly map to the NCWF, and NCAE-C competency-based education initiatives tie directly to the NCWF work roles.

- **The National Science Foundation (NSF) -** NSF cybersecurity education programs are closely aligned with the NCAE-C program. NSF has funded several grants at CAE-C academic institutions that directly support the program. The NCAE-C Candidates Program is based on a mentoring initiative started by NSF, providing mentors for institutions during their application process to become designated as a CAE. NSF co-sponsors the CyberCorps Scholarship For Service program, which awards scholarships to students at CAE-C designated institutions.

Thanks to Congressional funding add-ons provided in FY2020 and FY2021, the NCAE-C program awarded grants to coalitions of NCAE-designated schools to expand the reach of cybersecurity education funding K-12 outreach, faculty professional development, cybersecurity research, and other academic programs. In 2020, it put out the call for CAE-C schools 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. **This guide provides a summary of the programs and initiatives made possible by these federal grants.**

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.

There are 417+ institutions designated by the NCAE-C. For more information on the program, contact the NCAE-C program office by email at caepmo@nsa.gov, or visit public.cyber.mil/ncae-c or www.caecommunity.org.

The NCAE-C program and the CAE-C Community sincerely appreciate the support from Congress and federal partners as well as the commitment and expertise demonstrated by participating academic institutions.

PROGRAM SUPPORT

Institutions that aid in the management of the NCAE-C program to ensure organization and smooth functioning for the 417+ institutions within the CAE-C Community and the continued growth of the program.

PROGRAM SUPPORT

CAE in Cybersecurity Community National Center

Lead Institution: California State University, San Bernardino
POC: Dr. Tony Coulson
Email: tcoulson@csusb.edu
More Information: www.caecommunity.org

In 2019, California State University, San Bernardino (CSUSB) received a grant to establish the CAE in Cybersecurity Community, National Center to support and centralize functions of the CAE-C Community. Focused on the development of a robust cybersecurity workforce, the CAE-C Community National Center offers three primary functions to the 417+ CAE-C institutions and projects:

1. Engages and facilitates strategic initiatives for the Nation in the areas of research, student and faculty development, diversity, and other workforce development activities
2. Provides a portal of CAE-C resources for the community, geographic regions, and the Nation as a whole
3. Provides technical and logistical support for CAE events, activities, and curriculum

Components

Communities of Practice. The complexity of a cybersecurity workforce requires an ever-changing range of skills. The CAE-C Community National Center directly supports three CAE-C Communities of Practice, focusing efforts on cyber defense (CAE-CD), cyber operations (CAE-CO), and research (CAE-R). 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.

- **CAE Community of Practice – Cyber Defense:** Nova Southeastern University
- **CAE Community of Practice – Cyber Operations:** University of Mississippi
- **CAE Community of Practice – Research:** Northeastern University, Stevens Institute of Technology

CAE-C Regional Hubs. To coordinate and expand cybersecurity workforce initiatives throughout the country, the CAE-C Community National Center directly funds and supports five geographic areas, known as CAE-C Regional Hubs (CRHs).

These hubs are managed by a lead CAE-C institution or a consortium of institutions within that region:

- **Northeast Regional Hub:** Capitol Technology University, Mohawk Valley Community College, and Towson University
- **Southeast Regional Hub:** The University of West Florida, University of South 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

PROGRAM SUPPORT

CAE Candidates Program National Center (CNC)

Lead Institution: Whatcom Community College
POC: Corrinne Sande
Email: csande@whatcom.edu
More Information: ncyte.net/cae-program, caecommunity.org/about-us/cae-communities-practice

The CAE Candidates Program National Center acts as the entry point for all colleges and universities that plan to apply for either Academic Validation or NCAE-C Designation. This Center provides mentoring, resources, advice, and other support to colleges and universities that want to earn the NCAE-C designation. Additional services include validating academic programs as the first step in the process.

Whatcom Community College is home to the National Cybersecurity Training & Education Center (NCyTE), funded by the National Science Foundation's Advanced Technical Education (ATE) program as a National Center. Applicants benefit from both NCAE-C program and NCyTE resources and expertise. The centers are focused on expanding cybersecurity education to meet national workforce needs.

CAE Peer Review National Center

Lead Institution: Eastern New Mexico University - Ruidoso Branch Community College
POC: Stephen Miller
Email: stephen.miller@enmu.edu

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. Eastern New Mexico University - Ruidoso Branch 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.

QUALITY & EFFICACY INITIATIVES

Programs and projects that ensure academic excellence through knowledge unit management, faculty development, curriculum development, and resource development.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

With a critical shortage of cybersecurity professionals available to teach and perform faculty duties in cybersecurity, these initiatives seek to recruit, train, and/or upskill cybersecurity faculty. Their objectives are to:

- Expand the knowledge and teaching qualifications of existing faculty
- Recruit and train private and public industry professionals to full-time cybersecurity faculty members
- Recruit graduate students, particularly PhD candidates, to teach in cybersecurity
- Recruit military and civil service personnel transitioning from government cybersecurity work roles

University of Colorado Colorado Springs (UCCS) and Dakota State University (DSU) lead two different coalitions of 20 institutions working in coordination to support faculty development.

CAE in Cybersecurity Education Innovation (Awarded in FY 2020)

Lead Institution: University of Colorado Colorado Springs
POC: Dr. Gurvirender Tejay
Email: gtejay@uccs.edu
More Information: business.uccs.edu/CAEC-facdev

Initiative Description

UCCS serves as the lead institution for the consortium of educational institutions delivering a comprehensive, programmatic approach to cybersecurity faculty development. The coalition provides cybersecurity education and training to over 1,700 participants within faculty roles. This includes existing faculty, professors of practice, doctoral candidates, transitioning military, and transitioning civil services personnel. The partnership of academic institutions includes 10 prominent participants in cybersecurity instruction, ranging from community colleges to major research universities.

The partnering institutions collectively expand the knowledge and teaching qualifications of 1,335 faculty. This is accomplished by recruiting and training existing faculty through cybersecurity teaching workshops, courses, boot camps on tools and techniques, industry certifications, and program development workshops. Additionally, the coalition partners with the Cybersecurity Management Council to engage 100 institutions, by developing cybersecurity management programs and providing mentorship to 300 faculty members.

The consortium is recruiting 200 industry cybersecurity experts with existing credentials and/or a graduate degree. Approved candidates are then trained on pedagogy, curriculum development, and soft skills classroom dynamics. Taking current professionals in the cybersecurity field, providing them with an understanding of the 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-C institutions.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Graduate and doctoral students can supplement their education by taking online cybersecurity graduate certificate programs offered by select partners. The graduate certificate program actively recruits 250 graduates and doctoral students. Students are given access to pedagogical training which prepares them for a remarkably effective career in higher education. Students complete the program fully prepared to teach cybersecurity courses. Our Quality and Efficacy Initiatives will also provide scholarship opportunities, career guidance, and access into a placement program.

Accepted candidates have access to a Cybersecurity Capstone Field Trip, a live case study and educational trip, focused in the Washington D.C. and Colorado cybersecurity ecosystems. These trips allow students to experience the cybersecurity practice from a government or private sector vantage point, giving students a glimpse into a cybersecurity practitioner's day-to-day activities.

A similar initiative titled the Virtual Cybersecurity Teachers program, prepares graduate and doctoral students for education in high schools, community colleges, and online courses. The program brings practical experience to the graduate programs and adds to the availability of qualified faculty in community college cybersecurity programs.

The coalition is recruiting 267 transitioning military and civil service personnel, providing them with pedagogical training in becoming effective educators and works to prepare them for future careers in higher education. This initiative aims to develop 'Military Occupation Specialties (MOS) Pathways' program to award credits based on military occupation. This serves as an innovative approach to attract and recruit transitioning military personnel for cybersecurity faculty development. The military occupations are mapped to specific courses that correspond to general and industry certifications.

CAE in Cybersecurity Education Innovation Partners

Partner Institution: Arizona State University
POC: Dr. Brian Gerber
Email: Brian.Gerber@asu.edu

Description

Offers faculty development opportunities in the specific area of emergency management and homeland security by examining their intersection with cybersecurity issues. Faculty participants in this initiative also have access to two free courses in these same content areas. Finally, prospective students will receive scholarship awards to enroll in a graduate certificate in emergency management. 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 and risks.

Partner Institution: Florida International University
POC: Dr. Alexander Perez-Pons
Email: aperezpo@fiu.edu

Description

Focuses on Digital Forensics consisting of two workshops, four courses, and accompanying boot camps to build fundamental knowledge and exposure to industry standard tools and techniques. The courses are to assist cybersecurity faculty in gaining expertise in Digital Forensics, expanding their capability, and promoting research.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Partner Institution: Moraine Valley Community College
POC: Dr. John Sands
Email: sands@morainevalley.edu

Description

Provides faculty development workshops aligned to highly recognized industry credentials and emerging technologies. Courses include CISSP, CISA, CEH, Security+, CCNA Security Operations, Palo Alto Security Fundamentals, and Linux Professional Institute. Each course includes instructional best practices along with suggested content, activities, and assessment tools. These workshops provide institutions with the ability to improve faculty knowledge, skills, and abilities.

Partner Institution: National CyberWatch Center
POC: Dr. David Tobey
Email: dtobey@nationalcyberwatch.org

Description

Conducts Train-the-Trainer workshops, employing a fully online delivery model. The workshop topics provide the necessary IT foundation upon which existing faculty, doctoral students, and transitioning military personnel can leverage to further increase their capability in future cybersecurity course or workshop offerings delivered by other partners.

Partner Institution: Robert Morris University
POC: Dr. Lawrence Tomei
Email: tomei@rmu.edu

Description

Designs and teaches the workshop titled: Pedagogy and Technology for Cybersecurity Teaching. This workshop prepares cybersecurity professionals to teach cybersecurity at a post-secondary education level, with an emphasis in three areas: integration of technology, development and evaluation of cyber curriculum, and educational leadership.

Partner Institution: University at Albany, SUNY
POC: Dr. Sanjay Goel
Email: goel@albany.edu

Description

Trains faculty and students in Digital Forensics and Information Security Risk and Policies. Each of the courses are packaged with teaching materials, including presentations, videos, assignments, and assessments. The courses are for faculty looking to gain further expertise in these areas. There will also be workshops to help transition course materials to faculty. Additionally, students will be given scholarships to complete their certificate program with a pathway towards masters degrees and PhDs.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Partner Institution: University of Cincinnati
POC: Dr. Chengcheng Li
Email: li2cc@ucmail.uc.edu

Description

Creates a series of connected education programs to train a diverse population, ranging from existing faculty, PhD students, military and government personnel, and IT professionals to teach cybersecurity curricula. Two graduate certificates are being created to target instructors with different needs. The Graduate Certificate for Teachers and Instructors, which prepares students to teach entry-level cybersecurity courses; and the Data Driven Cybersecurity (DDC) graduate certificate, consisting of four cybersecurity courses. To further expand the impact of the project, two online courses and workshops are being conducted to train faculty on selected DDC topics.

Partner Institution: University of New Mexico
POC: Dr. Xin Luo
Email: xinluo@unm.edu

Description

Provides two online cybersecurity teaching courses and two hybrid courses for faculty career development. Additionally, providing scholarship support to graduate students, doctoral students, and military personnel without cybersecurity credentials to pursue the Information Assurance Graduate Certificate. Program details are carefully tailored for transitioning military and civil service personnel.

Partner Institution: Whatcom Community College
POC: Corrinne Sande
Email: CSande@whatcom.edu

Description

Provides faculty development workshops for colleges and universities that want to start a cybersecurity program or enhance an existing program with cybersecurity-related content. This project also addresses mapping military occupation specialties (MOS) to credit at colleges and 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.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Cybersecurity Faculty Development (Awarded in FY 2020)

Lead Institution: Dakota State University
POC: Dr. Josh Pauli
Email: josh.pauli@dsu.edu

Initiative Description

Dakota State University (DSU) serves as the lead institution for a consortium of educational institutions, each of which manages portions of the overall initiative of Cybersecurity Faculty Development, with special attention to scaling nationwide.

Programs developed by the consortium aim to expand the knowledge and teaching qualifications of existing faculty. Additional objectives are to recruit and prepare professors of practice from industry, from graduate and PhD programs, and transitioning military and civil service personnel to teach cybersecurity.

Cybersecurity Faculty Development Partners

Partner Institution: University of Texas at San Antonio
POC: Glenn Dietrich
Email: glenn.dietrich@utsa.edu

Description

Recruiting Transitioning Military and Civil Service Personnel – Recruits military and civilian personnel retiring from their current employment to have a career teaching cybersecurity in an academic institution. The project also concentrates on current military and civilian employees who want to work in academia part-time. Discussions with the major cybersecurity commands are integral to the process.

Partner Institution: University of North Texas
POC: Ram Dantu
Email: ram.dantu@unt.edu

Description

Recruit Graduate Students to Expand Faculty Numbers in Cyber – Hosts mentoring and training readiness activities for industry professionals and PhD students, in order to produce well-qualified faculty capable of teaching, inspiring, and engaging the next generation of cybersecurity professionals.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Partner Institution: Metropolitan State University
POC: Faisal Kaleem
Email: faisal.kaleem@metrostate.edu

Description

Minnesota Cyber Range and SOC Workshops – Provides professional development opportunities for existing cybersecurity faculty from colleges and universities and exposes 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 – Recruits interested cybersecurity subject matter experts from industry, leveraging the MN Cyber Institute's partner network and other organizations across the nation.

Partner Institution: University of West Florida
POC: Tirthankar Ghosh
Email: tghosh@uwf.edu

Description

Scenario-based Teaching Workshops – Provides workshops to existing university and college faculty to prepare them for scenario-based teaching and integrating scenarios into their curricula.

Veteran Recruitment Program – Establishes a recruitment program to identify veterans with appropriate experience and expertise, in order to provide them with relevant pedagogical and technical knowledge and skills to teach in designated and candidate CAE-C institutions.

Partner Institution: San Antonio College
POC: Kim Muschalek
Email: kmuschalek@alamo.edu

Description

Department of Defense-recognized IT Industry Certifications, with a Focus on Security+ — Prepares at least 25 existing cybersecurity faculty for leading their institutions' NCAE-C designation. SAC is also identifying at least 10 veterans or active duty military members who are employed in cybersecurity roles and have an interest in teaching cybersecurity. Over the grant period, SAC will help transition at least five of these individuals to adjunct or tenured positions at current or prospective CAE-C schools 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.

Partner Institution: University of Alabama in Huntsville
POC: Tommy Morris
Email: tommy.morris@uah.edu

Description

Concurrently Teaching Faculty and Students SCADA Security with Massive Online Academy – Teaches for credit online SCADA cybersecurity classes to students and faculty at UAH and university partners. Class enrollment across all participating universities is capped at 500 participants.

CYBERSECURITY FACULTY DEVELOPMENT INITIATIVES

Partner Institution: Moraine Valley Community College
POC: Dr. John Sands
Email: sands@morainevalley.edu

Description

Industry Certification Train-the-Trainer Workshops – The National Center for Systems Security and Information Assurance (CSSIA) Teaching and Learning Academy (Train-the-Trainer) is providing 10 workshops, serving 15-20 faculty members each. Each workshop will be aligned to recognize industry credentials, emerging technologies, and popular products. Courses include CISSP, CISA, CEH, Security+, CCNA Security Operations, Palo Alto Security Fundamentals, and Linux Professional Institute. Other workshops may include VMware, EMC, and Meraki.

Pedagogical Support via the National Academy – The CSSIA team provides pedagogical support systems through the National Academy, to include instructional best practices, suggested content, suggested 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.

Partner Institution: Dakota State University
POC: Kyle Cronin
Email: kyle.cronin@dsu.edu

Description

CAE Faculty Workshops – Hosts workshops that will have five separate topics from which attendees can select based on survey results from the Community. Each workshop will have five separate topics, hosting 30 CAE faculty each, totaling 150 participants per workshop. Two instructional staff lead each group of 30 participants through the exercises 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 hands-on tutorials on how to set up and execute each lesson.

CURRICULUM RESOURCES & DEVELOPMENT INITIATIVES

Consolidated CAE-C Professional Development Resources (Ethics & Professionalism for Students) Initiative (Awarded in FY 2020)

Lead Institution: Montreat College
POC: Kelli Burgin
Email: kelli.burgin@montreat.edu

Initiative Description

Montreat College leads this initiative to create consolidated CAE-C Professional Development Resources to provide all students in a CAE designated program with insight into careers in cybersecurity, professional behavior and ethics, and other soft skills in demand in the workplace. This initiative leans on contributions from other CAE-C Community schools, as well as government and industry professionals. These materials are intended for CAE-C schools and students.

1. Developing a Cybersecurity Ethics Book and Curricula

- Creates content, to include the creation of a cybersecurity oath
- Expansion of ethics within the cyber industry and training
- Inclusion of cyber case studies
- Inclusion of classical and modern ethical frameworks
- The application of Just War Theory into cybersecurity

Cybersecurity Ethics Book Advisory Group Partners

- **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

Curriculum Development Partners

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

2. Developing a Pilot Program for Professionalism and Soft Skills Curriculum

Creates a curriculum that emphasizes the importance of experiential learning and the resulting development of abilities and characteristics desired by employers across disciplines including critical thinking, problem solving, collaboration, and interpersonal skills. After the pilot program launched at Montreat College during the Fall 2021 semester, instructors and instructional designers are refining materials and creating a guidebook to share.

CURRICULUM RESOURCES & DEVELOPMENT INITIATIVES

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

- **Marie Wisner, PhD**
  Associate Dean for Calling and Career, Montreat College Thrive Cente
- **Greg Sayadian, MS**
  Assistant Professor of Cybersecurity, Montreat College

3. Producing Cybersecurity Career Videos

Creates a video library that features videos about individuals currently working in prevalent and/or emerging entry-level cybersecurity work roles. The videos aim to give the audience an understanding of life in that work role from an applied perspective someone who's doing it.

Chair Career Pathways Team

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

4. Directory of Materials and Creating Additional Materials

Publishes an online, continuously-modifiable directory of resources already in use by the CAE-C Community. CAE-C institutions will be able to submit listings for their own materials in the categories of critical thinking/problem-solving, teamwork/collaboration, professionalism/work ethic, oral/written communications, leadership, global/multicultural fluency, ethical judgement/decision-making, and career paths/management.

Chair Directory of 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
- **Anne Kohnke, PhD**
  Associate Professor of Cybersecurity, The University of Detroit Mercy
- **Vickie (Valerie) McLain**
  Cybersecurity Instructor, Alexandria Technical & Community College
- **Stephen Miller**
  Professor, Director Cybersecurity Center of Excellence, Eastern New Mexico University–Ruidoso Branch Community College

5. Dissemination of Curricula and Other Materials

Hosts workshops to enhance collaboration, conduct group review of materials, and train the trainers so that the CAE-C Community can take ownership and leverage the aforementioned materials.

Co-Chairs of the Dissemination Subcommittee

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

CURRICULUM RESOURCES & DEVELOPMENT INITIATIVES

Knowledge Unit Expansion Program (Awarded in FY 2021)

Lead Institution: University of Houston
POC: Dr. Art Conklin
Email: waconklin@uh.edu

Initiative Description

Knowledge Units (KU), are mandatory topics and associated objectives that must be included in an institution's degree or certificate program. The University of Houston is leading a coalition of CAE-C institutions to examine the existing KUs in the inventory to look for shortfalls, gaps, and deficiencies, with the objective to develop changes and create new KUs to address these issues, while supporting newer and broader areas of cybersecurity education. This is a comprehensive review of KUs, with an eye towards how they help define the knowledge, skills, and competencies needed in the cybersecurity workforce, both today and into the future.

The initiative will deliver the following to the CAE-C Community:

- An updated set of KUs with better documentation of learning objectives, making them easier to incorporate into curricula
- An expanded set of KUs covering new areas, such as AI, data analytics, Computer Science in Law and Medicine, IoT, Big Data, cybersecurity intelligence, and policy formation
- Connecting the KUs so that they align with the NICE Cybersecurity Workforce Framework (NCWF)
- The addition of competency elements within KUs to support advanced skill development

KU Expansion Program Partners

Partner Institution: Texas A&M University
POC: Dr. Drew Hamilton
Email: hamilton@tamu.edu

Partner Institution: Cedarville University
POC: Dr. Seth Hamman
Email: shamman@cedarville.edu

Partner Institution: Metropolitan State University
POC: Dr. Faisal Kaleem
Email: faisal.kaleem@metrostate.edu

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

CURRICULUM RESOURCES & DEVELOPMENT INITIATIVES

Cybersecurity Curriculum Task Force (Awarded in FY 2021)

Co-Lead Institution: Towson University
POC: Dr. Sidd Kaza
Email: skaza@towson.edu

Co-Lead Institution: Portland Community College
POC: Cara Tang
Email: cara.tang@pcc.edu

Initiative Description

Building a cyber-skilled workforce is critical to the continued security of the nation across social, economic, and political domains. Building such a workforce requires creating high-quality and relevant cybersecurity curricula in concert with efforts in faculty and workforce development, curricular guidelines, and other initiatives across the K-16 pipeline. Towson University is leading this curriculum task force to act as the Curriculum Committee for the NCAE-C program. The charter of the task force is to inventory, audit, analyze, and develop curricula to assist in creating a cyber-ready workforce.

Learning from the model of the Solarium Commission (www.solarium.gov), this task force will consist of four subcommittees: Reconnaissance, Gap Analysis, Construction, and Alignment.

This effort will synthesize existing and ongoing curriculum development initiatives and further the development of high-quality and relevant curriculum in filling the cybersecurity workforce shortage.

The subcommittees will:

- Assess the curricular needs of cybersecurity knowledge, tasks, abilities, competencies, skills (KTACS) aligned with the NICE Cybersecurity Workforce Framework (NCWF) and NCAE-C knowledge units
- Conduct a meaningful analysis of available curricula, their levels, depth, and recency
- Develop high quality and relevant curricula

Products of the subcommittees include CARD and CLARK. CARD refers to the Centers of Academic Excellence in Cybersecurity Resource Directory. CARD maintains a categorized collection of cybersecurity education resources developed by members of the cybersecurity community. Through the National Cryptologic Foundation, the National Security Agency funded the CARD system to provide CAE institutions, government organizations, and industry groups with cybersecurity education resources.

CARD's mission is to help produce high-quality cybersecurity professionals within the United States by providing high-quality and relevant resources.

CLARK, the Cybersecurity Labs and Resource Knowledge-base, is a platform for building and sharing free cybersecurity curricula. It includes a model for building curriculum, the digital library system, and distinct curriculum collections.

CLARK fulfills a demonstrated need for a high-quality and high-availability repository for curricular resources for the cybersecurity education community. It provides cybersecurity educators with the building blocks to train the next wave of researchers and better prepare the cybersecurity workforce.

CURRICULUM RESOURCES & DEVELOPMENT INITIATIVES

Cybersecurity Curriculum Task Force Partners

Partner Institution: Metropolitan State University
POC: Dr. Faisal Kaleem
Email: faisal.kaleem@metrostate.edu

Description

Metropolitan State University (MSU) co-leads the curriculum gap analysis subcommittee. The school will provide program leadership and management at MSU, establish and carry out program goals, policies, and procedures, direct and oversee program financial and budgetary activities, and serve as the program POC.

Partner Institution: Cedarville University
POC: Dr. Seth Hamman
Email: shamman@cedarville.edu

Description

Cedarville University co-leads the reconnaissance subcommittee, whose goal is to define a process and complete a comprehensive search for available curricula on cybersecurity repositories and directories within the CAE-C Community and the on-going initiatives.

Partner Institution: United States Naval Academy
POC: John Doherty
Email: jjdohert@usna.edu

Description

The United States Naval Academy (USNA) is leading the effort of the alignment sub-committee, a cross-cutting sub-committee to keep abreast with the changing knowledge units, competencies, and other standards important to the NCAE-C community and designations.

Partner Institution: University of West Florida
POC: Dr. Tirthankar Ghosh
Email: tghosh@uwf.edu

Description

University of West Florida (UWF) co-leads the curriculum gap analysis subcommittee. UWF will provide program leadership and management, establish and carry out program goals, policies, and procedures, oversee program financial and budgetary activities, and serve as a program POC.

Partner Institution: Coastline Community College
POC: Tobi West
Email: twest@coastline.edu

Description

Coastline Community College serves as co-chair of the construction subcommittee to guide the development of curricula across at least six new subject areas with an emphasis on emerging needs.

COMPETENCY DEVELOPMENT INITIATIVES

Programs and projects that give cybersecurity students opportunities to practice the skills they have learned in cyber education programs.

CYBER COMPETITION INITIATIVE

The National Initiative for Cyber Education (NICE) states that cybersecurity competitions encourage skill development and ethical practice. Participants have access to mentoring with talent identification, skill building resources, flexible learning opportunities, and job opportunities. Utilization of such tools by participants and facilitators contributes to the knowledge-base of cybersecurity practitioners, curriculum development, and an increased interest for incoming cybersecurity educators. The Cybersecurity Competition Initiatives recognize these values and are building a program with the following goals:

- Increase the capacity of students across CAE-C Community programs to participate in cybersecurity competitions through tutorial and live-practice in virtual environments
- Provide a positive initial competition experience for students that enhances student engagement with their academic work
- Provide an opportunity for collaboration between CAE-C institutions through challenge design
- Enhance the sense of community among students and faculty in the NCAE-C program

NCAE Cyber Games (Awarded in FY 2020)

Co-Lead Institution: Mohawk Valley Community College
POC: Jake Mihevc
Email: jmihevc@mvcc.edu
More Information: www.ncaecybergames.org

Co-Lead Institution: University of South Florida
POC: Ron Sanders
Email: rpsanders@usf.edu

Initiative Description

NCAE Cyber Games is dedicated to inspiring a new generation of cybersecurity professionals to help address the complex challenges facing our nation. This initiative combines Mohawk Valley Community College's success in designing and hosting cybersecurity competitions with USF Cyber Florida's national program management and outreach expertise. These two leading institutions have united to create a new kind of cybersecurity competition, one that welcomes first-timers and recognizes the full spectrum of skills needed in the field. New competitors can learn about cyber competitions in an environment focused on teamwork, building confidence, and growing skills. A practice environment became available in the Spring of 2021.

Regional competitions are scheduled for February and March of 2022, with the National Finals event scheduled for April. CAE faculty and industry partners are 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-C Community.

CYBER COMPETITION INITIATIVE

NCAE Cyber Games Regional Partners

Northwest Regional Partner
Partner Institution: Highline College
POC: Amelia Phillips
Email: aphillips@highline.edu

Southeast Regional Partner
Partner Institution: University of West Florida
POC: Anthony Pinto
Email: apinto@uwf.edu

Midwest Regional Partner
Partner Institution: Davenport University
POC: Lonnie Decker | Mark McKinnon
Email: mdldecker@davenport.edu | mark.mckinnon@davenport.edu

Southwest Regional Partner
Partner Institution: National University
POC: Nancy Jones
Email: njones2@nu.edu

Northeast Regional Partner
Partner Institution: Westchester Community College
Partner Institution: University at Albany
POC: John Watkins | Sanjay Goel
Email: john.watkins@sunywcc.edu | goel@albany.edu

EVIDENCING COMPETENCY INITIATIVE

Competency is the ability for students to complete a task in the context of a work role. This initiative will develop framework models and processes for evidencing competency that can be implemented through the NCAE-C program. The activities will serve as a comprehensive review of current marketplace cybersecurity measurements, tools, and cyber competitions.

Evidencing Competency Oversight (Awarded in FY 2020)

Lead Institution: Norwich University
POC: Dr. Sharon R. Hamilton
Email: shamilto@norwich.edu

Initiative Description

Norwich University is leading the Evidencing Competency Oversight Initiative with a coalition of partner institutions working on simultaneous efforts, to include:

- **Regional Cybersecurity Exercises –** Norwich University Applied Research Institute (NUARI) designs, develops, and conducts two cyber exercises in each of the five CAE-C Regional Hubs over the 24 months of the grant period. NUARI is coordinating with the NSA and the CAE-C Regional Hubs to identify region-specific issues for each exercise and to identify the participating CAE institutions. NUARI is working with each Hub to market the exercises and train faculty facilitators from the institutions.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 center is to create a comprehensive resource for CAE-C institutions to replicate the model at their home institutions. The objectives are to:

  - 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
  - Identify tasks in SSC Work Roles and develop competency statements to evidence the students' ability to successfully complete the tasks(s)
  - 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 –** In existence since 2018 and formalized with the grant in 2020, this working group has grown to approximately 60 individuals, predominantly in academia and includes government and industry participants. It consists of three sub-working groups with the following purposes:

  - Sub-Working Group 1: Definitions and Documentation
  - Sub-Working Group 2: Competency Development and Measurement Tools
  - Sub-Working Group 3: Cybersecurity Competitions as Competency Development and Evaluation Tools

EVIDENCING COMPETENCY INITIATIVE

For the second year of the grant, the working group will refine and publicize the essential elements framework for evidencing competency that can be implemented throughout the NCAE-C program. The activities will also employ the essential elements framework to coordinate a comprehensive review of the marketplace of cybersecurity measurements, tools, and cyber competitions.

Evidencing Competency Oversight Partners

Partner Institution: California State University, San Bernardino
POC: Dr. Vincent Nestler
Email: vnestler@csusb.edu

Description

Sub-Working Group 1: Defines the framework, definitions, and terminology for evidencing competency in approved NCAE-C programs.

Partner Institution: Stevens Institute of Technology
POC: Dr. Susanne Wetzel
Email: swetzel@stevens.edu

Description

Sub-Working Group 2: Explores cybersecurity skills assessment tools, develop the rubric to evaluate each tool, provide a list of the tools and the evaluation results for each, and shares the working group's results with other NCAE-C institutions. This is executed through the INSuRE (Information Security Research and Education) project, which aims to build research skills and experience for graduate students through a research network between CAE-Rs (Centers of Academic Excellence in Cyber Research) in Information Assurance and Cyber Defense. Through the project, students engage in interdisciplinary, distributed-team research on tasks in the national information security domain. The students learn to research by doing; building skills, expertise, and connections that will enable them to hit the ground running faster on information assurance research projects later in their careers.

The project backs a project-based research class, offered simultaneously and online at multiple institutions in the network. Students may also participate in parallel as research assistants, through research experiences, or for research credit; while the vast majority of INSuRE students have entered through the class, several students have entered or stayed attached to the network through other means.

In the class, students bid on and propose work on problems that have been contributed by problem sponsors. Research teams are formed and check in with technical advisors at these sponsors. Teleconferencing technology is used to connect students in simultaneous class sessions for problem overviews, student presentations, and other resource presentations. Students prepare formal proposal and report documents, and learn to work with mentors (and sometimes teammates) who are not co-located.

Partner Institution: Expert consultant
POC: Dr. Daniel Manson (Professor Emeritus, Cal Poly Pomona)
Email: dmanson@cpp.edu

Description

Sub-Working Group 3: Identifies and explores student cybersecurity competitions. Identifies established cybersecurity competitions that provide students with development of measurable competencies and document the competencies developed during competition.

SENIOR MILITARY COLLEGE (SMC) CYBER INSTITUTES

(Awarded in FY 2020 and FY 2021)

Lead Institution: Norwich University
POC: Dr. Sharon R. Hamilton
Email: shamilto@norwich.edu

Initiative Description

The Department of Defense (DoD) 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 for near-term and future emerging cyber challenges. Development of talent is a critical component of DoD success in keeping ahead of adversaries, defending the U.S., and protecting national interests. The DoD SMC Cyber Institutes pilot program consists of Norwich University, The Citadel, Texas A&M University, University of North Georgia, Virginia Military Institute, and Virginia Polytechnic and State University.

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, live in a military environment constantly, and are subject to military discipline. The SMC must include the development of character through military training and the regulation of cadet conduct as an objective according to principles of military discipline.

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. Unlike other colleges where ROTC cadets are required to sign a contract to take commission before entering their final two years, taking a commission upon graduation remains optional for SMC cadets. Five of the six SMCs in the US are designated NCAE-C schools.

This initiative addresses a DoD requirement, and will be executed in partnership between the NCAE-C Program Office, the Office of Secretary of Defense R&E, and US Cyber Command. The objectives for the Cyber Institutes and those of the NCAE-C Evidencing Competency Working Groups are closely aligned. Achievements of one will support the other. There are seven approved Lines of Effort (LOE).

LOE 1: Develop SMC DoD Cyber Institutes (Phase I - FY 21)

- Hire and designate SMC Cyber Institute director and program support (two full-time employees per SMC)
- Increase cybersecurity, data science, and AI faculty (as required by SMC)
- Establish Cyber Leader Development Program (CLDP)

LOE 2: Build Governance and Assessment Framework/Processes (Phase II – FY 2022/2023)

- Conduct assessment reporting and demonstrations
- Establish government governance (Senior Steering Group; Steering Group)
- Establish SMC Governance Group (Norwich Program Manager, SMC Cyber Institute Directors)
- Develop SMC Cyber Institute Senior Advisors Board

SENIOR MILITARY COLLEGE (SMC) CYBER INSTITUTES

LOE 3a: Expand and Sustain Cyber Experiential Programs (Internal to SMCs) (Phase II – FY 2022/2023 ; Phase III – FY 2024)

- Use Security Operations Centers (SOC) at Norwich/Texas A&M University for cyber threat assessment and analysis experience
- Develop joint SMC cyber and faculty summer immersions for freshmen and sophomore students

LOE 3b: Expand and Sustain Cyber Experiential Programs (External) (Phase II – FY 2022/2023; Phase III – FY 2024)

- Develop and share DoD internship opportunities amongst the SMC Cyber Institutes
- Establish SMC Cyber Institute USCYBERCOM, NSA, and CSC internships
- Support unclassified intern programs at USCYBERCOM DreamPort facility

LOE 4: Entry Level Education programs at SMCs (Phase II – FY 2022/2023; Phase III – FY 2024)

- Build capacity for cyber programs – address current and projected skills gaps (people, process, technology)
- Incorporate NSA adjuncts into course development and instruction (Virtual)
- Incorporate cybersecurity certifications into SMC Cyber Institute cohort
- Link undergraduate research programs to USCYBERCOM problem sets and requirements

LOE 5: Recruit, Train, and Deploy RC SMC Deputy Directors (Phase II – FY 2022/2023; Phase III – FY 2024)

LOE 6: Tailored Strategic Retention (one-year Army Cyber Command pilot program) (Phase II – FY 2022)

- Execute pilot program to transition early/mid-career active-duty Army Cyber soldiers to the Reserve Forces
- Provide focused academic counseling and career transition services

LOE 7: Develop Export Model for New DoD Cyber Institutes (Phase III – FY 2024)

- Identify candidate NCAE-C and ROTC institutions
- Provide DoD Cyber Institute CLDP process and one-on-one mentorship from SMC Cyber Institutes to candidate institutes

COLLEGE & CAREER READINESS PATHWAYS

Programs and projects that offer students and secondary school teachers opportunities for cybersecurity education.

COLLEGE PATHWAYS INITIATIVES

Outreach to the community is a fundamental requirement for designation in the NCAE-C program, and outreach to high schools is particularly important for success in development of future professionals. NCAE-C efforts are focused primarily on providing college and career pathways to high school students interested in joining the cybersecurity workforce.

Regions Investing in the Next Generation (RING) (Awarded in FY 2020)

Co-Lead Institution: The University of Alabama in Huntsville
POC: Dr. Tommy Morris
Email: tommy.morris@uah.edu
More Information: caecommunity.org/initiative/k12-ring

Co-Lead Institution: Moraine Valley Community College
POC: Dr. John Sands
Email: sands@morainevalley.edu

Initiative Description

RING is a combined effort of two coalitions to establish a CAE-C college and career pathway. This effort provides an online cybersecurity fundamentals course, which targets rural, under-resourced school systems; home school students; and schools without an established cybersecurity program. While both coalitions have distinct roles, they present a unified presence to schools, students, and partners, with common administrative functions.

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

This includes:

- Shared project name with delineated responsibilities for each effort
- Shared "Contact Us" account for email, phone, and social media housed at the National Center
- Shared graphics designers for a uniform look
- Shared web page housed on the National Center's website
- Common course application and registration through the National Center's website

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. RING is designed to give the high school learner the best online cybersecurity learning experience. This high school cybersecurity fundamentals course is based upon the Cybersecurity Curriculum Guidelines (CCG) and NCAE-C Knowledge Units. The course is inclusive, and is designed to be accessible to special populations. Interactive games, a virtual career experience, a student honor society, and access to hands-on labs ensures a quality student experience.

RING is designed to remove barriers to learning. By partnering with existing, accredited online K-12 schools, students can easily earn high school credit for their learning. Qualifying low-income students will receive loaner laptops and Internet service, allowing students from home, rural, and

COLLEGE PATHWAYS INITIATIVES

technology-deprived schools an equal opportunity to learn. Additionally, students will have the option to earn transferrable credit to institutions within the consortium, and select CAE-C institutions that have opted into the program. RING includes a student organization and honor society that tie students to the cybersecurity community, while offering opportunities to complete service projects and conduct focused research. These opportunities include after-school and extracurricular learning, combined with a national business partnership.

The University of Alabama in Huntsville (UAH) Coalition

The UAH coalition leads curriculum development, instructs the online course for a national audience, and leads the student organization and honor society.

UAH RING Partners

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

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.

Partner Institution: Dakota State University
POC: Dr. Josh Pauli
Email: josh.pauli@dsu.edu

Description

Dakota State University (DSU) serves as the Northwest region partner. As a leader in K-12 education, they enhance the project by:

- Advising effective delivery methods
- Providing feedback to a curriculum's suitability and age-appropriateness
- Participating in credit transfer agreements

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

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.

COLLEGE PATHWAYS INITIATIVES

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

Description
Coastline Community College is leveraging their online instructional expertise to review online delivery methods and accessibility to 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.

K-12 Partner Organizations: Alabama Connections Academy, Niswonger Online, and the National Rural Education Association

Description
Alabama Connections Academy and Niswonger Online recruit students, host curriculum, and help with high school course accreditation. They facilitate collaborations with school counselors and negotiate adoption by other K-12 entities. The National Rural Education Association assists with recruitment efforts.

Partner Institution: Dark Enterprises
POC: Melissa Dark
Email: melissa.dark@darkenterprisesinc.com

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

Moraine Valley Community College (MVCC) Coalition

The MVCC coalition leads development of four-stage career pathways, virtual challenges, career planning, business partnerships, and competitions under the honor society.

MVCC RING Partners

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

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

COLLEGE PATHWAYS INITIATIVES

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

Description

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

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

Description

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

Partner Institution: Forsyth Technical Community College
POC: Tony Brown
Email: tbrown@forsythtech.edu

Description

Forsyth Technical Community College leads the effort to create, distribute, and manage the National Directory of Cybersecurity K12 Pipeline Programs. This includes organizing an annual college fair.

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

Description

Cal Poly Pomona supports the national after-school and extracurricular learning program. It also tracks enrollment and participation of these events. Included in this program is the K12 CyberTalk show (*K12cybertalk.org*); a webcast "for students by students" that is designed to increase interest in cybersecurity through peer engagement.

COLLEGE PATHWAYS INITIATIVES

CAE High School Feasibility Study (Awarded in FY 2020)

Lead Institution: Cyber Center for Education & Innovation
POC: Mark Loepker
Email: mloepker@cryptologicfoundation.org

Initiative Description

Is a High School Center of Academic Excellence program an advisable and feasible approach to further support the much-needed cybersecurity education to career pipeline?

To answer the questions of feasibility and advisability, the National Cryptologic Foundation (NCF), along with its partners, Dark Enterprises, and CAE-C institutions in good standing, Moraine Valley Community College and The University of Alabama in Huntsville (UAH), are conducting an advisability and feasibility study of a High School Center of Academic Excellence program. To answer the overall research question of advisability and feasibility, this study will examine the acceptability, integration, implementation, utilization, sustainability, costs and benefits and practicality of a HS CAE program.

This two-year effort is complex in both scope and methodology. The interest in developing and establishing a program or process to recognize high school cybersecurity educational efforts is a multilayered challenge. The model postulated is the post-secondary Centers of Academic Excellence program sponsored by the National Security Agency and Department of Homeland Security. The high school community is more complex because of the State stakeholders' desire to determine how they will educate their citizens. Some stakeholders are reluctant to recognize any program that may result in their perception of relinquishing this local control. There is also a strong resistance to mandates or program requirements that do not include program funding or financial resources. This causes multiple standards and varying levels of oversight. This study is aimed at unraveling those nuances to articulate an appropriate recognition effort at the high school level.

CAE High School Feasibility Study Partners

Partner Institution: Dark Enterprises
POC: Melissa Dark
Email: melissa.dark@darkenterprisesinc.com

Partner Institution: Moraine Valley Community College
POC: Dr. John Sands
Email: sands@morainevalley.edu

Partner Institution: University of Alabama in Huntsville
POC: Tommy Morris
Email: tommy.morris@uah.edu

COLLEGE PATHWAYS INITIATIVES

Curriculum to Augment RING (Awarded in FY 2021)

Lead Institution: Brookdale Community College
POC: Michael Qaissaunee
Email: mqaissaunee@brookdalecc.edu

Initiative Description

Brookdale Community College is leading the effort to develop and disseminate new content to augment RING (Regions Investing in the Next Generation). The new content will be developed in conjunction with project partners, including MVCC and UAH. As current RING project team members, the team is well positioned to build upon existing RING content, employing identical systems and software.

The new content will serve the same RING target population, giving priority to a diverse population of home-schooled, rural, and underrepresented students. Other students may be admitted based on available resources. The new materials developed will be geared to eighth and ninth grades, to be integrated with curriculum currently in development and out-of-school materials developed under the original RING initiative. These materials will also be packaged for and disseminated to CAE-C institutions.

The goals and objectives of this initiative include:

- Developing a cloud-based HTML5 RING cybersecurity career orientation 2D virtual experience
- Integrating the 15 RING cybersecurity labs into the RING 3D/2D virtual environments
- Creating an additional 30 interactive activities to supplement the current RING curriculum
- Developing and disseminating a K-12 student interactive cybersecurity capstone exercise and assessment tool

The RING cybersecurity career orientation 3D virtual experience establishes the foundation for teacher, student, and parent awareness and understanding of cybersecurity careers and opportunities. Over the last five years, there has been significant growth in the use of 3D virtual worlds for e-learning and distance education. These immersive environments create complex, highly interactive simulations, using in-world work environments and interactive exercises.

Virtual learning environments enable students to practice skills and master the application of concepts and abilities in a work-based educational context. These environments offer the ability to manage the presentation of content, integrate challenges, and implement meaningful student competency assessments.

COLLEGE PATHWAYS INITIATIVES

Curriculum to Augment RING Coalition

Partner Institution: California State University, San Bernardino
POC: Dr. Vincent Nestler
Email: vnestler@csusb.edu

Description

The team from California State University, San Bernardino (CSUSB) play a key role in developing, promoting, and disseminating the NICE framework challenge. This project provides a national tool for performing in-depth student competency evaluation. CSUSB has extensive experience in developing practical exercises that require students to demonstrate critical thinking and troubleshooting skills. This team brings this expertise to the real-world scenarios for the Cybersecurity Teaching and Learning Simulator (CTLS) capstone exercises.

Partner Institution: Sinclair Community College
POC: Kyle Jones
Email: kyle.jones4990@sinclair.edu

Description

Sinclair Community College is a national leader in the field of competency-based education (CBE). All courses developed at Sinclair are offered in the following modalities: face-to-face, online, hybrid, and via CBE. Faculty from Sinclair will provide their expertise in the creation and delivery of competency-based courses. They will assist in developing, testing, and refining the competency-based capstone exercises and infusing competency-based teaching and learning throughout the curriculum.

Partner Institution: University of Alabama in Huntsville
POC: Jesse R. Hairston
Email: jesse.hairston@uah.edu

Description

University of Alabama in Huntsville (UAH) works to facilitate the alignment of new content with the existing RING curriculum and assists in dissemination efforts.

Partner Institution: Moraine Valley Community College
POC: Dr. John Sands
Email: sands@morainevalley.edu

Description

The team at Moraine Valley Community College coordinates the identification, development, and testing of new interactive content (EMATEs) for the project.

RING CAPACITY EXPANSION

(Awarded in FY 2021)

Lead Institution: University of Alabama in Huntsville
POC: Jesse R. Hairston
Email: jesse.hairston@uah.edu

Initiative Description

The University of Alabama in Huntsville (UAH) is expanding the capacity of the RING program through TRIP: Teaching Resources to Improve Performance. TRIP will provide review and improvement of the existing curriculum, add student seats to the online course, host lab space for teachers being trained to teach RING in face-to-face settings, and support a single point of registration, marketing, student outreach, and instruction/project management.

TRIP permits UAH to review and improve the existing RING curriculum. It will also allow the university to teach RING online to approximately 300 students in the 2022 school year and 700 students in the 2023 school year. This provides an opportunity for students from rural areas, students from under-resourced systems, students who are home-schooled, and students attending schools without cybersecurity programs the chance to take the class for free and receive high school credit.

Through UAH, students benefit from the experience of credentialed K-12 educators with cybersecurity backgrounds along with access to hands-on labs and activities that make learning cybersecurity practical and fun. Students will have the opportunity to participate in a cybersecurity club and honor society and will have the option to earn dual credit with participating CAE institutions.

TRIP allows UAH to partner with Coastline Community College to provide much-needed additional lab space to support students enrolled in RING's online course. These additional instances of lab space helps to increase the available seats for in-person instruction.

This allocation will increase during the optional third year of funding. These efforts are coordinated through a project management team who will handle registration of online student and teacher accounts, grant teachers access to the curriculum, coordinate with CAE institutions training teachers on the RING curriculum, and facilitate marketing and student outreach.

RING Expansion Project Coalition

Partner Institution: Coastline Community College
POC: Tobi West
Email: twest@coastline.edu

Description

Coastline Community College manages and provides the NDG NETLAB+ virtual lab equipment and environment to allow students across the nation to access RING lab resources. The environment will be available to students enrolled through the UAH courses, students enrolled in external RING courses, and teachers receiving RING curriculum training.

SECONDARY TEACHER INITIATIVES

Cybersecurity High School Innovations (CHI) (Awarded in FY 2021)

Lead Institution: City University of Seattle
POC: Morgan Zantua
Email: zantuamorgan@cityu.edu

Initiative Description

The Cybersecurity High School Innovations (CHI) initiative is building toward a sustainable network within the Northwest region, to train and prepare high school teachers to teach complete cybersecurity courses. City University of Seattle and its partners will use a systemic approach to simultaneously recruit administrators and teachers within school districts with supportive school boards. Using this approach, CHI ensures that selected high schools across the region will have stand-alone cybersecurity courses in their catalog, ready for delivery by the Fall of 2022.

In the first two years of the initiative, a multi-layer sponsorship network comprised of regional, state, and local organizations will be developed. This network will serve several functions, including: providing tours of facilities to help teachers better understand the cybersecurity workplace, offering summer internships to high school teachers to deepen their knowledge of cybersecurity work roles and responsibilities, staffing a 'speakers bureau' for guest lecturers in classes, providing student club mentors to support after-school student cybersecurity clubs and competitions, and conducting virtual and in-person tours to high school classes.

Sustainability beyond the optional third year of the initiative has already begun with research on how to leverage Perkins funding to supplement additional high school teachers.

CHI Coalition

Partner Institution: Regis University
POC: Walt Sulmeisters
Email: wsulmeis@regis.edu

Robert Bowles
rbowles@regis.edu

Description

Regis is actively working to educate the next generation of cybersecurity professionals, both inside and outside the classroom. As a partner, Regis University's contribution will focus on recruitment within Colorado, mentoring the recruited teachers, and resource development to continue the program beyond the grant period.

Partner Institution: North Idaho College
POC: Robert Quant
Email: robert.quant@nic.edu

Description

North Idaho College will contribute to this initiative by focusing on recruitment in the state of Idaho, resource development, mentoring, and instructing.

SECONDARY TEACHER INITIATIVES

Partner Institution: University of Idaho
POC: Michael Haney
Email: mhaney@uidaho.edu

Description
University of Idaho will contribute to this initiative by focusing on recruitment in the state of Idaho, resource development, mentoring, and instructing.

Partner Institution: Missoula College
POC: Cheyenne Laue
Email: cheyenne.laue@mso.umt.edu

Description
Missoula College will contribute to this initiative through resource development.

Partner Institution: Great Falls College
POC: Cheryl Simpson
Email: cheryl.simpson@gfcmsu.edu

Description
Great Falls College will contribute to this initiative by mentoring dual credit instructors.

Partner Institution: University of Montana
POC: Victor Valgenti
Email: victor.valgenti@mso.umt.edu

Description
University of Montana will contribute to this initiative by providing instruction and general aid.

Partner Institution: North Dakota State University
POC: Jeremy Straub, Rosie Kloberdanz
Email: jeremy.straub@ndsu.edu, Rosi.kloberdanz@K12.nd.us

Description
North Dakota State University (NDSU) is a newer CAE-C institution and has hosted two GenCyber camps, demonstrating experience with teaching cybersecurity to the K-12 population. NDSU will provide a graduate student to devote 320 hours of their calendar year in support of this initiative.

Partner Institution: Mount Hood Community College
POC: Tobin Shields
Email: Tobin.Shields@mhcc.edu

Description
Mount Hood Community College (MHCC) works within the local communities to support cyber education and connect with industry. MHCC will contribute to this initiative by providing instruction.

SECONDARY TEACHER INITIATIVES

Partner Institution: Dakota State University
POC: Robert Honomichl
Email: rob.honomichl@dsu.edu

Description

The Beacom College of Computer and Cyber Sciences at Dakota State University actively participates with GenCyber camps, Cyber Corps, CAE Workforce Development, and attends and presents at the NICE K-12 Cybersecurity Conference. For this initiative, DSU will serve as a mentor for participants, recruit in the state of South Dakota, and provide resource development and instruction in South Dakota.

Partner Institution: Green River College
POC: Ed Goad
Email: Egoad@greenriver.edu

Description

Green River College will provide both online synchronous and asynchronous delivery to high school teachers in 2022 and 2023. A 10:1 high school teacher to instructor is anticipated. In-person summer sessions may be conducted in sub-regional locations, depending on the number of teachers participating in the grant in 2023 and in the optional year 2024. High school teachers returning from the first year cycle for additional certification and training may be enlisted to assist instructors with the new cohort of high school teachers.

Partner Institution: University of Washington Bothel
POC: Marc Dupuis
Email: marcjd@uw.edu

Description

University of Washington Bothell provides summer camps through the Pacific Science Center, and ran a GenCyber camp in the summer of 2021. UW Bothell will provide on-site instructing during a CHI summer summit.

SECONDARY TEACHER INITIATIVES

The National Cybersecurity Teaching Academy (Awarded in FY 2021)

Co-Lead Institution: Depaul University
POC: Dr. Filipo Sharevski
Email: fsharevs@cdm.depaul.edu

Co-Lead Institution: University of Arkansas at Little Rock
POC: Philip Huff
Email: pdhuff@ualr.edu

Co-Lead Institution: University of Louisville
POC: Adel Elmaghraby
Email: adel.elmaghraby@louisville.edu

Initiative Description

Continued teacher learning via a variety of professional development opportunities is essential to student success, particularly to support educational innovations. Teachers need a depth of subject knowledge, technical skills, and appropriate instructional methods. This is certainly true with cybersecurity, which is often a new subject area for teachers who may or may not have computing or technical backgrounds.

With a dynamic, multi-disciplinary field such as cybersecurity, teachers need access to professional development that goes beyond the introductory one-day or one-week workshops that are often curriculum- or tool-focused. Teachers need to build robust cybersecurity knowledge and skills in order to support their students' learning beyond the boundaries of any particular set of instructional materials.

The National Cybersecurity Teaching Academy (NCTA) is a graduate-level, virtual cybersecurity certificate program for high school teachers across the United States, designed to provide the depth of knowledge and skills needed for teachers to implement cybersecurity courses, programs, and pathways. The NCTA is being implemented in the Midwest, Southwest, and Southeast regions, with an institution in each region that leads its own coalition.

The NCTA will provide teachers with the depth of cybersecurity knowledge necessary to develop and implement stand-alone high school cybersecurity courses that best impact student learning outcomes. The coalitions are also partnering with DARK Enterprises, a non-profit organization dedicated to developing, supporting, and stewarding excellent cybersecurity education at the secondary level. DARK Enterprises will be responsible for coordinating the work with all three coalitions.

The objectives of the NCTA are to:

- Design, develop, and implement the National Cybersecurity Teaching Academy virtually
- Recruit 90 high school teachers to participate in the National Cybersecurity Teaching Academy to earn a Cybersecurity Teaching Graduate Certificate
- Support these 90 high school teachers in developing their cybersecurity knowledge in order to teach high school cybersecurity

SECONDARY TEACHER INITIATIVES

DePaul University (Midwest Region)

Description

DePaul University will oversee all aspects of this initiative in coordination with DARK Enterprises, as well as creation of the overall curriculum content for the proposed National Cybersecurity Teaching Academy, in particular the DePaul University expertise of human-centered security. As lead of the Midwest Coalition, they will ensure consistency of the curriculum offerings across the academy and work with the coalition representatives to ensure a high quality participant experience. DePaul will recruit teachers from the Chicago Public School district, as well as across the state of Illinois. DePaul will offer the certification as part of their cybersecurity graduate programs.

Midwest Regional Coalition

Partner Institution: Purdue University
POC: Ida Ngambeki
Email: ingambek@purdue.edu

Description

Purdue University is a leading cybersecurity education and research institution, will develop and implement courses in the domain of cybersecurity pedagogy and human-centered security. The school will also assist in recruiting high school teachers in the Midwest region.

Partner Institution: Waukesha County Technical College
POC: Jason Huebner
Email: JHuebner6@wctc.edu

Description

Waukesha County Technical College in Wisconsin, will assist in developing educational materials and labs and adapting of the academy's curriculum towards the high school teachers' needs, knowledge, and classroom contexts. WCTC will also recruit high school teachers interested in cybersecurity education to participate in the Midwest region.

SECONDARY TEACHER INITIATIVES

University of Arkansas at Little Rock (Southwest Region)

Description

University of Arkansas at Little Rock (UALR) will oversee all aspects of this initiative, ensuring that all work will be performed as defined in the contract. In particular, UALR will coordinate the Graduate Program Certificate offering, course offerings, and graduate project, as well as curriculum development and recruitment.

Southwest Regional Coalition

Partner Institution: California State University, Sacramento
POC: Dr. Jun Dai
Email: daij@ecs.csus.edu

Description

Sacramento State will collaborate with the other partners to:

- Be part of the curriculum committee and the team to establish field experiences and research projects
- Recruit, recommend, and review teachers
- Provide outreach to states and communicate learning outcomes for certification
- Mentor teachers through field experience and research projects
- Conduct a virtual college fair among the nine institutions for teachers' high school students.

Partner Institution: Estrella Mountain Community College
POC: Tom Polliard
Email: thomas.polliard@estrellamountain.edu

Description

Estrella Mountain Community College will:

- Collaborate with the other partners, to include being part of the curriculum committee and the team to establish field experiences and research projects
- Recruit, recommend, and review teachers
- Outreach to states to communicate learning outcomes of certificate
- Mentor teachers through field experience and research projects
- Conduct a virtual college fair among the nine institutions for teachers' high school students.

SECONDARY TEACHER INITIATIVES

University of Louisville (Southeast Region)

Description

University of Louisville will oversee all aspects of this project in coordination with the Computer Science and Engineering department and the University of Louisville multidisciplinary faculty members. In particular, University of Louisville will coordinate the consistency of the course offerings with departmental policies and work with the department chair and staff to ensure the high quality of participants' experience.

Southeast Regional Coalition

Partner Institution: Tennessee Tech University
POC: Dr. Mohamed Mahmoud
Email: mmahmoud@tntech.edu

Description

Tennessee Tech will implement training courses during the project period and assist in the development of prerequisite material for advanced courses. Furthermore, they will develop hands-on labs for cyber-physical systems, a specific area of their expertise. Finally, Tennessee Tech will assist in recruiting high school teachers in the Southeast region.

Partner Institution: Bluegrass Community and Technical College
POC: Dana Brown
Email: dana.brown@kctcs.edu

Description

Bluegrass Community and Technical College (BCTC) will assist in developing educational materials and four labs, as well as running pilots of the program. BCTC will recruit high school teachers interested in cybersecurity education.

CYBERSECURITY EDUCATION STATE OUTREACH

Cybersecurity Education Innovation (Awarded in FY 2021)

Lead Institution: Moraine Valley Community College
POC: Charles Bales
Email: bales@morainevalley.edu

Initiative Description

Moraine Valley Community College (MVCC), the CAE-C Midwest Regional Hub, will lead a coalition of NCAE-C institutions in the region to disseminate content from the RING Project and promote the implementation of new cybersecurity courses and programs of study (PoS). The success of this initiative will be highly dependent on developing cyber champions at all levels of the K-12 cybersecurity community. These cyber champions start with representatives from each states' Department of Education, leaders from the business community, as well as higher education and postsecondary CTE/CS curriculum directors, counselors, advisors, teachers, parents, and students.

MVCC will lead the effort to identify and work with a CAE-C coordinator in each state. The Midwest Hub will establish a standardized process assessment instruments to collect data and implement a distribution network in each state. This coalition will disseminate these assessment instruments to the four other regional teams. This process will result in the collection of valuable data for promoting new courses and programs and continued support of individuals interested in expanding the national cybersecurity pipeline.

Goals of this initiative include:

- Forming statewide high school special interest communities within each state in the Midwest region for aligning and promoting cybersecurity programs of study
- Establishing a regional distribution network
- Publishing a final report documenting project data, success, and impact.

MVCC will have several personnel working on this initiative to coordinate the overall effort and research, as well as coordinate local events.

Coalition Partners

Ten states will participate in this initiative: Illinois, Indiana, Wisconsin, Minnesota, Ohio, Michigan, Iowa, Missouri, Kansas, and Nebraska. The specific partners are still being identified, but each state will have a state coordinator, who is responsible for identifying local stakeholders, securing meeting locations, and coordinating the local events. Each state coordinator will also be in charge of distribution of research and assessment instruments, as well as the promotion of the curriculum alignment. They will mentor the dual credit/dual enrollment participants.

CYBERSECURITY EDUCATION STATE OUTREACH

CAE Regional Hubs Collaboration with State Departments of Education for the Northwest Region (Awarded in FY 2021)

Lead Institution: University of Washington Bothell
POC: Marc Dupuis
Email: marcjd@uw.edu

Initiative Description

Many efforts have been undertaken to further enhance the capacity of the K-12 system to provide age-appropriate STEM education. The dominant focus for many years has been on providing opportunities for students to engage in computer science-related curriculum. The extent to which security concerns have been incorporated into the curriculum has varied significantly. Efforts focused specifically on cybersecurity in the K-12 system have been most pronounced through the NSA's GenCyber program. While this program has had many great successes, it was not designed to formally integrate within the K-12 system. Thus, opportunities for K-12 students to pursue cybersecurity within the established educational system remains bleak.

This initiative takes several important first steps toward addressing this problem through the following goals:

- Identification of stakeholders within the Departments of Education (or equivalent body) for each of the eight states in the NW Region that have a NCAE-C institution
- Identification of stakeholders within NCAE-C institutions being represented by the points of contact identified for each of the eight states in the NW Region
- Identification of processes, requirements, procedures, policies, rules, etc., at the state level, district level, and the NCAE-C institutions represented by the points of contact, as it relates to articulation, concurrent enrollment, transfer, and dual enrollment agreements between K-12 educational bodies and higher education institutions
- Development of one or more articulation, concurrent enrollment, transfer, and/or dual enrollment agreements between K-12 educational bodies and higher education institutions for each state with a NCAE-C institution in the NW Region

Led by University of Washington Bothell, which is also in charge of the effort in Washington state, each partner will focus on the above efforts within their own state. During the first year of the initiative the partners will focus on:

- Identifying stakeholders and developing relationships
- Identifying processes, requirements, procedures, polices, and rules
- Taking the initial steps in the development of one or more agreements

If the optional second year is selected for funding, the focus will shift toward initial and subsequent successes as it relates to the development of one or more agreements with K-12.

CYBERSECURITY EDUCATION STATE OUTREACH

Northwest Hub Regional Coalition

Partner Institution: Regis University
POC: Dr. Walt Sulmeisters
Email: wsulmeis@regis.edu

Partner Institution: Dakota State University
POC: Rob Honomichl
Email: Rob.Honomichl@dsu.edu

Partner Institution: North Idaho College
POC: Kathleen Czurda-Page
Email: Kathleen.Czurda-Page@nic.edu

Partner Institution: Brigham Young University
POC: Justin Giboney
Email: justin_giboney@byu.edu

Partner Institution: Missoula College
POC: Victor Valgenti
Email: victor.valgenti@mso.umt.edu

Partner Institution: Portland State University
POC: Julia Babcock
Email: jjb@pdx.edu

Partner Institution: North Dakota State University
POC: Jeremy Straub
Email: Jeremy.straub@ndsu.edu

ADVANCING THE CYBERSECURITY WORKFORCE

Programs and projects that leverage the expertise of CAE-C schools to have an impact on the cybersecurity workforce at the national, state, or local level.

DIVERSITY INITIATIVE

While the cybersecurity workforce faces a gap in the amount of talent needed to meet current and future cybersecurity needs, minorities are also significantly underrepresented within the field. These initiatives seek to feed the pipeline into cyber careers with diverse populations by creating opportunities for minorities to pursue a degree in a cybersecurity field.

Cybersecurity Education Diversity Initiative (CEDI) (Awarded in FY 2020)

Lead Institution: Fordham University
POC: Dr. Thaier Hayajneh Dr. Amelia Estwick
Email: thayajneh@fordham.edu aecedi@fordham.edu
More Information: www.fordham.edu/fcc/cedi

Initiative Description

There is a severe shortage of Minority Serving Institutions (MSI) amongst the CAE-C Community. CEDI acts as a conduit for schools that are eligible fora CAE-CD designation and require additional support to mature and grow their cybersecurity educational programs. To accomplish this goal, Fordham University, along with its nine coalition members, steer five major activities:

- **Faculty Development:** Provides Historically Black Colleges and Universities (HBCU) and other MSIs with the opportunities and assistance needed to develop cybersecurity programs that meet the institutions' objectives. This is achieved by sharing of faculty as guest lecturers, online guest lecturers, hiring of new qualified faculty, and training for existing faculty to instruct on cybersecurity topics.
- **Student Development:** Supports MSI students participating in competitions with other students and teams from coalition members. MSI students will also be ensured the availability of workforce development opportunities.
- **Curricula Development:** Provides HBCUs and other MSIs with opportunities and assistance to develop cybersecurity programs that meet the institutions' objectives through assistance with lab technologies, integrating NICE standard Knowledge Units (KUs) into course and lab materials, and sharing curricula.
- **Mentorship & Advisement:** Acts as advisors to assist MSIs, offering tailored support for MSIs
- **Articulation Agreements:** Provides students at HBCUs and other MSIs an opportunity to achieve a minor in cybersecurity or a cybersecurity certificate, as part of their degree program through articulation agreements, transfer agreements, or other innovative means.

These CEDI activities benefit MSIs nationwide, increasing resources and opportunities for their students. This in turn benefits the country as a whole as CEDI contributes to the development of a diverse, equitable, and inclusive cyber workforce.

CEDI has developed and established a sound infrastructure that will bolster program growth for years to come. Efforts for success include website creation, implementation of a clear coalition member reporting process to ensure CEDI standards ar upheld, and the development of two applications for MSIs and current CAE schools.

In addition to the coalition partners listed on the following pages, another 48 CAE-CD, CAE-CO, and CAE-R institutions have pledged to support the CEDI Initiative with further resources.

DIVERSITY INITIATIVE

CEDI Coalition

Partner Institution: Polytechnic University of Puerto Rico
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

The Center for Information Assurance for Research and Education at Polytechnic University in Puerto Rico (PUPR) plans on supporting up to 15 people in completing a certificate in either Secure IT Operation Management or Digital Evidence and Auditing. They are developing Capture the Flag (CTF) teams at other universities in Puerto Rico by hosting workshops at PUPR that provide training to students and faculty.

Partner Institution: Metropolitan State University of Denver
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

Metropolitan State University (MSU) of Denver is facilitating partnerships with the Mountain West Cybersecurity Consortium and the Colorado Department of Education to better position the region to bring in the next generation of cybersecurity experts and professionals. MSU Denver is also creating transfer agreements so students at two-year institutions can transfer to four-year institutions that have cybersecurity programs.

Partner Institution: University of Tennessee at Chattanooga
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

The University of Tennessee at Chattanooga (UTC) offers online cybersecurity workshops for MSIs. UTC provides a cloud-based cybersecurity training workshop three times a year, with a capacity of 20 MSI instructors for each workshop. Each workshop spans a five-week period with five days total of instruction time. UTC covers 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.

Partner Institution: North Carolina Agricultural and Technical State University
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

North Carolina Agricultural & Technical State University (NC A&T) shares cybersecurity course materials with MSIs. NC A&T hosts webinars and workshops to train educators to effectively teach their courses. For those institutions lacking computer facilities for labs, NC A&T created virtual machines on their own servers. Students can also engage in the Capture the Flag events involving college, high school students, and middle school, which are normally hosted at the university.

DIVERSITY INITIATIVE

Partner Institution: New Jersey City University
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

Provides consultation and course plans to HBCUs and MSIs so they can begin with introductory cybersecurity courses covering topics including automated information systems, security policies, and system operating environments. They have identified institutions with whom they will start the advising process to include Essex County College, Mercer County Community College, Bergen Community College, and Hudson County Community College. New Jersey City University is also creating a beginner-level cybersecurity training workshop, to be taught at those four institutions. A summer boot camp is also being planned for 15 students from each of the colleges to practice hands-on lab exercises.

Partner Institution: Bluegrass Community and Technical College
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

Bluegrass Community and Technical College (BCTC) Informatics Academy is expanding to include cybersecurity courses for high schools, allowing the lessons to count toward college credit. BCTC is also designing a 2+2 articulation agreement, so students completing an associate degree in Cybersecurity at BCTC can transfer to Kentucky State University and finish with a bachelor's degree.

Partner Institution: University of North Florida
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

University of North Florida (UNF) has four activities to develop a comprehensive cybersecurity partnership with Edward Waters College (EWC), a local MSI. The first is establishing a credit-transfer agreement with EWC, so that the course proposed by UNF will count toward cybersecurity certification. UNF is assisting EWC with creating a course schedule and the infrastructure for online teaching. Additionally, UNF is sharing cybersecurity curriculum with EWC faculty, to include a five-day workshop, 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. UNF is also creating a pathway for students at MSIs to participate in club meetings at UNF's student-led cybersecurity club, as well as developing a workshop for students, which will be jointly hosted by UNF and Florida State College.

DIVERSITY INITIATIVE

Partner Institution: University of North Texas
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

University of North Texas (UNT) is working on a three-step pathway for cybersecurity education, leading to a potential NCAE-C program designation at MSIs. UNT is inspiring students and growing interest in cybersecurity by hosting Capture the Flag and Digital Forensics Scavenger Hunt competitions. UNT is building an internship readiness tool that automates the mapping of job descriptions to knowledge units in courses that UNT covers. This allows instructors at universities to see how their courses prepare students for specific job roles. UNT is also developing bridge courses that are being offered to MSIs that do not have a cybersecurity program, so that students can either complete a certificate program or transfer to a four-year institution. UNT identified four colleges in the Dallas County Community College District and is discussing articulation agreements with them: El Centro College, Cedar Valley College, Del Mar College, and Odessa College.

Partner Institution: Tennessee Tech University
POC: Dr. Thaier Hayajneh and Dr. Amelia Estwick
Email: cedi@fordham.edu

Description

Tennessee Tech is expanding hands-on skill opportunities for MSI students by developing and orchestrating 24-hour Capture the Flag competitions, where the students can remotely participate to gain technical skills in cybersecurity. The school is also 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. To expand awareness, knowledge, and skill training opportunities for MSI students, Tennessee Tech is facilitating and programming their remote participation in two cybersecurity clubs and helping them to create and sustain such student organizations for their schools. Tennessee Tech is also providing guidance to MSI faculty about becoming NCAE-C designated by providing virtual advisement sessions to discuss considerations and issues related to applying for NCAE-C designations.

WORKFORCE DEVELOPMENT INITIATIVES

As cyber threats continue to emerge and proliferate, the need for a qualified workforce grows. Concurrently, there are many transitioning out of military or first responder careers and are looking for new opportunities that build on their experience. The professional experience of these transitioning military and first responders combined with training and certification in cybersecurity acts as an under-tapped resource to supply the cybersecurity workforce shortage. These workforce development initiatives offer certification opportunities to engage such professionals and grow the future cyber workforce.

National Cybersecurity Workforce Development Program (Awarded in FY 2020)

Lead Institution: University of West Florida
POC: Dr. Eman El-Sheikh
Email: eelsheikh@uwf.edu
More Information: cyberskills2work.org

Initiative Description

The University of West Florida is leading a coalition of 10 NCAE-C institutions to establish a nationally scalable and sustainable certificate-based cybersecurity workforce development program. The overall goal is to establish best-practices, nationally scalable, and sustainable certificate-based program with verifiable credentialing to more rapidly expand the cybersecurity workforce as follows:

- Increase the number of qualified, skilled professionals
- Support the 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 sectors
- Provide NCAE-C institutions access to curricular resources through the NCAE-C Resources Directory

Workforce Development Program Coalition

Partner Institution: Augusta University
POC: Dr. Michael Nowatkowski
Email: mnowatkowski@augusta.edu

Description

Augusta University targets transitioning military with the Cyber Workforce Transition Program. They are recruiting 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.

Partner Institution: University of Houston
POC: Dr. Art Conklin
Email: waconklin@uh.edu

Description

The University of Houston co-leads efforts focused on the development of best-practice workforce development and curricular models.

WORKFORCE DEVELOPMENT INITIATIVES

Partner Institution: Dakota State University
POC: Dr. Ashley Podhradsky
Email: ashley.podhradsky@dsu.edu

Description

Dakota State University targets transitioning military and first responders with their Digital Forensics and Open Source Intelligence (OSINT) Academy. The learner-centric competency-focused education trains students on evidence identification, acquisition, preservation and investigative processes for traditional hard disk drives, emerging IoT devices, cloud accounts, and online communication.

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

Description

Eastern New Mexico University – Ruidoso Branch Community College targets transitioning military and first responders and Native American populations with their Computer and Network Cybersecurity Certificate Program. They offer the Computer and Network Security Certificate integrated with an apprenticeship certificate program, leveraging expertise in Risk Management and DHS CSET Tool.

Partner Institution: Florida International University
POC: Randy Pestana
Email: rpestana@fiu.edu

Description

Florida International University targets 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.

Partner Institution: Metropolitan State University
POC: Dr. Faisal Kaleem
Email: Faisal.Kaleem@metrostate.edu

Description

Metropolitan State University targets transitioning military, first responders, and other underrepresented minorities with their Intensive Cybersecurity Program for our nation's heroes. The program implements an accelerated cybersecurity training program to prepare and place transitioning military veterans, first responders, and other underrepresented minorities into cybersecurity work roles.

WORKFORCE DEVELOPMENT INITIATIVES

Partner Institution: San Antonio College
POC: Kim Muschalek
Email: kmuschalek@alamo.edu

Description

San Antonio College (SAC) targets transitioning military, existing first responders, and 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 Finance degree earners who are prepared to defend our nation's security and prosperity via cybersecurity-related positions in San Antonio, Texas, and beyond.

Partner Institution: University of South Florida
POC: Dr. Ron Sanders
Email: rpsanders@usf.edu

Description

The University of South Florida is targeting 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. USF is co-leading efforts focused on employer and industry engagement and partnerships.

Partner Institution: University of Texas at San Antonio
POC: Dr. Glenn Dietrich
Email: glenn.dietrich@utsa.edu

Description

The University of Texas at San Antonio targets 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.

WORKFORCE DEVELOPMENT INITIATIVES

National CAE-C Cybersecurity Workforce Development Program - Healthcare (Awarded in FY 2020)

Lead Institution: University of Louisville
POC: Dr. Sharon Kerrick
Email: sharon.kerrick@louisville.edu
More Information: louisville.edu/education/nsacybersecurity/

Initiative Description

As technology continues to become more of an integral piece of our everyday lives, a strong cybersecurity industry and workforce are the most important protections to make financial and healthcare systems secure. The University of Louisville leads a coalition of schools called the Cybersecurity Pathways Coalition (CPC) that developed and piloted a Cybersecurity Workforce Certificate program.

The program focuses on enhancing student knowledge in the realm of cybersecurity foundational courses, while using healthcare data examples and use cases. The certificate includes basic elements of cybersecurity, cryptography, database, artificial intelligence, analytics, blockchain, Internet of Things (IoT), and other areas related to the healthcare industry. Students have the opportunity to earn technology industry badges and certificates including IBM, Microsoft, and Google. Authentic Use Cases were provided by national industry partners, including the Louisville Healthcare CEO Council. This six-month instructor-led online certificate utilizes applied and experiential learning modules with hands-on labs.

Healthcare Workforce Development Program Coalition

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

Description

The University of Arkansas at Little Rock (UALR) works 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.

Partner Institution: Kentucky Community and Technical Colleges
POC: Dr. Erin Tipton
Email: erin.tipton@kctcs.edu

Description

The Owensboro and Bluegrass branches of the Kentucky Community and Technical Colleges System (KCTC) offer robust courses in cybersecurity and have extensive technical knowledge and course development expertise. The workforce development constituents of the KCTC understand the practical hands on approaches that are critical to the certificate.

WORKFORCE DEVELOPMENT INITIATIVES

Partner Institution: University of North Florida
POC: Dr. Sherif Elfayoumy
Email: selfayou@unf.edu

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 (IBM and Microsoft), government (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 pilot program. Their partners of the PAX Technology Cybersecurity Lab and industry healthcare system experts will also teach or guest lecture. UNF has expertise in intrusion detection, forensics, disaster recovery, and preparedness.

National CAE-C Cybersecurity Workforce Development Program – Artificial Intelligence (Awarded in FY 2020)

Lead Institution: Purdue University Northwest
POC: Michael Tu
Email: Michael.Tu@pnw.edu
More Information: www.pnw.edu/cybersecurity/cwct

Initiative Description

Purdue University Northwest (PNW) established the Cybersecurity Workforce Development Consortium and developed a pilot Artificial Intelligence (AI) Cybersecurity certification-based national training program, following the U.S. Department of Labor apprentice training model for transitioning military, first responders, and other adult trainees. The main objectives of the pilot training program include:

- Developing AI and cybersecurity course curriculum with free online access
- Recruiting over 425 adult learners, primarily transitioning military and first responders
- Offering three training tracks in cybersecurity administration, digital forensics, and artificial intelligence, each with six eight-week online courses, to include exams from certification vendors to earn certifications
- Certification training in CompTIA A+, CompTIA Linux+, CompTIA Security+, Cisco CyberOps Associate, EC

WORKFORCE DEVELOPMENT INITIATIVES

Artificial Intelligence Workforce Development Program Partners

Partner Institution: Ivy Tech Community College
POC: Matthew Cloud Rami Maximus
Email: mcloud3@ivytech.edu rsalahieh@ivytech.edu

Description

Ivy Tech Community College is responsible for developing a three course curriculum for the AI-Cybersecurity training program, recruiting training participants, and providing placement service to training participants. Ivy Tech also leads the consortium on instructor hiring, instructor professional development training, industry and government agency partnership development, CyberRange lab management, and technical support technicians for students on labs.

Partner Institution: University of North Carolina at Charlotte
POC: Fareena Saqib Shagufta Y. Raja
Email: fsaqib@uncc.edu sraja1@uncc.edu

Description

University of North Carolina at Charlotte (UNCC) is responsible for developing one course curriculum of the AI-Cybersecurity training program, recruiting participants, offering one track of the training program, and providing placement service to the participants.

Partner Institution: University of Tennessee at Chattanooga
POC: Mengjun Xie Daniel Pack
Email: mengjun-xie@utc.edu Daniel-Pack@utc.edu

Description

University of Tennessee at Chattanooga (UTC) is responsible for developing one course curriculum of the AI-Cybersecurity training program, recruiting training participants, offering one track of the training program, and providing placement service to participants.

COMMUNITY DEVELOPMENT INITIATIVES

Cybersecurity is as important at the community level as it is nationally. It could be argued that starting smaller is the best approach to solving a problem. These initiatives take a look at cybersecurity at the community level, with an eye on establishing model approaches for other communities nationwide.

Inland Empire Cybersecurity Initiative (IECI) (Awarded in FY 2021)

Lead Institution: California State University, San Bernardino
POC: Dr. Tony Coulson
Email: tcoulson@csusb.edu

Initiative Description

California State University, San Bernardino (CSUSB) is leading a coalition of area NCAE-C institutions on the Inland Empire Cybersecurity Initiative, in alignment with state and regional efforts to alleviate the deficit in high-quality cybersecurity jobs that pay well.

IECI will identify and prepare cybersecurity talent for local employers and attract new employers who are seeking talent to create jobs in the Inland Empire. IECI will build on the nationally-recognized cybersecurity program at CSUSB and cybersecurity education in local community colleges and K-12 schools to establish a pipeline of world-class talent.

IECI will use cybersecurity apprenticeship to accelerate students' experience and education and meet employers' workforce needs. In IECI, students will evolve from exploration, to pre-apprentice, to apprentice in a structured program that includes career, curricular, and experiential learning, plus evaluations and completion requirements.

Unlike other cybersecurity credentialing programs that rely on lecture and lab-based training, IECI will emphasize learning outside of the classroom, on the job, with mentors and professionals. Apprentices will earn an income as they pursue their education and grow in the cybersecurity field.

CSUSB and its partners will build on their existing linkages to employers to create regional industry partnerships. A number of employers want to participate by hiring IECI apprentices; IECI will provide businesses with qualified, CAE-trained, talented employees who have the cybersecurity competencies that companies desire. Students who now seek employment outside the region will be more likely to stay in the Inland Empire with employers that have invested in their careers through apprenticeship. An ongoing talent pipeline in cybersecurity will attract employers and jobs to the region.

COMMUNITY DEVELOPMENT INITIATIVES

Goals of this initiative include:

- Expanding the K-12 pipeline and early interest among Inland Empire students in cybersecurity careers through outreach events and activities
- Implementing an evaluation of aptitude and readiness to recruit for cybersecurity careers
- Recruiting a cohort of at least 30 community college students

  or university freshmen in year one and a cohort of at least 30 in year two, who will commit to pathways to prepare for a local apprenticeship
- Establishing a management framework and portfolio system to track each student's goals in all the pathways
- Managing students through career, experience, and curricular pathways on their journey toward apprenticeship
- Creating a model for employer and talent coordination
- Establishing a credit-for-work curricular pathway for apprenticeships at CSUSB
- Placing IECI students in successful cybersecurity apprenticeships in the Inland Empire
- Establishing a sustainable model for cybersecurity apprenticeship in the Inland Empire
- Creating a model for employer and talent coordination, including a cybersecurity apprenticeship committee with area employers, to make recommendations for industry workforce needs

IECI Partners

Partner Institution: Moreno Valley College
POC: Dr. Kasey Nguyen
Email: Kasey.nguyen@mvc.edu

Description

Moreno Valley College (MVC) is a CAE-C candidate school with a strong cybersecurity program. As a partner, MVC will be responsible for:

- Identifying and recruiting community college students for IECI
- Aligning existing cybersecurity and apprenticeship efforts with IECI
- Coordinating with CSUSB and LAUNCH to build relationships among students, academia, government, and employers

Partner Institution: Riverside City College
POC: Skip Berry
Email: skip.berry@rcc.edu

Description

Riverside City College (RCC) is a CAE-C candidate school with a strong cybersecurity program. As a partner, RCC will be responsible for:

- Identifying and recruiting community college students for IECI
- Aligning existing cybersecurity and apprenticeship efforts with IECI
- Coordinating with CSUSB and LAUNCH to build relationships among students, academia, government, and employers

COMMUNITY DEVELOPMENT INITIATIVES

Partner Institution: San Bernardino Valley College
POC: Jesse C. Chou
Email: jchou@sbccd.cc.ca.us

Description

San Bernardino Valley College (SBVC) is a CAE-C candidate school with a strong cybersecurity program. As a partner, SBVC will be responsible for:

- Identifying and recruiting community college students for IECI
- Aligning existing cybersecurity and apprenticeship efforts with IECI
- Coordinating with CSUSB and LAUNCH to build relationships among students, academia, government, and employers

Partner Institution: LAUNCH Apprenticeship Network
POC: Charles Henkles
Email: charles.henkels@rccd.edu

Description

The Local Apprenticeships Uniting a Network of Colleges and High School (LAUNCH) Apprenticeship Network is a Workforce Intermediary Program Sponsor registered with the California Division of Apprenticeship Standards and the United States Department of Labor Office of Apprenticeship. LAUNCH will contribute to this initiative by registering the CSUSB baccalaureate apprenticeship pathway and pre-apprenticeship program in cybersecurity with the Department of Labor; incorporating IECI into a regional apprenticeship campaign; liaising with industry partners for apprenticeships; and supporting recruitment at community colleges and K-12 schools.

Partner Institution: Tomorrow's Talent
POC: Dale Marsden
Email: Dale@tomorrowstalent.org

Description

Tomorrow's Talent, founded by the former superintendent of San Bernardino City Unified School District, matches local employers to local talent using a scientific approach, focusing on building the relationships and social capital that are necessary for successful careers. Tomorrow's Talent will contribute to this initiative by providing outreach to employers, coordinating up to 100 work-based learning experiences for students over two years; using YouScience in student recruitment; liaising between industry partners and high schools and community colleges; using ImBlaze to connect students to work-based learning opportunities; and managing the process.

Partner Institution: San Bernardino County - Alliance for Education
POC: Carol Tsushima
Email: carol.tsushima@sbcss.net

Description

The San Bernardino County – Alliance for Education is a countywide network will:

- Provide events, camps, games, and clubs to K-12 students to explore careers in cyber and technology
- Facilitate micro-internships for K-12 students
- Disseminate cyber teaching resources to educators in 33 school districts

COMMUNITY DEVELOPMENT INITIATIVES

The 502 Project: Building Gateways to the Cybersecurity Community (Awarded in FY 2021)

Lead Institution: University of South Florida
POC: Nathan Fisk
Email: fisk@usf.edu

Co-Lead Institution: University of West Florida
POC: Eman El-Sheikh
Email: eelsheikh@uwf.edu

Initiative Description

While significant efforts have been made to develop, administer, and scale programs that foster cybersecurity career awareness and technical skill, little attention has been paid to ensuring students have ongoing access to the cybersecurity community.

The existing cybersecurity education landscape – particularly as driven by universities and academic researchers – has been primarily marked by individual, efforts. These efforts focus primarily on developing and administering educational programs to students K-12 through to the adult workforce. While these programs have achieved significant success in raising cybersecurity awareness and skills development locally, these efforts have been largely disconnected from one another. This disconnection causes reproduction of similar content with little or no capacity to scale in any meaningful way. As a result, some of the best and most impactful cybersecurity resources, curricula, and exercises are often used only for one-off, local events, limiting access and reach significantly.

The 502 Project (named for the -- Bad Gateway -- HTTP error code) seeks to develop a persistent cybersecurity community platform, simultaneously providing students with a gateway to the cybersecurity community and professionals with a broader networking space. Expanding upon recent successes with mature cybersecurity high school programs, via a partnership with Cyversity, students will be brought into the platform through regional events with key volunteers from their local cybersecurity community.

Centralized virtual events will continue to engage both students and cybersecurity professionals throughout the year, seeking to foster intergenerational connections, bridge regional communities, and maintain the momentum of local cybersecurity education programs. The proposed project is specifically intended to highlight, promote, and extend pre-existing efforts at the local and regional level, expanding the reach and scale of key curricula, exercises and events.

Finally, the 502 Project will work to connect the community platform and local events to formal cybersecurity career pathways. Explicitly providing access to local mentors and advising staff. The proposed community platform will automate the process of registering as mentors (volunteers), protégés (students), and advisors (university/college faculty and advising staff), allowing for scheduled meetings and check-ins to facilitate mentorship and progression along formal career pathways.

The platform will further provide social space for all university and college cybersecurity student organizations in the region, affording visibility between high-school students and undergraduates currently enrolled in cybersecurity programs. Overall, the 502 Project will provide support for students from initial gateway events through to enrollment in cybersecurity educational programs, and beyond into cybersecurity careers, drawing upon an extensive network of students, volunteers, community figures, and academic advisors.

COMMUNITY DEVELOPMENT INITIATIVES

To meet these objectives, the 502 Project will employ several innovative strategies:

- Create a platform to facilitate entry to the cybersecurity community
- Utilize regional events as a gateway to the cybersecurity community
- Leverage existing investments and technologies
- Partner with a national organization to "jump start" our mentorship engine
- Mobilize the platform to assess and track students

University of South Florida and University of West Florida are sharing management and leadership of this initiative, overseeing and guiding program activities. During the pilot phase, both universities will connect their high school cybersecurity events to the 502 Project platform.

The 502 Project Coalition

Partner Institution: Tennessee Tech University
POC: Dr. Ambareen Siraj
Email: ceroc@tntech.edu

Description

A pilot partner, Tennessee Tech is home to the Cybersecurity Education, Research and Outreach Center (CEROC), and Women in CyberSecurity (WiCyS).It brings expertise in high school cybersecurity education outreach yearly GenCyber summer camp in the state (since 2016), servicing high school students from across the state. Since the center's establishment, CEROC has interacted with over 7,000 K-12 students in Tennessee.

Partner Institution: Florida International University
POC: Randy Pestana
Email: rpestana@fiu.edu

Description

A pilot partner, Florida International University (FIU) hosts both the National Initiative for Cybersecurity Education (NICE) and NICE K-12 conferences. The team at FIU will work to connect the 502 Project to both local cybersecurity gateway events and a national network of cybersecurity and CAE-C partners.

Partner Institution: Forsyth Technical Community College
POC: Thomas W. Brown III
Email: tbrown@forsythtech.edu

Description

Forsyth Technical Community College, who has hosted GenCyber camps since 2017, will participate in the second year of the initiative.

Partner Institution: St. Petersburg College
POC: Dr. John Duff
Email: duff.john@spcollege.edu

Description

St. Petersburg College, which regularly conducts outreach to high school students, will participate in the second year of the initiative.

COMMUNITY DEVELOPMENT INITIATIVES

Partner Institution: Cyversity
POC: Maggie Domond
Email: maggie.domond@cyversity.org

Description

Cyversity is dedicated to the academic and professional success of minority cybersecurity students and professionals. The 502 Project will work with Cyversity to utilize its existing network of mentors to connect students to cybersecurity professionals. Cyversity will also work with the 502 Project to assist with identification of national and regional industry partners to continue to sustain the program.

Initiatives to Contribute to a Culture of Cybersecurity (Awarded in FY 2021)

Lead Institution: University of Texas at San Antonio
POC: Gregory White
Email: greg.white@utsa.edu

Initiative Description

A whole community approach needs to be taken by communities to protect their citizens from cyber attacks on any sector. This does not mean that local government should be responsible for any cyber attack that occurs on the community, but the local government can, and should, take a leadership position in encouraging a cross-sector cybersecurity program within the community.

Moreover, cyberattacks are much less effective when users know how to handle threats. Teaching cybersecurity to individuals at an early age will surely impact their behavior. What is needed is to establish a Culture of Cybersecurity within a community. This should start with K-12 programs, designed to introduce age appropriate cybersecurity concepts, thus shifting the culture to be more cyber aware and prepared to avoid (or thwart) cyber threats. Since 2002, University of Texas at San Antonio (UTSA) has been involved in developing and conducting cybersecurity exercises, training, and assessments for states and communities. Many of the pieces needed in a community cybersecurity program have been successfully developed but need to be integrated into a whole community program, starting with K-12.

This whole community approach seeks to develop a program that will be transferable and applicable to communities of any size. Initial steps include designing and implementing a program for the city of San Angelo, Texas, that can then be used as a model for communities nationwide. At the end of this program, the goal is to have San Angelo be a cybersecurity savvy community with sustainable initiatives that encompass the whole community. UTSA will establish several initiatives within San Angelo to reach this goal:

- **K-12 Initiative:** Working with school districts and the schools within them to introduce and implement cybersecurity games, curriculum, cybersecurity competitions, summer camps, and academic and professional planning information. Coordination with the NCAE-C K-12 RING initiative will occur as appropriate.

- **Culture of Cybersecurity Initiative:** UTSA created the CyBear family to initially assist in the introduction of cybersecurity concepts in grades K-5. These characters are being used in activity sheets and eventually in a series of books to introduce concepts to children. The CyBear family is designed to be the cyber equivalent to Smokey the Bear and McGruff the Crime Dog. Establishing a culture of cybersecurity starts with the children in the community and their parents, but will branch out from there.

COMMUNITY DEVELOPMENT INITIATIVES

- **Community Cybersecurity Needs Determination and Economic Development:** In conjunction with community leaders, an analysis will be conducted on the current need for cybersecurity professionals within the community. Additionally, this analysis will evaluate the possibility of cybersecurity becoming an economic development option for the community including establishing a cybersecurity service or product development sector within the community.

- **Collegiate Initiative:** This initiative is designed to help local colleges and universities develop cybersecurity programs. This initiative will consist of projects at different levels to include an outreach program to area high schools to advertise cybersecurity-related training and education programs, cybersecurity college fairs, assisting in two- and four-year institutions in meeting the requirements for being designated in the NCAE-C program, developing certification training at interested institutions, encouraging participation in cybersecurity competitions, establishing security clubs and associations, and encouraging student and faculty involvement in security-related research. Angelo State University, an aspiring CAE-C institution, is an integral part of this initiative, serving as the model of how communities should incorporate institutions of higher learning.

- **Continuing Education Initiative:** Encourage institutions or other entities to offer cybersecurity certification training. This will help with providing needed cybersecurity professionals in the community and can assist in the establishment of a base of local cybersecurity professionals that can help with things such as mentoring cyber competition teams or speaking at collegiate club meetings.

- **Establishment of Local Cybersecurity Associations:** Help local security professionals to join various professional associations (such as ISACA, ISSA, and ASIS), and to potentially establish local chapters if the community is of a size to support this.

- **Initiative to Establish a Community Cybersecurity Program:** City governments should not be responsible for the cybersecurity of all organizations within the community, rather they can become advocates for security throughout the community. They can do this by:

    - Helping the community to establish security programs within government organizations and within the critical infrastructures
    - Developing cybersecurity policies and plans (contingency plans, incident response plans, etc.) for the local government and critical infrastructures
    - Sponsoring the creation of a community-wide information sharing and analysis organization (ISAO)
    - Establishing a citywide “Cybersecurity Day;” initiating a series of cybersecurity webinars
    - Conducting a city-wide Cybersecurity Tabletop Exercise to increase awareness of cybersecurity within the community

- **Non-Profit Initiative:** The inclusion of non-profit organizations in the community’s cybersecurity programs.

It should be emphasized that many of the activities and items have already been produced and tested. The major aspect of this project will be to develop a plan to implement them in a coordinated manner within a community to lead the community to a viable and sustainable cybersecurity program and a whole-community culture of cybersecurity. The Initiatives to Contribute to a Culture of Cybersecurity will be implemented by several UTSA faculty and staff, in coordination with entities within the San Angelo community.

COMMUNITY DEVELOPMENT INITIATIVES

NW Region Cybersecurity Risk Management and Roadmapping for Smart Grid Critical Infrastructure (Awarded in FY 2021)

Lead Institution: Portland State University
POC: Birol Yesilada
Email: yesilada@pdx.edu

Initiative Description

The Smart Grid is a driving force for modernizing critical energy infrastructure and, in turn, the need to advance whole-of-state cybersecurity for emerging technologies. With the interface of billions of Internet of Things (IoT) devices with the power distribution system, the smart grid is creating a more diffuse frontier for cyber attacks. By enhancing communications around the nature of these threats in concert with adapting security measures across multi-sector actors, the U.S. can meet the challenge of cyberattacks and their increasing complexity. Whereas national attention has been at upgrading and securing the top level of such critical infrastructures, many have often overlooked America's soft-underbelly - local and regional governments, utilities, and special districts. Adversaries, both foreign and domestic, have increased their capabilities to access such backdoor entry points to test and take advantage of vulnerabilities.

This initiative will advance government and industry collaboration through a consortium of NCAE-C institutions in the Pacific Northwest region (specifically Oregon and Washington as leads, with Colorado, Hawaii, and Idaho as cooperating partners). By focusing on cybersecurity governance and the National Governors Association management framework, this initiative can strengthen the mix of control and influence necessary for mitigating and responding to shifting tactics and threats. Together, the coalition will conduct a risk assessment for smart grid critical infrastructure vulnerabilities, test cyber defense scenarios through tabletop exercises and co-design a technology roadmap (TRM) to strengthen cross-sector cooperation in cyber defense to strengthen local preparedness and response.

This initiative identifies the Smart Grid as one of the essential critical infrastructures, which represents a complex network managed across federal, regional, and local level actors. The coalition will assess the system's strengths and weaknesses to aid in bolstering cyber defense from physical infrastructure to human capacity through risk analysis of local and regional stakeholders' capabilities in cyber defense and the security of their connections to the Smart Grid. Tabletop exercises will show how academic, government and industry partnerships can address these vulnerabilities and provide practical workforce training and education pathways, with particular attention to the need for diversity and equity in cyber studies.

This initiative will serve as a model to build and strengthen the Northwest Region's cybersecurity defense system through cooperation and collaborative problem-solving to provide mutual benefits in security, education, and multi-level (federal, state, and local) policy and technology alignment.

COMMUNITY DEVELOPMENT INITIATIVES

This initiative will take a multifaceted approach, to include:

- Addressing workforce homogeneity and the significant shortage of cybersecurity capacity
- Assessing the severe vulnerabilities and risks of local and county governments and address corresponding risks to FEMA, DHS, and CISA Regions
- Working with NSA, DHS, and FBI to analyze national security risks with local implications to meet new challenges in cyberattacks from both foreign and domestic adversaries
- Developing evidence-based policy recommendations and a technology roadmap (TRM) to improve cybersecurity whole-of-state system strategy

Portland State University is leading this initiative, bringing expertise in international and national security advising, strategic management, risk assessment design, Smart Grid infrastructure, and TRM. Additionally, PSU offers local government experts and a process facilitator, as well as experts on Smart Grid energy, energy modeling, and public policy and administrative law. PSU will also conduct the Oregon Summer Fellows program and lead a Building Cyber Resilience Certificate Program.

NW Region Cybersecurity Risk Management Partners

Partner Institution: Chemeketa Community College
POC: Zachary Yamada
Email: zachary.yamada@chemeketa.edu

Description

Chemeketa Community College (CCC) will conduct student recruitment and participation with the Northwest Region to engage in risk assessment activities, tabletop exercises, and fellowships.

Partner Institution: University of Colorado Colorado Springs
POC: Gretchen Bliss
Email: gbliss@uccs.edu

Description

University of Colorado Colorado Springs (UCCS) will consult on management and/or defense of critical infrastructure and support and share past experiences with the team as well as serve as the focal point for disseminating best practices resulting from this work across the Northwest Hub to all CAE-C institutions in the region.

COMMUNITY DEVELOPMENT INITIATIVES

Partner Institution: University of Idaho
POC: Dr. Jim Alves-Foss
Email: jimaf@uidaho.edu

Description

University of Idaho will serve in a consultant capacity, to include participation in the Northwest Region Steering Committee and co-designing partner and student engagement activities.

Partner Institution: University of Hawaii
POC: Dr. Jodi Ito
Email: jodi@hawaii.edu

Description

University of Hawaii will serve in a consultant capacity, to include participation in the Northwest Region Steering Committee and co-designing partner and student engagement activities.

Other Partners

The Northwest Region Cybersecurity Risk Management and Roadmapping for Smart Grid Critical Infrastructure coalition also includes a number of industry partners, to include T-Mobile, the cyber specialty consultancy CGS Strategies, Oregon State University Electrical & Computer Engineering department, Link Oregon, the Pacific Northwest National Laboratory, and Energy Sec. These partners will provide subject matter expert knowledge; assist in faculty-industry-government meetings; help the PI and co-PIs in project-related task planning and implementation; troubleshoot; and assess results.

Virginia Cyber Navigator Internship Program (Awarded in FY 2021)

Lead Institution: University of Virginia
POC: Jack W. Davidson
Email: jwd@viginia.edu

Initiative Description

Fair and secure elections are essential to democracy. As such, voting systems are as much a part of our nation's critical infrastructure as are transportation, energy, financial, communications, and water systems. Information technology is now a central part, arguably the backbone, of election processes. While offering numerous opportunities for improving and streamlining election processes, information technologies (IT) also open the door to new threats and increasingly adept bad actors.

To help enhance the security posture of local election infrastructures in Virginia, this initiative seeks to build a regional cybersecurity coalition of Commonwealth of Virginia universities and colleges partnering with the Virginia Department of Elections, and industry. The effort builds on the Virginia Department of Elections Cyber Navigator Program (CNP) to create an cybersecurity experiential learning experience for students at Virginia universities and colleges. The project includes a course on election security and the VA Cyber Navigator Internship program, where students will gain real-world experience in securing critical election infrastructure.

The overarching goal of VA-CNIP is to improve the security of Virginia's election system, a system that includes 133 local election offices (95 in counties and 38 in independent cities).

COMMUNITY DEVELOPMENT INITIATIVES

To achieve this, VA-CNIP will:

- Create a regional coalition
- Provide students with cybersecurity education focused on election systems and a service learning experience as interns in election districts working on their cyberinfrastructure
- Have the internship program serve as the focal point for coalition collaboration
- Posture the coalition for future and sustainable collaboration

Virginia Cyber Navigator Partners

Partner Institution: George Mason University
POC: Massimiliano Albanese
Email: malbanes@gmu.edu

Description

George Mason University (GMU) will contribute to VA-CNIP by participating in the design of the common cybersecurity course in the first year, participating in the evaluation and refinement of the course, offering and promoting the designed cybersecurity course at George Mason University, and recruiting appropriately prepared students to be cybersecurity interns.

Partner Institution: Virginia Commonwealth University
POC: Robert Dahlberg
Email: dahlbergra@vcu.edu

Description

Over the first year, a cybersecurity course will be designed at VCU for the purposes of student teams to perform security audits and evaluations, as well as other skills and knowledge students need to improve the Virginia election infrastructure. The course will be refined during the second year. VCU will actively promote the course to prospective students, from which the appropriately prepared students will be recruited as cybersecurity interns. The students will be actively mentored and given technical assistance during their internship. Periodically, students will be gathered for debriefing and problem-solving sessions with the coalition partners. Finally, student interns will contribute evaluations, documentation, playbooks and procedure to aid and assist Virginia's counties and municipalities.

Partner Institution: Virginia Tech
POC: Janine Hiller
Email: jhiller@vt.edu

Description

Virginia Tech (VT) will contribute to VA-CNIP by participating in the design of the common cybersecurity course in the first year; participating in the evaluation and refinement of the course; providing the cybersecurity and election security modules across Virginia Tech in multiple disciplines and appropriate courses across multiple majors and minors; recruiting appropriately prepared students to be cybersecurity interns; and actively mentoring and assisting interns' experiential activities.

COMMUNITY DEVELOPMENT INITIATIVES

Partner Institution: Norfolk State University
POC: Mary Ann Hoppa
Email: mahoppa@nsu.edu

Description

Norfolk State University (NSU) will be involved in the projects goal of improving the cybersecurity of local registrar offices across the commonwealth, while simultaneously providing a valuable educational experience for students.

Partner Institution: Old Dominion University
POC: Hongyi Wu
Email: h1wu@odu.edu

Description

Old Dominion University (ODU) will contribute to VA-CNIP by participating in the design of the common cybersecurity course in the first year, participating in the evaluation and refinement of the course, offering and promoting the designed cybersecurity course at ODU, recruiting appropriately prepared students to be cybersecurity interns, and actively mentoring and assisting interns during their summer activities.

Other Partners

Additional VA-CNIP partners include the Virginia Department of Elections (ELECT), Greater Washington Partnership Leidos, Veracode, Ernst & Young LLP, Capital One, Accenture Federal Services, Mitre, and General Dynamics Information Technology (GDIT).

ReCIPE: Regional Coalition for Critical Infrastructure Protection, Education, and Practice (Awarded in FY2021)

Lead Institution: Iowa State University
POC: Doug Jacobson
Email: dougj@iastate.edu

Initiative Description

As adversaries' skills are rapidly escalating and capable system defenders are in great demand, this coalition will actively align practical stakeholder requirements with innovate educational solutions to form a sustainable engagement and delivery model available to inform, consult and serve the region's stakeholders, as they identify and integrate a workforce that must be ready to address the increasingly complex security of its cyber-physical critical infrastructure.

The coalition will evolve into a driving force capable of influencing innovative defense practices and creating learning solutions, informed by the uniquely collective experiences of its membership, in ways that strategically prepare emerging learners to step into roles and prepared to make immediate impact in the region's critical infrastructure defense.

To assure a central purpose of the regional coalition formation, its existence and potential for impact must have permanency and be self-sufficient beyond the term of the initial funded period. The sustainability of the resulting coalition will depend heavily on a clearly-articulated value proposition created by participation and commitment from government and industry.

COMMUNITY DEVELOPMENT INITIATIVES

Students of a wide range of NCAE-C programs, from full-time students to mid-career workers, as well as government, industry, and its trade associations will gain unique value from the successful combination of real-world needs and experience focused educational material. The combined resources of the coalition will serve as a vehicle for active consultation to the region's critical infrastructure providers in ways that leverage learned experiences, emerging technology, shared information, and innovative solutions to address cyber risk.

To aid in the defense of the region's critical infrastructure, the coalition is committed to creating uniquely designed deliverables that include:

- Practical hands-on experiences
- Capstone design projects
- Realistic scenario-based table-top and testbed-based exercises
- Inquiry-based cyber defense competitions
- Necessary supporting educational materials

ReCIPE Partners

Partner Institution: University of Illinois at Urbana-Champaign
POC: David M. Nicol
Email: dmnicol@illinois.edu

Partner Institution: Moraine Valley Community College
POC: John Sands
Email: sands@morainevalley.edu

Partner Institution: University of Colorado Colorado Springs
POC: Tejay Gurvirender
Email: gtejay@uccs.edu

Other Partners

ReCIPE will be joined in this effort by a number of additional industry, government, and community partners, to include: the Association of Illinois Electric Cooperative, MidAmerican, Illinois Manufacturers Association, Collins Aerospace, Iowa National Guard, Iowa Homeland Security and Emergency Management, City of Ames, Illinois National Guard, and Argonne National Laboratory.

COMMUNITY DEVELOPMENT INITIATIVES

North Carolina Partnership for Cybersecurity Excellence (NC-PaCE) (Awarded in FY 2021)

Lead Institution: North Carolina State University
POC: Laurie Williams
Email: lawilli3@ncsu.edu

Initiative Description

The economic imperative of cybersecurity has never been more clear. Cybersecurity expertise is in high demand. Employers are desperate for cybersecurity expertise to protect citizens, companies, and the nation; but also to enable organizations for economic growth or to prevent organizations from being crushed with the reality of cybersecurity requirements. The supply for cybersecurity expertise is not keeping pace with the demand, especially in NC.

NC-PaCE's overarching goal is to develop and implement a cybersecurity strategy for the commercial industrial sector, state government agencies, and the Defense Industrial Base (DIB) in North Carolina, and to establish the state as a national leader in cybersecurity. The strategy includes the development of a state-wide cybersecurity ecosystem through education and workforce development, innovative research, effective service, and community outreach.

This initiative will serve the NC industrial sector and government agencies' needs in cybersecurity research and services, and at the same time, create educational opportunities to develop a diverse workforce with cybersecurity skills that will serve the North Carolina community today and in the future.

NC-PACE Partners

Partner Institution: East Carolina University
POC: Dr. Kamran Sartipi Dr. Te-Shun Chou
Email: sartipik16@ecu.edu chout@ecu.edu

Description

East Carolina University (ECU) and its Center for Advanced Manufacturing and College of Engineering and Technology (CET) faculty will provide a range of advanced training and services to industries to promote their knowledge and skills in outpacing information attackers who are becoming increasingly intelligent and effective. The Computer Science Department will establish a new cybersecurity stream, offer two or three courses at the second, third and fourth years, and will practice the empirical aspects of cybersecurity training through major team projects in the courses. ECU will extend the mission of the ECU's CET with a cloud center and virtual training of students at statewide colleges and universities, as well as regional industries and governments.

Partner Institution: Forsyth Technical Community College
POC: Thomas W. Brown III
Email: tbrown@forsythtech.edu

Description

Forsyth Technical Community College (FTCC) will enhance the cybersecurity curriculum and increase the number of completions of cybersecurity certification testing. FTCC will review current curriculum and work to implement supplemental modules for courses. FTCC will enhance the cybersecurity certification testing process by providing guidance on testing procedures and processing testing vouchers.

COMMUNITY DEVELOPMENT INITIATIVES

Partner Institution: North Carolina A&T
POC: Dr. Hossein Sarrafzadeh Dr. Mohd Anwar
Email: hasarrafzadeh@ncat.edu manwar@ncat.edu

Description

North Carolina A&T's (NCAT) goal is to develop and implement a cybersecurity strategy for the commercial industrial sector, state government agencies, and the Defense Industrial Base (DIB) in North Carolina.

Partner Institution: University of North Carolina at Wilmington
POC: Dr. Ulku Clark Dr. Geoff Stokerr Jeff Greer
Email: clarku@uncw.edu stokerg@uncw.edu greerj@uncw.edu

Description

UNC-Wilmington will support the NC-PaCE leadership team with specific requirements, promote and oversee UNCW support of semiannual state-level cybersecurity symposia, and recruit regional government, industry, and academic organizations to the NC-PaCE coalition.

Partner Institution: University of North Carolina at Charlotte
POC: Dr. Bill Chu
Email: billchu@uncc.edu

Description

UNC-Charlotte will provide project management of the outreach projects, as well as coordinate project activities at the other sites, provide outreach to local communities, and provide project-reporting support.

Partner Institution: Pitt Community College
POC: Dr. Greg Robison Joseph Jeansonne
Email: grobison@email.pittcc.edu jjeansonne@email.pittcc.edu

Description

Pitt Community College (PCC) will recruit new members into NC-PaCE, establish regional communities-of-practice, and conduct a gap analysis of the cybersecurity needs of the state. Additionally, PCC will develop a scholarship program to enable deserving students to take security certification exams and provide student internship sponsorship for community college cybersecurity students.

Partner Institution: Wake Technical Community College
POC: Dr. Keith Babuszczak Carolyn DeSimone
Email: kbabuszczak@waketech.edu cgdesimone@waketech.edu

Description

Wake Tech IT Division faculty members will write curriculum and learning materials for topics/courses identified by a consortium-wide gap analysis. The courses and enhancements will be applied to courses currently being taught; courses approved by the North Carolina Community College System but are not yet part of our Cybersecurity degree/certificate programs, and courses that may be newly proposed for approval by the North Carolina Community College System. Faculty members will write lessons and develop materials to support students in preparation for certification exams.

COMMUNITY DEVELOPMENT INITIATIVES

Improving Indiana's Local Cybersecurity Infrastructure (Awarded in FY 2021)

Lead Institution: Purdue University
POC: Mat Trampski
Email: mtrampski@purdue.edu

Initiative Description

Indiana local governments and the K-12 education institutions that serve those communities have increasingly become the targets of cyberattacks. Efforts have been undertaken by Indiana local governments and within its K-12 communities to improve cybersecurity postures, but these efforts have not been coordinated among those entities and the communities they serve. While Indiana K-12 systems currently utilize information and educational material from multiple sources, including private IT providers, Cyber.org, Project Lead the Way (pltw.org), and the Indiana Department of Education to educate students, train school staff, and advance their cybersecurity postures, there is no unifying principle or centralized guidance as to which services or providers will best meet those organizations' needs.

Similarly, Indiana's local governments rely on information, tools, and training from private IT providers, the Governor's Executive Council on Cybersecurity's Local Government Working Group, MS-ISAC, and others. Though Center for Education and Research in Information Assurance and Security (CERIAS) and Purdue University Technical Assistance Program (TAP) participate actively in both spaces, cybersecurity efforts in both spaces are fragmented, lack sufficient funding, and are not making full use of Purdue's expertise to advance cybersecurity among these populations.

To enhance cybersecurity maturity in Indiana's local governments and their K-12 educational partners, this initiative will create an infrastructure that coordinates the numerous activities required to create and maintain mature cybersecurity postures among these groups, directs the appropriate resources to needful organizations, and provides uniquely expert cybersecurity resources where required. The goal of this work will be to reduce the number and severity of cybersecurity incidents in Indiana's K-12 school systems and Indiana local governments by increasing communication among these groups and increasing the cybersecurity maturity of entities in these populations.

To meet these goals, this initiative will:

- Facilitate increased cybersecurity-focused communication and relationships among Indiana's local government officials, personnel from the Indiana Department of Education and Indiana Office of Technology, K-12 school district IT representatives, and cybersecurity experts at Purdue University
- Provide direct cybersecurity risk management support to selected local governments and K-12 districts in Indiana through cybersecurity assessment
- Adapt, create, and assist with the implementation of cybersecurity-related policies, procedures, tools and training to the needs of these populations and to specific local governments and K-12 districts in Indiana.

This program will significantly advance cybersecurity maturity in the target populations by providing more financial resources and greater technical and risk management resources. Gains in cybersecurity maturity will be enhanced and made robust through the creation of a community of diverse experts to guide continued work through the next decade.

COMMUNITY DEVELOPMENT INITIATIVES

Cybersecurity Education for Critical Infrastructure Protection through Regional Coalition (Awarded in FY 2021)

Lead Institution: University of Memphis
POC: Dipankar Dasgupta
Email: dasgupta@memphis.edu

Initiative Description

This initiative's mission is to prepare the current and next generation of professionals on complex cyberattacks on industry-specific critical infrastructures and how to identify and handle emerging threats. Led by the University of Memphis, a coalition of CAE-C institutions will develop a comprehensive sector-specific cybersecurity program to better prepare for incident response and recovery in crisis.

The overall project goal is to design and develop a multi-disciplinary critical infrastructure cybersecurity program to address the technical needs of NCAE-C students (future workforce), state and local government, and industry partners in energy, water and wastewater systems, as well as related Critical Infrastructure sectors. The initiative objectives include:

- Designing and developing an education and outreach program to enhance cybersecurity expertise for critical infrastructure security professionals in state and local government and industry, with an emphasis on energy, water and wastewater systems, and related CI sectors across the NCAE-C Southeast Region
- Developing and delivering competency-based training courses and workshops to upskill and reskill professionals in those organizations that leverage the expertise of the NCAE-C coalition to provide fundamental knowledge, skills, and competencies to critical infrastructures
- Providing educational experiences for NCAE-C students to enhance their expertise and future support of CI security through specialized courses and seminars, internships to support the proposed cybersecurity consultation and services for the region's government and industry critical infrastructure partners, and opportunities to network with the region's critical infrastructure partners to expand workforce development pathways

The successful outcome of this project will create a strong southeast regional coalition, leveraging the CAE-C institutions' expertise in cybersecurity in assisting local and state governments and critical infrastructure partners in the region and the nation. Moreover, this cybersecurity community development project will design activities to be continued with supports from our industry partners beyond the project period as outlined in the proposal.

COMMUNITY DEVELOPMENT INITIATIVES

Critical Infrastructure Protection Partners

Partner Institution: University of West Florida
POC: Dr. Guillermo Francia Dr. Eman El-Sheikh
Email: gfranciaiii@uwf.edu eelsheikh@uwf.edu

Description

University of West Florida (UWF) will manage and implement program goals and initiatives, to include: the analysis, design, and development of course curriculum, tabletop exercises, and labs, and certificate and digital credentialing; overseeing implementation and evaluation of effectiveness of the courses; assisting in dissemination of course materials for widespread adoption; and assisting with preparation of annual reports.

Partner Institution: North Carolina A&T State University
POC: Dr. Xiaohong Yuan Dr. Kaushik Roy
Email: xhyuan@ncat.edu kroy@ncat.edu

Description

North Carolina A&T State University (NCAT) will be responsible for overall project direction and coordination; assuring successful project completion; arranging workshops and overseeing research activities; course curriculum development; teaching a cybersecurity course; and recruiting supervising students for the program.

Partner Institution: The Citadel, The Military College of SC
POC: Dr. Shankar Banik, Dr. Cory Nance, Dr. Melissa Graves
Email: shankar.banik@citadel.edu, cnance@citadel.edu, mgraves2@citadel.edu

Description

The Citadel will be responsible for leading the successful implementation of the initiative, curriculum development, organizing the summer workshop to train faculty on the developed modules, and designing case scenarios for cyber tabletop exercises for critical infrastructure.

Partner Institution: Indian River State College
POC: Dr. Kevin Cooper
Email: kcooper@irsc.edu

Description

Indian River State College (ISRC) will co-develop, deliver, and evaluate courses within this initiative.


NCS
NATIONAL
CRYPTOLOGIC
SCHOOL