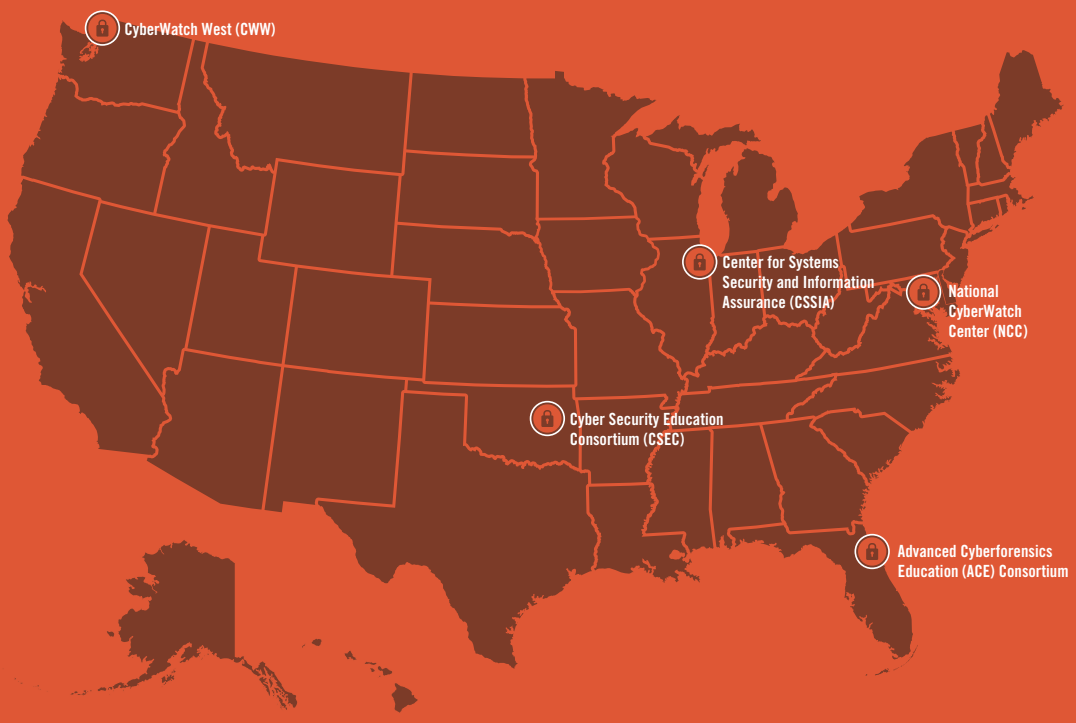
ATE CENTERS

ATE CENTERS FOR
CYBERSECURITY EDUCATION



This publication was produced by the Division of Academic and Student Affairs of the Maricopa County Community College District with support from the National Science Foundation under grant **DUE-1261893**.

For additional information about the ATE program, visit **www.nsf.gov/ate**.

For additional information about the ATE centers and projects, visit **www.atecenters.org**, **www.atecentral.net**, and **www.aacc.nche.edu/ateprogram**.

The National Science Foundation's Advanced Technological Education (ATE) program provides grants that support the development of innovative approaches for educating highly skilled technicians for the industries that drive the nation's economy. The program funds educational initiatives across the full range of high-tech fields—biotechnology, chemical technology, engineering technology, advanced manufacturing, energy and environmental technology, information technology, and others.

Two-year college educators lead most ATE initiatives because public community and technical colleges are the major sources for technician education in the United States. The program also encourages partnerships with employers, universities, and secondary schools. As a result, the innovations that ATE grantees devise and test are model programs that reach students from secondary schools to community colleges and universities. They also generate career pathways for students to follow from certificate and degree programs to employment in established and emerging industries.

ATE grantees focus on boosting both the quantity and quality of technicians in the workforce. They test new ways of teaching about established and emerging technologies. Results include new instructional modules, new courses, and entire certificate and degree programs. In tandem with creating products to improve students' learning, many ATE grantees offer professional development for faculty. Through these opportunities, community college instructors and secondary school teachers learn about cutting-edge technologies and how to utilize proven teaching techniques to meet a wide array of industry-identified needs for the workforce.

The ATE program funds large, comprehensive Centers of Excellence, as well as smaller-scale, more focused projects. Each ATE Center generally involves a collaboration among several educational institutions, along with partners from business, industry, and government, all of which work together to improve education and build the workforce in a particular area of technology. The approximately 40 ATE Centers provide leadership, have a broad impact, and act as resources for curricula and faculty development either within a defined geographic region or across the nation.

Complementing the broad missions of the ATE Centers, approximately 300 smaller project grants focus more narrowly on specific aspects of technician education, such as developing or improving educational materials, learning environments, courses, and curricula; providing professional development for educators; preparing future K-12 teachers with strong backgrounds in technology; or giving students the business and entrepreneurial skills needed to succeed in the modern workplace.

> *"AACC is proud to serve as a long-standing partner of the National Science Foundation's ATE program, which provides invaluable support to our nation's community colleges enabling them to expand institutional capacity, develop effective collaborations with industry, and strengthen innovative STEM technician education programs across the country."*
>
> ***Walter G. Bumphus***
> *President & CEO, American Association of Community Colleges*

ATE CENTERS FOR CYBERSECURITY EDUCATION

Advanced Cyberforensics Education (ACE) Consortium | Daytona Beach, FL

www.cyberace.org

The ACE Consortium involves over a dozen institutions across Florida, Georgia, South Carolina, and North Carolina. The primary goals are to develop and disseminate cyberforensics curricula, provide professional development for faculty members, and create interest in cybersecurity among high school students.

Center for Systems Security and Information Assurance (CSSIA) | Palos Hills, IL

www.cssia.org

This resource center for colleges across the nation focuses on providing faculty development and a cutting-edge virtual teaching and learning environment. CSSIA's Faculty Development Academy has offered courses and workshops (both face-to-face and online) for thousands of educators. CSSIA's virtual teaching and learning environment has been adopted by several hundred educational institutions and is also used extensively for cybersecurity student competitions.

Cyber Security Education Consortium (CSEC) | Tulsa, OK

www.cseconline.net/2014/

This regional center has over 40 active two-year program sites in eight states, with over 100 active faculty members offering courses based on CSEC's core information assurance and forensics curriculum, which encompasses information assurance principles, secure electronic commerce, network security, enterprise security management, and digital forensics. Particular emphases are automation and control systems security and mobile-device security.

CyberWatch West (CWW) | Bellingham, WA

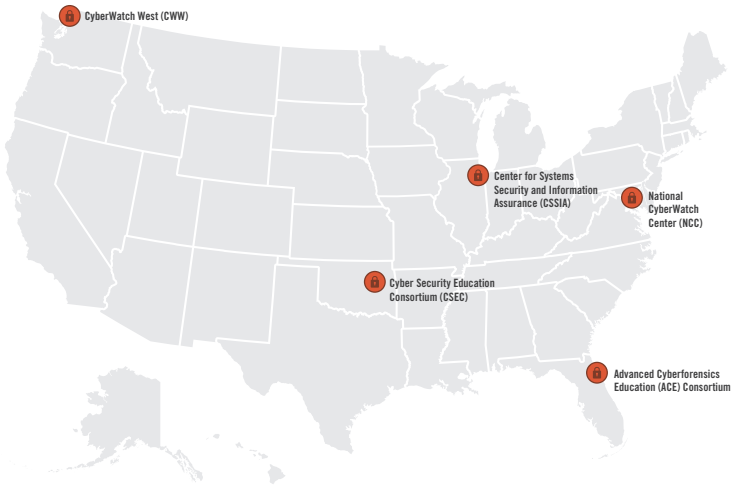
www.cyberwatchwest.org

This regional center focuses on cybersecurity education and workforce development in 14 Western states. Activities include providing model curricula, offering workshops for faculty, facilitating student participation in intercollegiate cyber defense competitions, and mentoring community colleges that aim to achieve designation as a National Center of Academic Excellence in Cyber Defense—2-Year Education (CAE-2Y).

National CyberWatch Center (NCC) | Largo, MD

www.nationalcyberwatch.org

This national center cultivates collaborations among educational institutions, businesses, government agencies, and professional organizations to grow and strengthen cybersecurity education programs and the cybersecurity workforce. NCC's network includes over 200 two-year and four-year institutions in almost all 50 states. Key initiatives include developing and updating cybersecurity degree and certificate programs in cyber defense, network forensics, network security administration, secure software development, and systems security administration; mapping curricula to federal and industry knowledge-and-skill standards, job roles, and professional certifications; and creating model transfer pathways that allow students to move between two-year and four-year degree programs.



This publication was produced by the Division of Academic and Student Affairs of the Maricopa County Community College District with support from the National Science Foundation under grant **DUE-1261893**.

For additional information about the ATE program, visit **www.nsf.gov/ate**.

For additional information about the ATE centers and projects, visit **www.atecenters.org**, **www.atecentral.net**, and **www.aacc.nche.edu/ateprogram**.

ACE

Advanced Cyberforensics Education Consortium

DAYTONA STATE COLLEGE | DAYTONA BEACH, FL

www.cyberace.org

- Offers comprehensive curriculum to bootstrap course offerings at 12 partner institutions in Florida, Georgia, and the Carolinas.
- Provides online faculty professional development.
- Creates workshops and certificate programs for workforce retraining.
- Partners with K-12 schools and other organizations to engage students.

ACE Engages Students in Cybersecurity & Cyberforensics

ACE holds cyber camps for ninth-to-twelfth graders to promote cybersecurity skills and encourage enrollment in STEM fields in college. To recruit and retain more female students, ACE revised its camps. This resulted in a 44% female participation rate in the summer 2015 camp attended by 60 students. Altogether more than 250 students have completed one of the six camps conducted since 2013.

For college students ACE offers five courses consisting of 150+ video lectures and scenario-based assignments. Students learn to combine "real-life" technical skills with advanced report writing, a skill that is often lacking among technicians in advanced technology fields.

High school students use teamwork during an ACE cyber camp competition.

DOD Recognizes Quality of ACE Courses

With Daytona State College's recent accreditation as a Center of Digital Forensics Academic Excellence by the US Department of Defense's Cyber Crime Center's Academic Alliance, ACE has external evidence of the high quality of its curriculum. More than 1,500 college students have completed at least one of ACE's five courses since 2012.

ACE Provides Resources for Faculty Development

Cyberforensics is an emerging field, and as such, there is a shortage of faculty members with the necessary skill set. ACE provides faculty development through a series of four self-paced, online courses. Faculty members are urged to use the resources on its learning management system—video lectures, assignments, and quizzes—to bootstrap course offerings at their home institutions. In 2015 ACE's learning management system had 110 registered educators from 58 institutions across 25 states. ACE also provides institutions with mentoring and funding for cyber-related activities. Professional development and additional funding have resulted in new courses in cyberforensics being offered at ACE institutions, as well as cyber camps for college and high school students.

> *"The Advanced Cyberforensics Education Consortium has partnered with non-profit organizations to provide 9-12 grade students with real-world, practical, and engaging educational programs. These programs educate and enable students to transition seamlessly into cybersecurity degree programs, careers, and other areas of technical mentorship."*
>
> *Lee V. Mangold, Vice President*
> *Florida Cyber Alliance*

A technician uses a hardware write-blocker while creating a forensic copy of a hard drive.

ACE Expands Cyberforensics Knowledge

ACE has been developing cyberforensics skills among faculty and students since 2012.

# of partner institutions
12
in 4 states

# of ACE course completers
1,500

# of faculty in training
110
in 25 states

# of K-12 competing in cyber camps
250

CSSIA

National Center for Systems Security and Information Assurance

MORAINE VALLEY COMMUNITY COLLEGE | PALOS HILLS, IL

www.cssia.org

KEY ACTIVITIES

- Operates a national faculty development academy that provides innovative cybersecurity curriculum.
- Conducts research on the use of virtual reality in cybersecurity instruction.
- Develops outreach and support of a national pipeline that encourages enrollment of minority, female, and veteran populations.

Multifaceted Approach Prepares Students for Cybersecurity Careers

CSSIA uses a three-pronged approach to student success.

Its virtual teaching and learning environment engages students in experiential learning. By working in CSSIA's safe "sandbox" environment separate from colleges' networks, students across the US are learning the skills required in today's challenging cybersecurity profession.

By developing and expanding student cybersecurity skills competitions, CSSIA enables students to leverage the knowledge and skills they learn in classrooms and to hone their workforce abilities.

CSSIA's partnerships with the Association of Computer/Information Science Engineering Departments at Minority Institutions and the Society for Advancement of Chicanos/Hispanics and Native Americans in Science connect minority and underrepresented populations to cybersecurity workforce opportunities.

In cybersecurity competitions students defend networks from attacks like those that companies face.

CSSIA Virtual Environment Provides Instructors with Up-to-Date Resources

CSSIA prepares the next generation of cybersecurity practitioners by incorporating current technologies, equipment, and products into its virtual teaching and learning environment. The virtual teaching and learning center continuously evolves and partners with major vendors to provide instructors with resources that incorporate technologies, equipment, and products used in today's information systems.

The CSSIA virtual teaching and learning environment has been adopted by 250 educational institutions. Instructors at these institutions impact more than 10,000 students enrolled in cybersecurity courses, certificate programs, and two-year degrees. Students who use the virtual environment develop problem solving, network defense, and troubleshooting skills that are critical for today's cyber workforce.

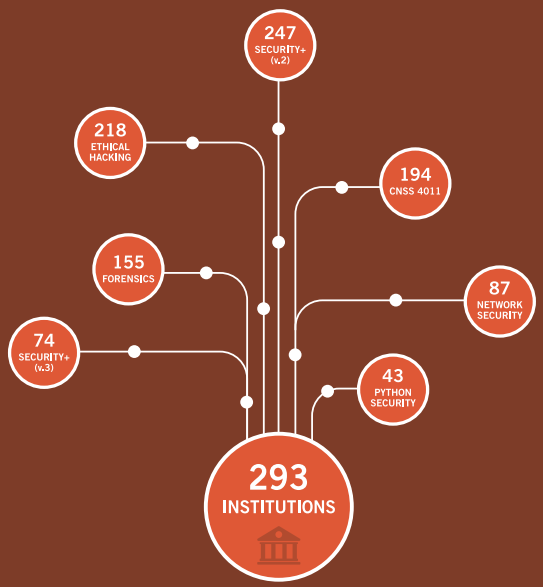
CSSIA's virtual gymnasium is also utilized by several national cybersecurity student competitions. These competitions connect students with employers, who assist with these events. Employers evaluate students' knowledge, technical skills, teamwork, and problem solving in the cyber attack situations posed within the dynamic competition environment. Aside from the opportunity to interact with employers, the competitions broaden students' employability by enabling them to incorporate virtualization in their learning.

> *"In today's environment where data breaches make daily headlines, well-trained, qualified cybersecurity practitioners need a place to learn their trade. Centers like CSSIA provide the research, focus, and resources that enable our nation's cybersecurity programs to be effective."*
>
> *Nathan Evans, Cyber Operation and Analysis Lead*
> *Argonne National Laboratory*

Technicians review specifications on equipment being deployed.

Use of CSSIA Courses Spreads

Since 2011, 293 higher education institutions have utilized one or more of CSSIA's courses.



CSEC

Cyber Security Education Consortium

UNIVERSITY OF TULSA | TULSA, OK

www.cseconline.net/2014/

CSEC

KEY ACTIVITIES

- Cultivates a highly skilled cyber workforce.
- Helps reverse offshoring and outsourcing.
- Develops and disseminates high quality cybersecurity curricula.
- Offers faculty development programs to eight states.
- Creates physical system and mobile communication device centers of excellence.

CSEC Advances Cybersecurity & Homeland Defense

CSEC's centers of excellence serve as hubs for education and economic activity in strategic technology areas such as physical systems, secure coding, and mobile communication devices.

In addition to educating 1,500 security degree majors, CSEC institutions helped 721 incumbent workers upgrade their physical system and cybersecurity skills during 2014-15. These workers included Department of Defense employees and federal, state, and local law enforcement personnel. They completed intense multi-day programs in mobile and embedded device forensics that align with industry certifications. Due to their expertise and hands-on experience, CSEC graduates are highly sought after by business, industry, government, the military and intelligence community.

Oklahoma State University Institute of Technology students assess a telecommunications network's performance.

> *"Demand for highly trained cybersecurity industry professionals is at an all-time high ... It is imperative that we support and establish strong educational programs which aim to develop cybersecurity professionals so that we can keep pace in combating this global concern."*
>
> *Scott Fry, Director of Workforce Development*
> *MidAmerica Industrial Park*

Faculty Expertise Supports Economic Development

CSEC began in 2004 with 11 cybersecurity instructors at eight Oklahoma institutions. As a result of its successful initiatives, CSEC now has 43 active two-year program sites in eight states with 111 active faculty members offering courses based on CSEC's core information assurance and forensics curriculum. Altogether 408 faculty have attended CSEC professional development; they have developed 70 distinct courses.

CSEC institutions offer rigorous cybersecurity curricula encompassing information assurance principles, secure electronic commerce, network security, enterprise security management, and digital forensics. CSEC is now creating centers of excellence in automation and control systems and mobile communications device. The University of Tulsa also developed three state-of-the-art forensics courses, and five CSEC institutions have developed automation and control systems curricula.

CSEC's centers of excellence serve as hubs for education and outreach activities in strategic technology areas, providing launching points for job growth and spin-off companies.

CSEC graduates maintain retinal scanners and operate other security system equipment.

CSEC Delivers Security-Credentialed Technicians to the Workforce

Students enrolled in CSEC programs can earn industry certifications, associate or bachelor degrees.

1,502
2015 DECLARED SECURITY MAJORS

1,249
ASSOCIATE DEGREES (2004-15 GRADUATES)

1,663
INDUSTRY CERTIFICATIONS (2004-15 GRADUATES)

308
BACHELOR DEGREES (2004-15 GRADUATES)

2,982
2014-15 SECURITY RELATED ENROLLMENTS

CWW

CyberWatch West

WHATCOM COMMUNITY COLLEGE | BELLINGHAM, WA

www.cyberwatchwest.org

KEY ACTIVITIES

- Leads academic institutions' efforts to strengthen cybersecurity education and workforce infrastructure in 14 western states.
- Facilitates student participation in inter-collegiate cyber defense competitions.
- Maps curriculum to national standards.
- Mentors and provides resources to faculty.
- Involves industry partners as speakers, for internships, and in regional cyber risk summits.

CWW Puts Students on Path for Success

In 2014, 1,407 students enrolled in security programs at CWW core institutions—Whatcom Community College; California State University, San Bernardino; California State Polytechnic University, Pomona; Coastline Community College. Of these students, 341 completed the program, and 985 are still enrolled; 71% were minorities.

Since its inception in 2011 CWW has offered 17 skill-building workshops for 267 member-college faculty. Topics have included Certified Ethical Hacker and forensics. Faculty also received mentoring to build courses using virtual repositories for images. CWW makes new curriculum resources, such as 13 open source courses on critical infrastructure security and resilience, available to faculty via its website.

Students in an industrial control systems security class identify programmable logic controller vulnerabilities.

> *"As a founder of two West Coast-based information security businesses it's crucial that CWW exists to help fill the talent gap that currently exists."*
>
> *Kris Rides, CEO & Founder*
> *Tiro Security, LLC*

CWW Builds Capacity

During the fall 2014 National Cyber League competition, students participated online in a "capture-the-flag" exercise using skills that included web application exploitation, network traffic analysis, recon, scanning, and enumeration to find and retrieve files containing passwords (flags). Of the 1,368 students who participated—a 48% increase over the previous year—1,040 (76%) captured at least one flag. Through participation in such competitions, students develop and validate cybersecurity skills that are valued by employers.

CWW has expanded its membership and services into 14 states, contributed to increasing the number of Centers of Academic Excellence for two- and four-year institutions, supported the development of a thriving cybersecurity education community, and enhanced the cybersecurity workforce through these combined efforts.

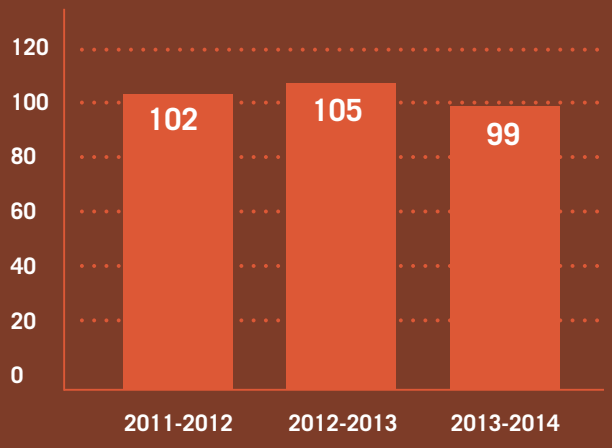
CWW Shares Expertise with Industry

CWW's positive economic impact extends to its work with various industry sectors to help employers protect their companies from cyber attacks. In 2014 three core CWW institutions held Cyber Risk Summits. A total of 605 people attended including CEOs, CTOs, and personnel from businesses' human resources, accounting, and legal departments. Participants learned how to assess their companies' vulnerabilities and develop risk mitigation solutions.

Troubleshooting is a key skill covered in CWW's curriculum.

CWW Increases Student Internship Placements

CWW has consistently exceeded its goal of placing at least 25 additional students each year in internships beyond the 54 interns it had placed annually when its ATE grant started.



NCC

National CyberWatch Center

PRINCE GEORGE'S COMMUNITY COLLEGE | LARGO, MD

www.nationalcyberwatch.org

NATIONAL CYBERWATCH CENTER

KEY ACTIVITIES

- Leads collaborations to strengthen cybersecurity education workforce.
- Sets educational, training, and assessment standards for the information security field.
- Validates cybersecurity skills using performance-based assessments.
- Develops new skills-based learning curricula tied to job roles and industry certifications.

NCC Collaborations Benefit Students

NCC cultivates collaboration by coordinating broad national networks that involve students, schools, alumni, industry, and government partners.

Thousands of students and hundreds of faculty participate in the annual National Cyber League (NCL). This event provides an ongoing virtual training ground for collegiate students and faculty to develop, practice, and validate cybersecurity knowledge and skills. These high-fidelity simulation environments contain content aligned with industry certifications.

The National Cybersecurity Student Association advances students' educational and professional development with activities, networking, and collaboration.

Model transfer pathways include lateral and reverse transfers, as well as transitions between two-year and four-year institutions.

College students from the Mid-Atlantic region setup and harden networks at the Collegiate Cyber Defense Competition.

NCC Increases Quantity & Quality of Community College Information Security Programs

By fostering a culture of collaboration and innovation amongst industry, government, and academia, NCC's leadership has increased the quantity and quality of community college information security programs nationwide.

This large network has more than 200 partners from higher education institutions, public and private schools, businesses, and government agencies. It focuses on a coordinated approach for advancing cybersecurity education and strengthening the national cybersecurity workforce.

For example, NCC-led initiatives

- facilitated new and updated information security degree and certificate programs. Thanks to the national effort, programs are mapped to federal work roles and industry-recognized professional certifications;
- helped set public and private-sector information security standards related to job roles and a common lexicon; and
- developed a comprehensive support and technical assistance system for institutions that need to re-designate, as well as those that are new to the National Security Agency/Department of Homeland Security National Centers of Academic Excellence in Cyber Defense program.

> *"With resources and technical assistance provided to us by the National CyberWatch Center, we were able to obtain our re-designation as a National Security Agency/ Department of Homeland Security National Centers of Academic Excellence in Cyber Defense Two-Year Education through 2021."*
>
> *Aaron Tanaka, Professor of Computing, Electronics & Networking Technologies Honolulu Community College*

Students add physical security to a mock pharmaceutical dispensary for a cybersecurity simulation.

National Cyber League Participation Grows

College students' participation in the National Cyber League grew at a steady pace from 2013 through 2015.