BEYOND DESIGNATION

Practices, Resources, and Pathways for Continued Growth and Lasting Impact as a Center of Academic Excellence in Cyber

EDITED BY **ZOE FOWLER, PHD**

Beyond Designation is a publication by
DoW Cyber Academic Engagement Office and
the National Centers of Academic Excellence in Cybersecurity.

Contents

Acknowledgments

Foreword *Scott Nelson*

The CAE Community *Dr. Tony Coulson*

Introduction *Dr. Zoe Fowler*

Beyond Designation Practices of Excellence

Advisory Boards
- CASE STUDY: **Bossier Parish Community College** / 1

Careers and Student Services
- CASE STUDY: **Moraine Valley Community College** / 9
- CASE STUDY: **Montreat University** / 12
- CASE STUDY: **Florida Agricultural and Mechanical University** / 13

Community Outreach
- CASE STUDY: **Florida State University** / 20
- CASE STUDY: **Metropolitan State University** / 21

Competitions
- CASE STUDY: **California State University Chico** / 27

Cyber Clubs
- CASE STUDY: **College of Coastal Georgia** / 39
- CASE STUDY: **Cal Poly Pomona** / 40
- CASE STUDY: **Eastern Washington University** / 42

K12 Engagement
- CASE STUDY: **Cedarville University** / 47
- CASE STUDY: **Florida State University** / 50

Regional Engagements
- CASE STUDY: **University of Colorado, Colorado Springs** / 55

Student Security Operations Centers
- CASE STUDY: **Coastline College** / 61
- CASE STUDY: **The Citadel** / 63

Using AI
- CASE STUDY: **California State University San Bernardino** / 69

CAE Resources

CLARK Curriculum / 75

Grants / 78

New and Early-Career Faculty Development / 85

XP Cyber / 88

Conclusion / 92

Acknowledgements

As with the majority of initiatives across the CAE Community, the Beyond Designation Handbook grew out of a collaborative effort, and I am deeply grateful to everyone who contributed to its success.

My sincere thanks go to Marina McClelland, Robert Young, Renita Wigfall, Omar Garada, and Carolyn Vernan for their invaluable work as interviewers and fact-finders, as well as to Lindsey Castin, John 'Chip' Bircher, and David Zou for their vital support across the wider team. I am also grateful to our Office Director, Scott Nelson, whose leadership and organizational support created the environment that made this project possible.

This handbook would not exist without the generous participation of everyone who agreed to be interviewed; it is their willingness to share their insights, ideas, and experiences that is the foundation of this work. Finally, I want to recognize the broader NCAE cyber education community, whose daily dedication defines, demonstrates, and drives forward academic excellence in cyber, ultimately forging the future cyber warriors who will safeguard our nation's critical digital infrastructure and contribute to the enduring national security of the United States.

Foreword

Scott Nelson,
Principal Director of the DoW Cyber Academic Engagement Office

Throughout American history, academic institutions have been indispensable partners in the defense of the nation. They are not only places of learning, but also engines of discovery, reservoirs of expertise, and proving grounds for the talent and ideas on which national security depends.

During the Second World War, the United States and its Allies mobilized mathematicians, linguists, engineers, physicists, and scholars from across the academic community. Their expertise helped break adversary codes, advance radar and communications, and solve complex scientific and operational problems. In the decades that followed, the nation again turned to its universities and colleges to support the space program. Academic researchers, educators, laboratories, faculty, and students helped develop the technologies, systems, and human expertise that ultimately placed Americans on the Moon.

These achievements resulted from a national commitment to bring government, industry, and academia together around missions of extraordinary importance: government established priorities and requirements; industry transformed ideas into operational capabilities; academic institutions supplied research, innovation, intellectual diversity, and generations of talented Americans prepared to serve.

Our nation faces another such moment today. Cyberspace is now central to military operations, critical infrastructure, economic prosperity, and daily life. Strategic competitors are investing aggressively in cyber capabilities, artificial intelligence, quantum technologies, autonomous systems, and techniques designed to disrupt the systems on which our society and military depend. This is not solely about technology, it is about people, the scientists, engineers, educators, operators, analysts, policymakers, and leaders capable of turning knowledge into national advantage.

The Department of War (DoW) Cyber Academic Engagement Office (CAEO) serves as the Department's focal point for coordinating and integrating universities, colleges, and academic institutions into the cyber mission. Working with partners across government and industry, CAEO helps mobilize academic capacity, cultivate talent, operationalize partnerships, integrate efforts, and accelerate innovation in support of Department and national-security requirements.

This work must move beyond engagement for its own sake. Academic partnerships solve real problems, develop mission-ready talent, and create measurable value. The National Centers of Academic Excellence in Cybersecurity (NCAE-C) represent one of the nation's most important assets in defending our nation's cyberspace. This community of universities and colleges connects students, faculty, researchers, employers, communities, and government missions across the country. Its institutions educate the cyber workforce, expand pathways to public service, strengthen local and regional ecosystems, advance research, and help the nation anticipate emerging technologies and threats.

This book captures best practices developed throughout that remarkable community. It presents lessons from institutions that have built strong cybersecurity programs, aligned education with workforce needs, created meaningful student experiences, strengthened partnerships, and translated academic excellence into public value. These practices deserve to be shared, adapted, and scaled. The best practices presented in this volume also demonstrate that excellence does not require every institution to look the same. Community colleges, minority-serving institutions, research universities, liberal arts colleges, technical institutions, and regional universities each bring distinctive strengths. That diversity of geography, mission, perspective, and expertise is a strategic advantage.

The historic mobilizations of the twentieth century remind us that America's greatest advantage has never been technology alone. It has always been our ability to assemble talented people and institutions around a common purpose. The codebreakers of the Second World War and the pioneers of the space program succeeded because the nation recognized academic capability as a strategic resource and connected it to clearly defined missions.

We must now bring that same sense of urgency and purpose to cyberspace. The NCAE-Cs are more than a collection of designated institutions. They are a national network of talent, knowledge, innovation, and service. By learning from their best practices and strengthening the partnership among academia, industry, and government, we can better prepare the nation for the challenges ahead.

This work is not only about educational excellence. It is about national preparedness, mission readiness, and ensuring that the United States can draw upon the full strength of its academic institutions. Most importantly, it is about preparing a new generation of Americans to defend our security, prosperity, and freedom in a rapidly changing world. •

The Importance and Power of the CAE Community

Dr. Tony Coulson

Why the CAE Community Matters

The United States has a persistent shortage of qualified cyber professionals, once estimated at more than 500,000 unfilled positions nationally in 2021 testimony before the House Committee on Homeland Security. But the deficit is not the story. The story is what fills it. No single university or college, no single agency, nor any company has been able to build a scaled, credentialed, continuously renewed cyber talent pipeline on its own, and no single top-down federal program has managed it either, until now. The CAE Community has over 500 colleges and universities working in direct, standing partnership with the National Security Agency and the DoW's Cyber Academic Engagement Office. It does more than train and educate students and the broader workforce. It runs applied research on live national security problems, helps federal and state governments define what a cyber workforce is supposed to look like, and invents new ways to meet workforce needs in emerging technologies. Nothing on that scale has been attempted since the Apollo moonshot.

Where and when else has the United States found more than 500 colleges and universities working together, with government and industry, in one national security mission? Nowhere else, and that is the point. This is not a program that was announced. It is a community that was built, through innovation, ideas to action, and notably, a small amount of money. It began in 1999 with seven schools. It is a working example of what a public, private partnership can produce when it is built for the nation and not for any single sponsor.

How It Works

Like the internet, the CAE Community was designed to be flexible, adaptive, and resilient. Not based on one technology, one vendor, one large contractor. The CAE Community was purposely built for the nation by combining the strengths of three institutions that rarely operate on the same clock or speak the same language: government, academia, and industry. Each brings something the others cannot supply on their own, mission and scale from government, research and talent development from academia, and investment and hiring demand from industry. The CAE Community's job is to turn those three strengths into mutual benefit and real understanding between the parties, and out of that understanding, a genuine synergy to innovate and solve problems none of the three could solve alone.

The Government's mission is to win. It operates through command and control, a structure that is efficient for its mission and a world away from a university faculty senate, and it ultimately serves the American People, not a shareholder. That is why the CAE Community's standard-setting work matters as much as any single class taught: its principal investigators sit on the DCWF 8140 committee that helps define the cyber work roles the Department of War and the United States use. It gives government what it actually needs, a workforce definition it can trust, built by the people doing the training and education.

Industry has a fiduciary duty to its shareholders. Hiring is good, but industry would rather treat it as an investment, and return on a workforce investment is notoriously hard to quantify. That tension is why a pipeline industry can actually see and measure matters more than another certificate program: the National Cybersecurity Virtual Career Fair (part of the CAE Community and National Cyber Training and Education Center) connects thousands of students to employers every year, students that meet cybersecurity education standards along with key experiences from competitions, apprenticeships, cyber ranges, and AI, covering the entire United States. The CAE Community turns an abstract ROI question into a concrete one, here are candidates, here is what they know, here is how to reach them.

Academia is perceived to resist the idea of producing workforce as its core mission. This is not a fact. The United States has the best higher education system in the world, one that thousands of students from around the world seek to take part in. Academia supports the nation by producing thinkers, ideas, and research. Often seen as slow and ponderous, academia is governed by committees, scholarship, curriculum, and outcomes assessment, a genuinely different logic than mission or ROI. The CAE Community works with that logic instead of overriding it. Communities of Practice let Cyber Defense, Cyber Operations, Research, and Cyber AI institutions coordinate with true academic peers, and the National Center runs the shared events, standards work, and a shared curriculum library, CLARK, without dictating what any individual faculty member teaches. This is an army of the willing, an army of the best educated subject matter experts in the United States, all part of a community built to educate and provide workforce.

Turning that synergy into real problem-solving is not a command-and-control exercise, it takes idea before action, every time. Give institutions the actual problem. Give them the freedom, and sometimes the funding, to experiment and show what works. Give them a real avenue for that work, not just a publication but a competition, a range, a device, room to actually play

with the problem. When someone comes up with a genuine idea, the job is to link them up with whoever else can use it and get out of the way. That order, idea before action, is what produces velocity: a good idea can move from one campus to the whole network faster than a new federal program could ever be authorized. National Security Agency seeded four cyber clinics through CAE grants, and the model has since drawn more than $25 million in private sector investment and opened clinics at 45 more institutions. That is the foundation of the CAE Community: Idea to Action.

The dynamic underneath all of it is closer to a recipe than a blueprint, and it is a good one. It calls for understanding the actual benefits each side is after, to the nation and to the localities where these institutions sit, to the industries that hire, real listening, genuine encouragement, the right incentive at the right moment, and enough boldness to try something that has not been tried before. Beaten, whipped, agitated, folded together, and given real heat, those ingredients have produced something worth sharing widely. There are hundreds of versions of this recipe across almost 500 institutions, each adapted to a different region and a different mission. What all of them produce, in the end, is something the whole country benefits from, not just the people who built it.

The Success

What this partnership produces is not just a credential. It is an education. A designated institution is accredited, peer-reviewed, and re-designated on a recurring cycle. It is accountable not for confirming a single skill but for whether a graduate can reason through a problem no one has seen yet, produce research that invents the future, and keep learning after the technology changes. That is what the nation is buying when it invests here.

That is not a self-assessment. The Office of the National Cyber Director, reporting in 2024 on the National Cyber Workforce and Education Strategy, wrote that the program "goes beyond accreditation as it sets the gold standard for cybersecurity education." The same report counted nearly 500 institutions, a 13 percent increase in one year, serving a projected 174,000 students annually.

Nor has the Community treated skills-based hiring as a threat. It has been the fastest mover on it, running registered apprenticeships, certificate and skills programs, high school dual credit, and accelerated degrees, fielded faster than any federal specification process could authorize them. That is the advantage of building skills programs inside accredited institutions rather than outside them. The student earns the skill an employer can hire tomorrow and the education that outlasts the tool.

That is the synergy in practice. Government gets a workforce definition it trusts and the critical skills behind it. Industry gets a pipeline it can measure and hire from. Academia keeps doing what academia does. All three reinforce one another instead of competing.

That had to be built, institution by institution, over more than a decade, which is why the alternatives have not managed it. Concentrating investment in a few elite research universities does not work: a 2021 Hewlett Foundation evaluation profiled the CAE Community by name, then 335 institutions, and concluded that "the assumption that elite universities are best placed to enable multidisciplinary cyber education is not borne out by our evidence." A single top-down federal program does not work at this scale either. The 2020 Cyberspace Solarium Commission report put it plainly: "sometimes success in building a robust federal workforce depends on elements outside of the federal government." Almost 500 institutions under real, recurring academic review is the approach that scaled.

The CAE Community is not a downstream beneficiary of federal funding. It is a direct, joint operation of the National Security Agency and the Department of War, built into the DoW's own workforce architecture. The task ahead is not to build something new. It is to fund and strengthen infrastructure that NSA and DoW already built, and that is already producing the workforce, research, and standards the nation depends on.

So ask the question one more time. Where and when else have you found almost 500 colleges and universities working together, with government and industry, in one mission? There is no second example. The faculty who built this did it on top of their teaching loads, the agencies stayed with it across administrations, and the employers showed up year after year. That is worth recognizing, and it is worth protecting.

See what a working community looks like

"In my 46 years of government service I never saw a more energetic, committed and creative group of professionals than I found in the CAE community. Collaboration is the community's key strength, not only resulting in amazing resources for all participants, but also providing the highest level of credibility in academia."

Lynne Clark

Introduction

Dr. Zoe Fowler

In an era of shifting enrollments, rapid technological change, new cyber threats, and intensifying competition for workforce talent, the National Centers of Academic Excellence in Cybersecurity (CAE) community demonstrates the future of American higher education. We are a community of institutions that remain competitive, resilient, and relevant by working collaboratively to share resources and good practices. Through creative innovation and pedagogical rigor, faculty across this network design and deliver learning experiences that forge their students' long-term career success. Students from CAE-designated institutions graduate with the substantive, work-relevant experiences needed to meet workforce demands and bolster national cyber security.

This handbook provides a practical compendium of case studies and actionable guidance. While achieving CAE designation is a rigorous and necessary milestone, what follows designation is far more consequential. Academic excellence must be continuously enacted, refined, and sustained. To that end, this book is designed not as a theoretical treatise, but as a navigational guide. The following chapters signpost good practices and shared resources that you can adapt and scale within your own college or university.

The case studies collected here document excellence across several foundational dimensions:

- **Industry Alignment:** How proactive advisory boards can keep academic pathways tightly coupled to regional and national employer demand.
- **Holistic Student Support:** How career and student services can cultivate and inspire future talent, dismantle practical and financial barriers that too often sideline capable students, and provide evidenced career pathways for students to follow.
- **Pipeline Development:** How community outreach, collegiate cyber clubs, offensive and defensive competitions, and K–12 engagement can expand participation and build public trust.
- **Consortium Synergy:** How regional hubs can synchronize urban and rural institutions around shared capabilities, joint grants, and collective impact.
- **Curricular Agility:** How faculty might embed emerging technologies into coursework so that graduates step into an evolving operational environment fully prepared.

Complementing these institutional case studies, later chapters detail resources built within and shared across the CAE community. These include the CLARK curriculum repository, registered apprenticeship frameworks, federal grant acquisition strategies, early-career faculty development, and the XP Cyber Range. These shared assets lower the barrier to entry for newly designated institutions and contribute to established programs, ensuring that an innovation launched on one campus can quickly benefit hundreds of others.

Complementing these institutional case studies, later chapters detail resources built within and shared across the CAE community. These include the CLARK curriculum repository, registered apprenticeship frameworks, federal grant acquisition strategies, early-career faculty development, and the XP Cyber Range. These shared assets lower the barrier to entry for newly designated institutions and contribute to established programs, ensuring that an innovation launched on one campus can quickly benefit hundreds of others.

Looking ahead, the CAE national network will continue to expand. New institutions will achieve designation and join the ecosystem, where they will find ready access to mature curricula, technical ranges, and seasoned peer mentors.

The pages that follow are candid, pragmatic, and oriented toward implementation. Use them as a toolkit: benchmark your initiatives against these case studies, draw on the signposted resources, and adapt these practices to strengthen your own institution's mission. •

An effective advisory board can:

- **Create direct, high-yield pipelines for student placement.**
- **Bring real-world industry intelligence and trend spotting.**
- **Maintain curriculum relevance.**
- **Create faculty integration opportunities.**
- **Provide a vehicle for developing community awareness.**

Advisory Boards

Introduction

Advisory boards are strategic partnerships composed of industry professionals, government representatives, and subject matter experts who collaborate with academic institutions to guide program development. These boards provide a critical bridge between academic theory and practical workforce demands. An effective board provides faculty and administrators with real-world insights into emerging technologies, shifting threat landscapes, and the specific skill sets required by local and national employers.

Advisory boards typically function through structured, periodic engagements, often convening annually or bi-annually. Members review curricula, assess proposed changes, and discuss industry trends. By providing strategic feedback on course offerings and facilitating deeper ties with the professional community, advisory boards ensure that academic programs produce graduates who are immediately employable and well-prepared for the rigors of the modern tech sector.

An effectively executed advisory board can transform students' learning journeys through increasing the relevance and timelines of curricular offerings, widening the range of internship opportunities, increasing awareness of cyber careers, and directly hiring graduating students.

CASE STUDY: Bossier Parish Community College

(Interviewee: Professor Chris Rondeau)

For Bossier Parish Community College (BPCC), the initial impetus for developing a functional advisory board was generated by the need of ensuring the college's computer science offerings aligned with the requirements of both local industry and the prospective arrival of the U.S. Cyber Command at the nearby Barksdale Air Force Base. Although engagement with the regional Cybersecurity Education Consortium (CSEC), a 12-state federal grant initiative, had helped BPCC design a core set of six foundational courses, the college wanted to elicit specific guidance from its local employment ecosystem to ensure the rest of its program was timely and relevant.

Recruiting the best people to the advisory board required a multi-pronged strategy that combined direct outreach with systematic networking. As Professor Chris Rondeau, the program head, recounts, the process began with *"literally cold calling and just going and knocking on doors."* BPCC also leveraged its existing relationship with the Cyber Innovation Center (CIC), a local research park housing numerous defense contractors and tech companies. CIC became a key facilitator, making introductions that lent credibility to the college's efforts.

Although the initial purpose of reaching out to industry and federal employers had been to recruit to the Advisory Board, the process also embedded faculty in the local professional community. Faculty began attending, and continue to attend, meetings for groups like the Armed Forces Communications and Electronics Association (AFCEA) and "Tech by 20," a regional technology meetup. These networks provide ongoing opportunities to ensure faculty remain up-to-date and aware of the evolving cyber workforce.

BPCC has developed a diverse advisory board that includes representatives from multinational corporations like General Dynamics and Microsoft alongside small, local "mom and pop" IT shops. This approach ensures a representative cross-section of the regional economy and promotes the broad range of cyber careers available to graduating students. While all voices on the board are considered equal regardless of company size, BPCC learned a crucial lesson about the need to balance individual requests against the overall group perspective early in the Advisory Board's development. A single company made a request for employees skilled in the Ruby programming language and BPCC invested resources in developing this course, before realizing there was no broad demand for this skill in the region. The Ruby course was ultimately shelved. From this, a key principle was established: any proposed curricular change must be vetted by the entire board and secure at least 50% buy-in before the college commits resources. This process ensures the program remains aligned with the collective needs of the regional workforce, not the niche interests of a single partner.

The operational framework of the advisory board is structured to be both efficient and effective. The board convenes once a year for a single, intensive 2.5- to 3-hour meeting, a cadence that respects the demanding schedules of its 15-20 industry members. To maximize productivity, proposals for program changes and accompanying rationales are circulated in advance of the annual meeting to ensure members arrive prepared for a substantive discussion.

Rondeau recommends that significant attention should be given to preparing and following up on Advisory Board meetings. Valuable ideas often need *"translating across stakeholders"* because industry requests often need to be adapted to fit effectively within the practical realities of academic accreditation standards and course contact-hour requirements.

The board's function and value extend beyond the annual meeting. Employers on the board, confident in the rigor of BPCC's CAE-designated program, frequently send job descriptions directly to the faculty and seek recommendations for qualified students. The board has also facilitated numerous internship opportunities, guest lectures, and facility tours, giving students direct exposure to the industry and reinforcing the real-world applicability of their classroom learning. This symbiotic relationship, built on a foundation of consistent communication and mutual respect, demonstrates how a well-managed advisory board can become a cornerstone of a successful cyber education ecosystem.

Key Considerations

1 / Strategic Recruitment
Utilize a multi-pronged approach that combines direct outreach with systematic networking. Leverage local tech hubs, innovation centers, and defense contractors to build credibility and secure introductions.

2 / Board Diversity
Ensure the board represents a realistic cross-section of your employment ecosystem. Balance voices from large multinational corporations with those from local, small-to-medium IT businesses.

3 / Operational Efficiency
Respect the demanding schedules of industry partners. Consolidate engagements into focused sessions (e.g., a single 2.5- to 3-hour annual meeting) and distribute all proposals and rationales well in advance to maximize discussion time.

4 / Consensus-Driven Recommendations
Avoid tailoring academic programs to the niche needs of a single employer. Establish a clear threshold (e.g., requiring at least 50% board buy-in) before committing academic resources to new programming languages or courses.

5 / Continuous Faculty Integration
Treat the board as a two-way street. Faculty should actively embed themselves in the local professional community (e.g., attending industry meetups and association events) to stay current on workforce trends outside of formal board meetings.

Summary

A well-managed advisory board creates a symbiotic educational ecosystem and a robust talent pipeline by facilitating internships, guest lectures, and direct hiring opportunities. Ultimately, it ensures that STEM and cyber programs remain rigorous, relevant, and tightly aligned with the collective, long-term needs of the regional workforce.

Some Examples of Professional Networks Include:

Cybersecurity

- Information Systems Security Association, ISSA
- Information Systems Audit and Control Association, ISACA
- Women in CyberSecurity, WiCyS
- InfraGard National Members Alliance, INMA

Education and Workforce Development

- National Initiative for Cybersecurity Education Community, NICE Community
- National CyberWatch Center, National CyberWatch
- National Cybersecurity Training and Education Center, NCyTE
- Colloquium for Information Systems Security Education, CISSE

Defense and Military

- Armed Forces Communications and Electronics Association International, AFCEA
- Air & Space Forces Association, AFA
- Association of the United States Army, AUSA
- National Defense Industrial Association, NDIA

Intelligence and National Security

- Intelligence and National Security Alliance, INSA
- Association of Old Crows, AOC
- National Defense University Foundation, NDU Foundation

"By taking the chance to be a part of the CAE community, I was immensely surprised at the warmth and 'family' feel that has led to valuable relationships that go beyond sharing resources, curricula, labs, and collaboration opportunities. The CAE is comprised of many small families that all roll up into a well-coordinated and forward-moving entity!"

Dr. Stanley J. Mierzwa, Kean University

A well-informed and proactive career and student services approach can:

- Adopt a 'whole person' model that shatters the 'hoodie hacker' stereotype and guides students, including traditional, first-generation, working, military-affiliated, and non-traditional, toward the cyber pathways that fit their strengths and circumstances.
- Address practical barriers (food security, professional attire, reliable internet, transportation, and basic navigation of higher education) so that passion and ability, not resource gaps, determine who succeeds.
- Leverage free interactive platforms (TryCyber, TryHackMe) and national pipelines (such as DoW Cyber Service Academy) while building local employer and alumni networks that produce internships, interviews, and direct hires.

Career and Student Services

Introduction

The Department Cyber Workforce Framework (DCWF) describes 77 distinct work roles spanning highly technical offensive and defensive positions through governance, risk, compliance, policy, and enabling functions. Cyber careers are not one-size-fits-all. Effective career and student services demystify this range, help students build technical portfolios and industry-recognized certifications, translate classroom experiences into résumé language, prepare for interviews and federal background processes and, critically, remove the non-academic barriers that prevent capable students from reaching those opportunities.

The most effective programs address three interconnected populations and the systems that support them:

1 / K–12 gatekeepers (counselors, parents, advisors) who shape early awareness.

2 / Current student cohorts, including traditional 18–21-year-olds and the growing numbers of first-generation, working, military-affiliated, adult, and otherwise non-traditional students.

3 / Industry, federal, and alumni networks that convert preparation into placement.

Many institutions discover that the students with the strongest passion for cyber are precisely those least equipped with the background knowledge, financial buffers, or social capital that traditional pathways assume. Housing instability, food insecurity, lack of professional clothing, unreliable internet, and unfamiliarity with how to package oneself for employers are not peripheral issues; they are career-readiness issues. Addressing them is not charity, it is workforce development.

1 / K12 Engagement

Building a state-of-the-art cyber program is only half the battle: if counselors, parents, and academic advisors do not understand the career opportunities available in the field, classrooms will remain empty. Institutions need to work

with high school careers services to actively demystify cyber careers, breaking the stereotype of the isolated, nefarious actor in a hoodie and replacing it with a diverse, accessible professional pathway that will attract a range of courses to an institution's cyber courses.

2 / Existing student cohorts

By implementing career readiness competencies (including technology, communication, and professionalism), integrating specialized career management software, and matching knowledge and skills to frameworks such as the DCWF, careers services and educators can collaborate to transition from passive degree providers to active workforce pipelines. Résumé writing and editing, tutoring on interview strategies, staging mock interviews with careers staff and/or alumni, and career mentoring also provide valuable contributions towards students' future successes.

3 / Industry and federal networks

As with the previous chapter's focus on building an effective advisory board, career services need to maintain networking engagements with local employers. Building these relationships can ensure career services are aware of upcoming job vacancies, changing cyber work roles, and have a bank of stakeholders willing to provide talks and attend careers fairs.

CASE STUDY: Moraine Valley Community College

(interviewee: Dr. Kristine Christiansen)

At Moraine Valley Community College (MVCC) in Illinois, Dr. Kristine Christensen, Director of Faculty Development and Professor of Computer Information Systems, identified a persistent challenge in cyber education: many of the people helping students make educational and career decisions did not fully understand the breadth of the cyber workforce or feel confident guiding students toward cyber careers. Through conversations with educators, counselors, and advisors, Christensen repeatedly encountered the same issue: cybersecurity was often viewed narrowly as hacking, coding, or highly technical work rather than as a field encompassing dozens of technical and nontechnical roles across nearly every industry.

As Christensen observed: *"A lot of times, counselors and advisors had no idea how broad cybersecurity really was. They pictured a nefarious actor in a hoodie, sitting in a white van outside your house trying to break into a system."* If counselors, advisors, parents, guardians, and students are unfamiliar with the range of cyber careers, students may never discover opportunities that align with their interests, strengths, academic backgrounds, or career goals.

With support from the National Science Foundation Advanced Technological Education program, Christensen and the MVCC team developed Explore Cyber, a cyber career awareness and exploration initiative designed to make cyber careers, workforce frameworks, educational pathways, and career resources easier to understand and use. Resources are available through ExploreCyber.org, with interactive career exploration tools available through the site.

The MVCC team deployed a multi-faceted approach:

1 / Making Workforce Frameworks Approachable: Explore Cyber introduces students, counselors, and advisors to the DCWF and the NICE Workforce Framework. The goal is not only to explain what the frameworks are, but to help users apply them to career exploration, skill identification, job searches, résumé writing, interview preparation, and long-term career planning.

2 / **Matching Interests to Cyber Careers:** Tools such as the DCWF Role Matcher, NICE Role Matcher, and Personality Explorer help students discover cyber roles that align with their interests and strengths. Students interested in law, business, manufacturing, communications, data, policy, engineering, or other areas can see how those interests connect to cyber work.

3 / **Connecting Cyber to Critical Infrastructure:** Explore Cyber is expanding career awareness by mapping cybersecurity roles to critical infrastructure sectors. This helps students understand that cybersecurity is needed in energy, transportation, healthcare, communications, manufacturing, financial services, water systems, and other essential industries.

4 / **Serving as a Cyber Connector:** Explore Cyber does not try to recreate every existing cybersecurity resource. Instead, the project helps counselors, advisors, students, parents, and guardians understand what trusted resources already exist, how to use them, and how they connect to education and workforce pathways. The toolkit helps students move from discovering a role to trying the skills associated with it. A student can identify a work role through the DCWF, explore the knowledge and skills connected to that role, and then use resources such as TryCyber, TryHackMe, Cisco Skills for All, picoCTF, or the National Cyber League to gain hands-on exposure.

5 / **Providing Information to Early Entry Points for Students:** For high school students, resources such as the Regions Investing in the Next Generation (RING) cybersecurity curriculum provide an accessible introduction to cyber concepts and help students build foundational knowledge before entering a college program.

6 / **Equipping Counselors, Advisors, and Families:** Explore Cyber is designed for more than students. Toolkits, workbooks, presentations, and workshops give counselors and advisors practical resources they can use in career conversations, while parents and guardians can better understand the range of opportunities available and support students in making informed decisions.

7 / **Creating Shareable Resources:** Through ExploreCyber.org, the project makes toolkits and workbooks, PowerPoint presentations, activities, career exploration tools, and supporting materials available for use by colleges, universities, schools, workforce organizations, community groups, counselors, advisors, students, and families.

8 / **Building a Community of Practice:** Explore Cyber is developing a Community of Practice where counselors, educators, advisors, and other stakeholders can share resources, strategies, lessons learned, and effective approaches to cyber career awareness and a complementary video series is also being developed.

9 / **Broadening Participation:** Explore Cyber is working with the CAE Rural Community of Practice to expand access to cyber career-awareness resources in communities that may have limited cybersecurity programs, instructors, employers, or advising resources. The goal is to help students discover cybersecurity opportunities regardless of geography or prior exposure to the field.

The larger goal of Explore Cyber is not simply to increase enrollment in cyber programs. It is to help students and the people who guide them understand what cyber work looks like, where those careers exist, why they matter, and how to prepare for them.

CASE STUDY: Montreat College

(interviewee: Thomas Hill)

Montreat College's philosophy is to educate the whole student, and this informs their proactive approach to collaborating with the career services housed at their Thrive Center. Students receive holistic guidance on all aspects of their career journey, from learning how to dress professionally and conduct themselves in work settings, to deciphering job postings and articulating their relevant experiences through résumés and interviews.

Montreat's career services support students in translating abstract classroom achievements into concrete workforce competencies. A cornerstone of this collaboration is the integration of cognitive and personality assessments. Students undergo Myers-Briggs Type Indicator (MBTI) profiling to understand their natural thinking processes. Thrive Center advisors then sit down with students to map these cognitive profiles to specific industry frameworks, including the DCWF and the NICE Framework. This approach demystifies job postings. By looking past vague, high-level job titles, students learn to analyze the specific knowledge, skills, abilities, and tasks (KSATs) outlined in postings and to explicitly relate them to what students already know, what they have already done, and where they want to develop their careers.

Montreat's Thrive Center also posts internships and job vacancies. It maintains regular contact with local businesses, and facilitates institutional careers fairs.

In his role as a professor at Montreat, Thomas Hill seeks to continuously map the relevance of his classroom activities to work roles and the KSATs that define them. In an interview for this chapter, he explained how this explicit mapping can create life-changing career milestones for students. For example, one of Hill's students secured an interview with the North Carolina Department of Information Technology (GDIT). During the interview, the student presented the risk-assessment tool he had developed in Hill's class and explained to the panel how the tool could proactively protect their organization. The state IT panel was so impressed by the practical maturity of the work that they explicitly told the student his classroom creation was technically superior and more functionally effective than the commercial, professional-grade risk management platforms they were currently using.

CASE STUDY: Florida A&M University

(interviewee: Idongesit Mkpong-Ruffin)

All institutions have vulnerable students who represent a vital, yet often overlooked, part of the future cyber workforce. These students possess significant potential, but many institutions lack the knowledge and resources needed to provide the targeted support required for them to thrive academically and successfully transition into the cyber workforce. To address this gap, Dr. Idongesit Mkpong-Ruffin is co-chairing a CAE Community of Practice dedicated to equipping institutions with practical strategies and insights. This group offers actionable guidance on how to better support vulnerable students, helping them overcome barriers, complete their degrees, and enter the cyber workforce.

Florida A&M University (FAMU) serves a student population that includes traditional-age learners alongside a high proportion of first-generation college students, working adults, and military-affiliated learners. Mkpong-Ruffin knows the genuine passion many of these students have for cyber careers and also recognizes that some might lack the family history, financial scaffolding, or institutional navigation knowledge that traditional pathways presuppose. Across all institutions of higher education there are students who are ambitious to achieve cyber careers but who are also contending with food insecurity, housing instability, lack of professional attire, and unfamiliarity around how to present themselves to employers. FAMU has responded with an infrastructure of de-stigmatized support and structured professional development including:

- **Practical resource infrastructure.** An interview clothes closet and a campus "Mall Day" partnership with retailers such as JC Penney enables students to obtain a full professional suite for a nominal $10 contribution, with faculty and staff underwriting the difference. Departmental snack bars and food resources, stocked through faculty and alumni donations and placed in open, non-stigmatizing locations, ensure students can eat. Importantly, faculty and staff normalize use so that taking a snack or borrowing attire became ordinary rather than exceptional.

- **Credit-bearing professional development.** A one-credit Professional Development course, offered in the freshman year and again in the junior year, teaches students how to package themselves, how to interpret internship and job opportunities, and how to build mentoring relationships.

Because the college's corporate liaison is herself an alum of the department, the mentoring network is personal and sustained. Graduates who have been supported become the next generation of supporters and recruiters.

These local practices have informed a broader CAE-Community effort. Recognizing that many institutions maintain siloed but effective resources (for example, food pantries, professional closets, certification-exam funding, résumé templates, mock-interview banks, portfolio frameworks, micro-credential pathways, and summer checklists), Mkpong-Ruffin and colleagues in the CAE-CD Community of Practice established the Working, Armed Forces, Non-traditional, and Transitioning Students (WANTS) group. The group meet regularly and have created a shared resource page so that proven approaches can travel across the community rather than remaining locked inside individual campuses.

The FAMU experience demonstrates that careers and student services succeed when they treat basic needs, professional self-presentation, and technical preparation as inseparable components of the same pipeline.

Key Considerations

Map skills, portfolios, and lived experience to the DCWF and the NICE Framework.

Explicit mapping helps every student translate what they know and have done into language employers and federal hiring systems recognize. This also supports students in discovering their passions within the field of cyber and to actively pursue specific careers.

Implement gatekeeper "cascade" training for K–12 counselors and advisors.

Short, focused professional-development sessions for the adults who influence student choices can act as a force multiplier, rather than focusing on one-by-one student recruitment.

Integrate psychometric and strengths-based assessments.

Tools that connect natural cognitive preferences and personality traits to specific cyber specializations reduce intimidation and broaden the pool of students who see themselves in the field.

Treat practical barriers as career-readiness issues.

Food security, professional clothing, reliable connectivity, and basic navigation of higher education are not peripheral; they determine who can complete certifications, attend interviews, and accept internships. Design an infrastructure of support that is visible, de-stigmatized, and normalized. Our current students are the cyber talent of tomorrow.

Embed professional development inside the curriculum.

Design credit-bearing courses that provide students with practical steps in résumé building, interview behavior, job-hunting and self-packaging. Through building these into the curriculum, they become accessible to all students rather than being delivered through optional workshops that busy or working students might not be able to attend.

Build and sustain alumni virtuous circles.

When current students experience tangible investment, many return as mentors, employers, and material supporters. Structured corporate-liaison roles and recurring alumni events convert that goodwill into ongoing pipeline strength.

Empower employer partnerships through hands-on and gamified experiences.

Capture-the-flag events, hiring simulations, and challenge-based interviews give both students and employers concrete evidence of capability beyond transcripts.

Summary

Effective career and student services move beyond résumé workshops and job boards. They combine early awareness work with K–12 gatekeepers, rigorous mapping of student strengths to national workforce frameworks, credit-bearing professional development, and practical supports that remove the non-academic barriers many students face. When institutions invest in the whole student, the result is not only higher retention and placement but a more resilient national cyber workforce.

Communities of Practice Career Resources

CAE Virtual Careers Fair

The National Cybersecurity Virtual Career Fair (VCF) platform is an online space where job seekers and employers connect through live chats, video calls, and digital booths. It replicates the experience of an in-person career fair, but from anywhere with an internet connection.

This event is open to students from any of the more than 500 institutions designated as Centers of Academic Excellence in Cyber, as well as institutions in the Candidate's Program (pending approval).

Explore Cyber

Explore federal cyber job opportunities near CAE institutions

Search for a CAE institution and view federal job opportunity data in the surrounding metro areas.

Working (Non-Traditional) and Military Students

This CAE Community of Practice Cyber Defense (CoP-CD) initiative promotes resources and activities for Working, Armed forces, Non-traditional, and Transitioning Students (WANTS) at CAE institutions. This new CoP-CD initiative will include a yearly workshop and a list of resources to be shared on the CoP-CD page on embracing and supporting working (non-traditional) students (full-time and part-time), military students, women, single parents, first-generation students, veterans, and students with learning and other special needs who are enrolled in cybersecurity programs. The goal is to develop a working list of resources and tools that faculty can use to help coach and guide students who need a little extra help.

Initiative Co-Chairs:

- Florida A&M University
- Terra State Community College

National Cybersecurity PhD Student Club

This CAE Community of Practice Cyber Research (CoP-R) initiative is designed to grow a network of current and previous PhD students and provide valuable resources and opportunities.

Initiative Co-Chair:

- University of Alabama in Huntsville

A well-informed and proactive career and student services approach can:

- Strengthen regional cybersecurity resilience
- Increase visibility of the institution within the community
- Promote experiential opportunities for students
- Drive increased understanding of the relevance and applications of learning.

Community Outreach

Introduction

Community engagement is a collaborative approach to outreach that brings faculty and student knowledge and expertise beyond campus boundaries and into the communities they serve. Community engagement makes practical, accessible training and services available to a broader audience, thereby helping individuals and organizations build the skills needed to navigate cyberspace and increasing the security of regional communities.

Effective community engagement often focuses on groups that may be more vulnerable to cyber threats or have limited access to technical education. These audiences can include senior citizens, high school students, and veterans. Community engagement can also provide free IT services to local civic organizations such as libraries, fire departments, and community centers. By meeting people where they are and addressing real-world challenges, cyber outreach programs can help strengthen digital awareness, resilience, and confidence across the community.

For academic institutions, community engagement demonstrates a commitment to civic service, advances institutional mission objectives, and creates meaningful connections with future students, partners, and supporters. These initiatives also help establish the university or college as a visible and trusted presence within the local community.

The benefits extend to students as well. Engagement activities enhance their future employability through providing them with opportunities to serve as instructors, mentors, and ambassadors where they learn to translate complex technical concepts into language that diverse audiences can understand and develop valuable communication and leadership skills. Students also see firsthand how their knowledge can create a positive impact in the lives of others.

At its best, cyber community engagement transforms cyber education from a classroom experience into a community resource, creating lasting value for institutions, students, and the people they serve.

CASE STUDY: Florida State University

(interviewee: Dr. Xiuwen Liu)

For many newly designated Centers of Academic Excellence (CAE) institutions, community outreach can seem like an important but difficult next step: between developing academic programs, supporting research, and preparing students for cyber careers, extending cyber education beyond the campus may feel like a secondary priority. Florida State University (FSU) demonstrates that it does not have to be.

FSU has built a student-driven outreach model that serves two important audiences: senior citizens navigating an increasingly digital world and high school students exploring opportunities in cyber (discussed in K12 chapter of this handbook). Led by Professor Xiuwen Liu, the program shows how community engagement can strengthen both the local community and the institution itself.

Like many institutions, FSU initially encountered challenges when trying to establish community partnerships. Early outreach to local senior centers often went unanswered: *"Initially, we had trouble with the Senior Center because they were very busy,"* Liu recalled. *"So they ignored us. It takes some time to establish the relationship."* Rather than giving up, FSU students visited senior centers in person to introduce themselves and to learn more about the organizations' needs and schedules. That persistence paid off, ultimately leading to a partnership with the Tallahassee Senior Center and its branch locations. Together, they have developed a series of workshops delivered through the Leon County Main Library and nearby senior centers that focus on practical skills that participants can apply immediately: for example, recognizing scams, identifying fraudulent emails, and practicing safe online behavior. The most hands-on components involve mobile security workshops where seniors can bring their own smartphones and work directly with student instructors to review privacy settings, manage permissions, and improve device security. As interest in AI has grown, students have also demonstrated how convincing fake videos and audio recordings can be and have helped seniors better understand emerging risks. *"We demonstrate to the seniors how easy it is to make videos that look very authentic,"* Liu explained.

During the academic year, student instructors volunteer their time and receive official recognition for their service through documented community engagement hours on their academic transcripts. *"There is a way to report this so that actually there is going to be showing on their official record they have done this service,"* Liu noted. During the summer, research grants help support student instructors through paid internship opportunities.

The model creates benefits for everyone involved. By teaching cybersecurity concepts to seniors and high school students, student instructors deepen their own technical understanding while developing leadership and communication skills. *"One of the best ways to learn any skill is to teach it to others, ideally in a live setting where the audience can ask questions and interact with the presenter,"* says Matthew Christoffel, founder of the Cybersecurity Community Outreach Organization at FSU.

Perhaps more important, community engagement helps students see the broader impact of their work. *"For the students," Liu reflected, "serving the community really makes them feel like their knowledge and skills are being appreciated and valued."* For CAE institutions looking to expand their impact, FSU's experience offers a valuable lesson: meaningful community engagement begins with relationships, student leadership, and a commitment to serving local needs. The result is stronger communities, stronger students, and a stronger cybersecurity workforce pipeline.

CASE STUDY: Metropolitan State University

(interviewee: Dr. Faisal Kaleem)

The Cyber Clinic at Metropolitan State University is an innovative public-service initiative, initially funded by the NSA and designed to protect under-resources local organizations from cyber attacks while providing upper classman students with critical real-world industry experiences. The clinic provides free cybersecurity risk assessments, defensive social engineering, and provides student experiential learning.

When Dr. Kaleem joined Metropolitan State University in 2014 there was a single computer security course in its catalog. Kaleem envisioned a future

where Metro State would not only educate the next generation of cyber professionals, but also serve as a vital community partner, protecting the digital infrastructure of the Minnesota community and beyond.

Initially, he set about igniting interest across the student body by establishing a student cybersecurity club, a place for aspiring cyber-warriors to gather, learn, and hone their skills. In 2015, Metro State's first-ever Collegiate Cyber Defense Competition team secured a second-place finish in the state, proving Metro State's cyber program was not to be underestimated, but had opportunity to grow and develop.

With this newfound momentum, the program grew at an astonishing pace. A minor in cybersecurity was introduced, followed by a Bachelor of Science in 2018, a Master of Science in Cyber Operations in 2019, and an accelerated combined BS/MS program in 2020. The curriculum was designed to be rigorous, practical, and aligned with the workforce needs of industry.

But a world-class cyber program needed more than just great courses; it needed a place for students to put their knowledge to the test. Dr. Kaleem's vision included a virtual battleground where students could face real-world threats in a safe and controlled environment. Driven by a philosophy of "relationships as infrastructure", Kaleem forged and established partnerships with Elbit Systems of America, securing a large investment of $1.5 million to develop a cyber range at no cost to the university. But the range came with its own set of challenges: the restrictive licensing and limited scenarios hampered the program's scalability. This led Kaleem to secure funding through state appropriations and federal grants, allowing them to partner with a new provider, Cloud Range, and build Minnesota's largest NetLab environment, a foundational private-cloud lab automation platform.

But even the most realistic simulations can't replicate the pressure and complexity of a real-world cyberattack. To bridge this gap, Kaleem launched the Metro State Cyber Clinic, a student-run consultancy providing free cybersecurity services to under-resourced organizations. The clinic was a resounding success of which Kaleem is very proud! With the guidance of Minnesota IT Services, the state's executive branch IT agency, students provide vulnerability assessments, security posture evaluations, and policy development to over 500 public-sector and non-profit clients. They aren't just learning about cyber, they are actually doing it, making a real difference in their community and community partners.

The clinic has evolved into a two-semester internship program, a capstone experience for the university's top cyber students. In their first semester, they learn the ropes, shadow senior peers and undergo rigorous training. In their second semester, they take the lead, delivering reports and recommendations directly to clients. The clinic is making steady and continual strides.

Metro State demonstrates how a university with a cyber program can also be a community partner, a regional hub of cybersecurity expertise, and a testament to the power of a clear vision, a dedicated team, and the unwavering belief that relationships are the most valuable infrastructure of all.

Key Considerations

1 / Build relationships before programs

Community engagement starts with trust. As FSU discovered through its work with the Tallahassee Senior Center, even the most well-intentioned outreach efforts can stall if community partners are already stretched thin or unfamiliar with the institution. Rather than viewing unanswered emails as a setback, institutions should be prepared to invest time in personal outreach, listening, and relationship building. Strong partnerships are often the foundation upon which sustainable and impactful programs are built.

2 / Design around community needs

The most effective outreach initiatives focus on the needs of the audience rather than the expertise of the institution. Whether helping older adults recognize scams, understand deepfakes, and secure their mobile devices, or introducing high school students to cyber career pathways, FSU tailors its programming to the interests and challenges of each group. Meeting learners where they are creates a more meaningful experience, increases participation, and demonstrates the practical value of cyber education in everyday life.

3 / Make learning active and accessible

Engagement increases when participants can immediately apply what they learn. Removing barriers through accessible locations, practical content, and supportive learning environments helps participants gain confidence while making cyber feel less intimidating and more relevant.

4 / Empower students and create sustainability

Student involvement is often the key ingredient that transforms outreach from a short-term activity into a lasting program. FSU leverages scholarship-supported students as instructors and mentors, providing opportunities for service recognition, internship experiences, and professional development. In the process, students strengthen their own technical knowledge, develop valuable communication and leadership skills, and gain a deeper appreciation for the impact their expertise can have on others. When outreach is integrated into student success and institutional priorities, it becomes easier to sustain over time.

Summary

Community engagement is not separate from a CAE institution's mission. It is a natural extension of it. By sharing knowledge, building relationships, and creating opportunities for students to serve, institutions can transform cyber education into a community resource that benefits everyone involved.

"The CAE designation may start with an impressive certificate bearing the logos of our federal partners on the wall, but its real value lives far beyond it. What keeps me engaged is the community and the camaraderie, the way faculty openly exchange what works, institutions help each other instead of guarding ideas, all with the shared goal of creating opportunities for students and strengthening the much-needed cybersecurity workforce in ways no single institution could do on its own."

Dr. Faisal Kaleem, Metro State University

Cyber competitions can:

- Bridge theory and live-fire reality
- Forge business acumen, professional skills, and resilience
- Provide an inclusive on-ramp for all skill levels
- Increase students' hireability through evidencing abilities and experiences required by employers

Competitions

Introduction

A cyber competition is a real-time experiential learning event designed to evaluate and sharpen the technical, operational, and cognitive skills of participants under high stakes conditions. Reflecting the vast diversity of real-world cyber roles, these competitions range from solo, highly structured puzzle-solving tournaments (such as Capture the Flag events) to dynamic, team-based simulation environments that mirror actual business or critical infrastructure operations. Depending on their design, some challenges are purely technical, while others introduce sudden, chaotic operational tasks ("injects") or require competitors to defend against active, live adversaries (Red Teams). Competitions demand an elite combination of rapid critical thinking, technical prowess, crisis management, and strategic business communication. This chapter provides an overview of some of the key competitions across the US as well as a case study exploring how competitions can be used as a valuable learning resource within the classroom.

CASE STUDY: California State University Chico

(Interviewee: Professor David Zeichick)

Professor David Zeichick introduced his students to the National Cyber League (NCL) competition ten years ago while he was teaching an "Introduction to Cybersecurity" course. His original intention was to use the NCL practice grounds and competition challenges as interactive hands-on learning experiences to support his curriculum. Since then, CSU Chico's involvement in the NCL has rapidly grown and the institution has now fielded several winning teams.

The mission of the NCL competition is to prepare the next generation of cyber professionals through providing high school and college students and their coaches with an online, safe platform of real-world challenges. The competition is structured around nine skill categories informed by cyber work role tasks, such as identifying hackers from forensic data, pen-testing, auditing vulnerable websites, and recovering from ransomware attacks.

The challenges address a range of abilities from introductory level problems through to exercises that require a higher level of skill and expertise.

Not all competitions are attractive to every student and this can limit participation, but Zeichick was determined that all of his students should gain from the valuable learning opportunities the NCL provides. Therefore , he experimented with different ways to link student grades to participation in competition activities and subsequently settled upon a formula where every student in his "Introduction to Cyber" class is required to participate in the practice competition. For this practice competition, the students work in small groups to solve challenges and then teach their solutions back to the whole class. Two weeks later, all students are required to participate in the individual competition, a 3-day event that equates to three labs in Zeichick's grading structure. Students can then elect to participate in the team competition, and extra credit is provided to those students. In terms of learning, the peer-to-peer instruction built into Zeichick's learning design and subsequently emulated in cyber club activities has proved particularly effective.

Although participation in the NCL began as a means of complementing a classroom course, CSU Chico's engagement in the competition has rapidly expanded. Students have introduced NCL challenges into their cyber club meetings and the cyber club now fields additional teams beyond the students in Zeichick's class. The synergy between the foundational curriculum and the student-led club has created a sustainable recruitment cycle: the increased successes of the CSU Chico team has led to increased interest from high performing students and, in turn, this has further strengthened the competitiveness of the team.

Zeichick observes that building successful competition teams has benefits for students, for faculty and for the institution as a whole. In addition to benefitting students' learning, students who participate in competitions also increase their hireability through developing material they are able to include on their résumé and gaining experience of real-world scenarios to discuss during interviews. Graduating students continue to communicate with the institution as alumni; for example, providing talks about cyber careers and their own workplaces to the cyber club, offering expert knowledge, and contributing funding to the cyber club that helps support the competition team. For faculty, the NCL competition provides access to valuable hands-on learning labs that can be used within the classroom and as co-curricular activities. The institution also benefits from the media coverage, and stories about winning teams can be a valuable marketing tool for future potential students.

Zeichick points out that while academic interest drives the technical focus in competitions, basic hospitality also goes a long way in sustaining attendance: *"they need pizza!"* he says, *"that's always helpful and seems to get students there!"*

An Overview of Key US Cyber Competitions

There are a vast number of competitions across the US, and a comprehensive list is available through the CAE Cyber competition atlas posted on the CAE Community website (https://cyber-atlas.caecommunity.org/). Monthly meetings hosted by the CAE-CD 'Meet Your Competition' special interest group showcase different competitions and present conversations with competition designers and participants.

The remainder of the chapter provides a brief overview of examples of different kinds of competitions, each of which creates valuable learning experiences for students and contributes to their future employability.

The Global Collegiate Pen Testing Competition (CPCT)

COLLEGIATE PENETRATION TESTING COMPETITION

"It's not just about the hack, it's about the business."

The CPTC is an elite, international ethical hacking competition run by the Rochester Institute of Technology (RIT) that tests both technical prowess and business acumen.

The competition is an in-person event based on scenarios occurring in a real life infrastructure. Instead of traditional "capture the flag" or defensive exercises, students act as an external consulting firm hired to perform a real-world penetration testing engagement. Each year, organizers build an expansive, custom model of a different critical infrastructure company or industry. It utilizes state-of-the-art infrastructure, such as RIT's Cyber Range (supported by IBM), which can replicate real-world disaster scenarios and stressors to provide a physically and mentally realistic testing environment.

Teams are tasked with actively hunting and exploiting vulnerable spots within a complex computer network, and then, critically, presenting a professional report detailing their findings and making actionable plans to secure the network. Recent winners from UC Irvine stood out because of their ability to translate complex, critical software exploits into a polished business presentation that a corporate C-suite could understand and act upon. Rather than just handing over a list of system bugs, they provided the client with structured, categorized risk frameworks and direct prioritization roadmaps, telling the business leaders exactly what to patch first, why it mattered to their bottom line, and how to protect their assets moving forward. This provides an opportunity to emulate a key part of working in cybersecurity: providing informative briefs to the C-Suite. A significant weight of the final score is given to this report.

The CPTC serves as a direct pipeline for workforce development. Because it demands that students not only hack systems but also communicate technical risks to business leaders (just like professional penetration testers), it mirrors exactly how they will operate in the private or public sector. This hands-on experience bridges the gap between classroom theory and the real-world demands of offensive security roles.

Collegiate Cyber Defense Competition (CCDC)

"Keeping business services on-line while fending off adversaries"

The National Collegiate Cyber Defense Competition (NCCDC) is the largest and "blue-team" (defensive) cybersecurity competition for college students in the United States. Unlike traditional offensive security hackathons or Capture the Flag (CTF) events, CCDC focuses entirely on the operational defense, administration, and survival of an existing, compromised corporate enterprise network.

Blue Teams are graded in real-time during a multi-day live-fire event. There are three distinct areas of scoring:

- **System Hardening & Threat Mitigation (The Red Team Battle):** Teams inherit a pre-built commercial network (containing Windows, Linux, active directory services, mail, and web databases) littered with hidden backdoors and severe misconfigurations. They must immediately audit, patch, and defend their infrastructure while the Red Team attempts to steal their data and lock them out of their own systems

- **Service Availability (The Scoring Pings):** The company's core business services (e.g., e-commerce portals, corporate email, websites) must remain online. An automated grading system pings these services every few minutes; if a service crashes or is successfully taken down by the Red Team, the Blue Team rapidly loses points

- **Business Injections (Administrative Tasks):** The "C-suite" (the competition organizers) regularly drops surprise executive orders, known as injects. These can include tasks like installing a new software package, generating an incident response report, or drafting a policy memo. Teams must complete these business tasks on tight deadlines while actively defending their infrastructure

CCDC maps directly to real-world employment demands, forcing students to realize that security does not exist in a vacuum and that a business needs to keep its servers running, even under active cyberattack.

The high-pressure environment combined with the need for effective teamwork and rapid incident triaging makes CCDC a premier scouting ground for recruiting elite Tier 1/Tier 2 security analysts, threat hunters, and system administrators straight into national security and enterprise defense roles.

US Cyber Games: The Cyber Olympics

"Scouting, coaching, and training the nation's elite cyber athletes."

The US Cyber Games act as an Olympic-style training pipeline for the nation's elite cyber athletes. Depending upon the tier they enter, students and young professionals aged between 18 and 25 participate in a series of grueling cyber challenges.

The program has been designed to treat cyber as a competitive sport and features highly interactive, gamified live-play arenas. US Cyber Games relies on a rigorous coaching model with world-class mentors who run tactical practices , evaluate playbooks, and foster intense teamwork and communication under simulated, high-stress international attack scenarios.

Competitors receive certified digital badges and scouting reports that validate their competencies in incident response and threat mitigation. Government agencies, defense contractors, and private-sector tech giants often identify and target talent through observing participants in action.

NCAE Cyber Games

"Demystifying competitions and inspiring new competitors"

While CCDC, CPTC, and US Cyber Games are examples of competitions that focus on elite athletes, the NCAE Cyber Games is specifically designed for students who are typically newer to cyber. The competition provides a developmental sandbox where students can practice red-vs-blue infrastructure mechanics as well as cryptography, reverse engineering, web security, and network analysis challenges. The infrastructure is built with incremental growth in mind, scaling up in difficulty so that students can progressively test their defensive and analytical skills.

In many ways, the NCAE Cyber Games serve as an on-ramp for the cyber talent pipeline. By introducing students to both live red-vs-blue scenarios and CTF challenges early in their academic careers, it bridges the gap between foundational knowledge and higher-lever cyber competitions such as CCDC, NCL, or CPTC. It is designed to help students identify their strengths, whether in defense, operations or analysis, preparing them to enter the cyber workforce as highly motivated, capable and battle-tested graduates. Through participating, students not only learn new elements of cyber, but are also introduced to the world of cyber competitions and build their self-confidence around operating in competitive and contested environments.

Department of War Cyber Workforce Competition

The Department of War (DoW) is rapidly evolving its cyber talent pipeline by transitioning the Cyber Workforce Competition (CWC) into a highly competitive, tiered national framework. Building on the momentum of the inaugural CWC won by the University of North Georgia, this forward-looking strategy establishes dedicated regional feeder events as the exclusive pathways to qualify for the CWC National Championship. This expansion kicks off with the newly planned CWC West competition, taking place directly at the prestigious WEST Conference from February 16-18, 2027, in San Diego, CA, a premier defense event co-sponsored by AFCEA and the U.S. Naval Institute. CWC West will provide elite teams from designated Centers of Academic Excellence (CAEs) across the United States a high-visibility opportunity to showcase their tactical capabilities on a national stage. Rather than hosting a traditional Jeopardy-style Capture the Flag (CTF) event, this competition series utilizes active, multi-domain cyber-physical ranges that simulate real tactical weapon systems to focus on kinetic-cyber mission convergence, yielding directly applicable combat skills. Furthermore, the competition directly maps to critical Department Cyber Workforce Framework (DCWF) roles, ensuring participants develop highly specialized, mission-essential capabilities.

In tandem with the West Coast expansion, the annual NSA National Cyber Exercise (NCX) is being integrated into this system as the premier regional feeder event for teams representing the U.S. Service Academies and Senior Military Colleges. This dual-track regional qualifying structure establishes a highly selective and rigorous path to the finals. The top four teams from CWC West and the top four teams from the NSA NCX will earn coveted invitations to advance to the CWC National Championship. By implementing this tiered competitive model that blends hands-on tactical weapon simulations with strict alignment to DCWF work role specializations, the DoW is systematically scaling its ability to discover, vet, and develop the next generation of military cyber leaders, ensuring they are prepared to defend critical networks and achieve multi-domain mission readiness.

Key Considerations

The growing ecosystem of cyber competitions represents more than an extracurricular academic exercise: they are a critical infrastructure for workforce development.

1 / Bridging the Gap Between Theory and Reality: Competitions provide a valuable link between classroom theory and real-world application. Whether a student is operating in a developmental sandbox like the NCAE Cyber Games or defending a live network under fire in CCDC, these experiential learning environments force students to apply abstract concepts to chaotic, unpredictable scenarios. This builds resilience, forges learning, and builds their work readiness.

2 / Developing "Professional Skills" in the Crucible of Competition: Technical prowess alone is not sufficient for the modern cyber workforce. Competitions simulate the business pressures of the workplace, teaching students vital "professional skills" such as crisis management, teamwork, rapid triage, and the ability to translate complex technical vulnerabilities into actionable executive-level (C-suite) briefings.

3 / A Diverse Ecosystem for a Diverse Workforce: The cyber industry requires a vast array of specialized roles, from offensive threat hunters and defensive SOC analysts to policy writers and social engineering experts. The wide variety of competitions mirrors this diversity, ensuring there is a training ground for every type of practitioner and every skill level.

4 / A Win-Win for the Entire Cyber Ecosystem: A robust competition program benefits all stakeholders. Students gain verified competencies and highly employable résumés; faculty gain dynamic, peer-led lab environments; institutions benefit from recruitment and engaged alumni; and employers gain access to a battle-tested, highly motivated talent pipeline.

Summary

Cyber competitions can transform students from passive learners into active practitioners. Participation is as valuable as winning when students have an opportunity to build their competency, evidence their ability, and forge the resilience necessary for a high-stress, competitive workplace.

Cyber competitions can:

- Increase students' passion and curiosity around cyber.
- Build opportunities for students to collaborate on co-curricular and extra-curricular challenges.
- Provide hands-on learning experiences.
- Evidence students' leadership, critical thinking, and collaboration skills.

Cyber Clubs

Introduction

At its core, a cyber club is a student-led, co-curricular organization at a university, college, or high school dedicated to exploring computer security, network defense, and information technology. Unlike a traditional academic class, a cyber club is an active, collaborative, and hands-on community where students learn by doing, teaching one another, and solving real-world challenges.

An effective cyber club becomes a social and academic home for students, providing opportunities to network with and to learn from other students. For an institution, it can generate a motivated and engaged alumni body who continue to have a strong affinity with the club and the institution. For students, the cyber club can provide a safe place to take risks, to engage in hands-on learning and discovery, to build resilience, and to develop hands-on capabilities that will enhance their employability. For the faculty who were interviewed for this chapter, engagement with the cyber club provides invaluable opportunities to build lasting relationships with students.

CASE STUDY: College of Coastal Georgia

(Interviewee: Dr. Nelbert "Doc" StClair)

The College of Coastal Georgia is a small state college with a diverse student body. The cyber defense program is a concentration spread across five different bachelor's degrees. The College of Coastal Georgia's cyber club provides an essential hub for unifying students from these varied academic backgrounds.

In the absence of an existing program, Dr. Nelbert "Doc" StClair set about building a club from scratch, borrowing a governance structure from another area of the institution. The philosophy was clear from day one: the club had to be for the students, by the students. As the club's advisor, StClair's role is not to lead the students, but to empower them: *"The club is student-led and student-driven. I don't teach during club events: I'm there as the 'dad, as the supply person, as the Uber driver."*

The club's activities emphasize real-world application, with students gaining hands-on experience through competitions such as the National Cyber League (NCL). These competitions serve as more than just opportunities to win -- they drive practical learning, strengthen teamwork, and foster professional growth. In the weeks leading up to each event, the faculty advisor provides guidance and resources that help students explore relevant concepts and skills, encouraging independent learning rather than teaching directly to the competition.

The club provides a real world simulation, hands-on environment where failure is not just accepted but seen as a crucial part of the learning process: *"I prefer my students make their mistakes in college rather than in the real world,"* explained StClair, and then demonstrated this principle through the example of a student who accidentally locked her entire team and the competition's red team out of their virtual environment. Though the mistake cost the club's competition team their ranking, the experience later became a discussion focus point of this student's interview and led to her landing a position with Space Force.

In summary, StClair reflected that a student-led cyber club provides a safe arena where students can develop critical thinking, resilience, and the invaluable skill of leading peers. By fostering student autonomy and building lasting relationships that extend far beyond graduation, the club transforms students into confident, job-ready professionals and builds a body of alumni who continue to volunteer and participate in club activities, thereby continuing to build the reach and relevance of the club's activities.

CASE STUDY: Cal Poly Pomona

(Interviewee: Dr. Dan Manson)

At Cal Poly Pomona, the classroom is only part of a student's journey into the world of cyber: the student-run cyber clubs provide a space where students find a sense of belonging and community that traditional academic settings often lack. These clubs become the place where students with a shared passion foster an environment where they can learn and grow together outside the curriculum.

Dr. Dan Manson celebrates the fact that club activities can be as diverse as the field of cyber. At Cal Poly Pomona, the clubs are entirely student-run. Students organize everything from their own multi-category information technology competitions to six-week-long summer "boot camps" designed to prepare for major national contests; they host tech symposiums where students present alongside industry professionals and alumni, and they create their own competitive events like "King of the Hill." These activities are not just for practice; they are real-world projects that require students to manage logistics, raise funds, and collaborate with professional organizations. As one student shared, the experience can be transformative: *"I didn't know I wanted to pursue cybersecurity till my second year of college... As I became involved [in the club], my passion for it only grew more and I knew I wanted to pursue this as my career."*

Effective cyber clubs have extensive benefits for students. Beyond the technical skills gained, these clubs become incubators for leadership and professional development. Manson advises his students to not only attend cyber club events, but to also become active participants. He tells his students that when being interviewed for a job, the most impressive answer they can give is: *"I was active in a club. I was an officer in a club. I helped lead and develop the activities that the club had."* This hands-on experience in leading projects and motivating peers is what truly sets them apart: students don't just learn about cyber; they live it, building confidence and crucial networking skills that directly translate to enhanced employability and career success.

The cyber clubs also have considerable benefits for the host institution. They build a powerful and engaged alumni network, and Manson observes that many graduates proudly identify with their club long after they've left campus. This network not only supports current students but also enhances the school's reputation, creating a virtuous cycle of success and visibility that attracts new talent and industry partners.

CASE STUDY: University of Eastern Washington

(Interviewee: Dr. Stu Steiner)

Eastern Washington University is split across two locations. Students begin their first year of cyber studies on a main campus in Cheney, Washington, and spend their junior and senior years 20 miles away in Spokane. The student-run cyber club has built an essential bridge that unifies these two communities and streamlines the students' experiences of studying cyber. The primary goal for the institution is to keep students engaged in their field from the moment they start their academic journey. Activities are driven by student interest, often determined through regular polls sent out by the club's student officers, and cyber clubs alternate between the two campuses. This means the club ensures that all students have a consistent, welcoming hub to connect and immerse themselves in cyber, regardless of where their classes are held.

For the students, the benefits of joining a cyber club extend far beyond a traditional classroom environment. A session might kick off with a member delivering a short 15-to-20-minute lecture on a topic like Wi-Fi hacking, followed by a live demonstration. The room then transitions into a collaborative lab where students pair up to practice the techniques they just learned. The club operates on a powerful model of near-peer mentoring and upperclassmen provide direct guidance and support. This highly interactive environment fosters a deep sense of accomplishment and builds technical confidence. Dr. Stu Steiner highlights the impact of this approach, noting that when students leave a meeting, *"they walk away feeling they've learned something … that they were engaging in active learning lessons."* The cyber club also serves as a vital incubator for leadership, allowing students to take the reins, pitch presentation topics, and drive their own educational journey.

The secret to the club's vibrant energy lies in this student-led autonomy rather than strict faculty control. As Steiner observes, *"Just let the student leaders do what they need to do and just be there to support them because if you try and control them, your cyber club's going to wither and die very, very quickly."*

Key Considerations

1 / Establish the Club as a Community Hub

A successful cyber club is not just an academic extension; it is the social glue of your program.

- **Bridge Divides**
  Whether your students are split across multiple physical campuses or come from entirely different degree paths (for example, business, computer science, and engineering), use the club as the central unifying identity.

- **Engage from "Day One"**
  Do not wait until students are in upper-level courses to invite them. Engage freshmen immediately to build early passion. This can dramatically improve retention and cohort cohesion. Provide peer mentoring opportunities for first year students in the club.

- **Cultivate Belonging**
  Traditional academic settings can feel isolating. The club can provide a space where students find their "tribe" and build a professional network that lasts long into their alumni years.

- **Engage with the Professional Community**
  Encourage students to join student chapters of professional associations such as ISACA (Information Systems and Audit Control Association). Encourage professional association sponsorship and engagement in club activities.

2 / Enable Student-Led Autonomy

The most consistent piece of advice across all successful programs is that the club must be run by the students, for the students.

- **Redefine the Faculty Role**
  Faculty should act as the "backstop," the "supplies person," or the "Uber driver." As one advisor noted, if faculty try to control the meetings or teach it like a class, the club will "wither and die."

- **Crowdsource the Curriculum**
  Allow the student executive board (President, VP, Treasurer) to poll the membership weekly or monthly. Let the students decide what topics they want to explore based on their current interests.

- **Identify the Employability Potential in Student Leadership**
  Emphasize to students that being a club officer isn't just an extracurricular activity. Managing logistics, raising funds, and organizing boot camps give students tangible leadership experience to discuss in job interviews.

- **Develop Annual Signature Club Activities**
  Annual club-led cyber competitions and symposiums enhance reputation and enable ongoing club success and leadership opportunities.

3 / Foster Active Learning and "Near-Peer" Mentoring

Avoid treating club meetings like solitary homework sessions or passive lectures.

- **The "Lecture-Demo-Lab" Format**
  Support students in structuring club activities around micro-learning. For example, a student might present a concept followed by a live demonstration, and participants might then break into small groups to practice the skill immediately.

- **Utilize Upperclassmen Mentors**
  Have juniors and seniors circulate the room to help freshmen and sophomores during hands-on exercises. This reinforces all students' knowledge while making the material less intimidating for beginners.

- **Avoid Solitary Screen Time**
  While platforms like TryHackMe are great for individual practice, club time should be highly interactive. Focus on team-based table-top exercises and collaborative hacking rather than having everyone stare silently at their own screens.

- **Encourage high school cyber student participation**
  Encourage local high school CyberPatriot students to be part of club mentoring and support. Use the club as a recruiting tool to attract top high school cyber students into your cyber program.

4 / Cultivate a "Safe to Fail" Environment

In a real-world enterprise, a major configuration error can cost a company millions. The cyber club can be a sandbox where massive mistakes are not just tolerated but celebrated as learning moments.

- **Celebrate the "Oops" Moments**
  Encourage students to take risks. A student who accidentally locks their entire team out of a competition network learns a lesson they will never forget.

- **Reframe Failure as Interview Material**
  Mistakes made in the safety of a club environment become incredible stories of resilience and problem-solving during job interviews. As one advisor noted, an epic failure in a club competition actually helped a student land a job with the Space Force because she could articulate exactly what went wrong and how she handled it.

Summary

To build a sustainable cyber club, educators must step back from the podium and allow students to take the wheel. By focusing on near-peer mentorship, hands-on application, and a culture where it is safe to fail, you transform a simple student organization into a powerful incubator for job-ready cybersecurity professionals.

What does K12 engagement look like?

- **Near-Peer Outreach & Mentorship:** Utilizing current undergraduate cybersecurity students to deliver interactive classroom presentations, guest lectures, and career discussions directly within local schools.
- **Structured After-School Programs & Micro-Camps:** Designing low-barrier, non-residential, multi-week programs (e.g., meeting once a week for a month) that focus on specific, hands-on technical concepts like cryptography, digital citizenship, and foundational coding.
- **National Summer Camp Collaborations:** Hosting intensive, federally sponsored summer camps, such as GenCyber programs, which introduce middle and high school students to fundamental security principles in an immersive setting.
- **Collaborative Curriculum Integration & Virtual Labs:** Partnering with K-12 computer science teachers to integrate specialized cybersecurity modules or provide access to virtual training grounds.
- **Community-Wide Cyber Celebrations & Capstones:** Hosting family-friendly events where younger students demonstrate practical skills, such as securing a simulated network or solving puzzles, in front of parents, care-givers, siblings, and community members.

K12 Engagement

Introduction

For higher education institutions, K-12 engagement can generate many benefits: early outreach demystifies cyber at a stage when students are first forming career aspirations and making future study plans. Exposing middle and high schoolers to the broad spectrum of cyber, colleges and universities can break through common cultural stereotypes, such as the myth that cyber is solely for technical introverts or bad actors and generate an enrollment pipeline. Participants gain hands-on technical literacy, undergraduates develop critical communication and leadership skills, and the academic institution establishes itself as a supportive and highly visible community leader.

CASE STUDY: Cedarville University

(Interviewee: Dr. Seth Hamman)

The development of a dedicated academic cyber center is a requirement of CAE-CO designation, and Cedarville developed its academic cyber center alongside building its CAE-CO designation application in 2018. To secure institutional support from university leadership, Dr. Hamman and his colleagues structured the center's mission around three distinct pillars:

1. **Develop cyber leaders in the classroom (academic excellence).**
2. **Shape cyber education in the Academy (national advocacy, pedagogy, and CAE committee contributions).**
3. **Promote cyber awareness in society (community outreach).**

Under this third pillar, the Cyber Center launched a series of ambitious K-12 education initiatives aimed at local rural public schools, private schools, and regional homeschool networks.

Rather than relying on already overburdened faculty members to design and run outreach programs, Cedarville adopted a decentralized model that utilized student-led execution. Hamman compares this to collegiate

sports teams: just as varsity soccer players run community youth leagues, undergraduate students can serve as the visible vanguard of the cyber program. This near-peer dynamic is incredibly powerful: because college students are close in age and culture to middle and high schoolers, their lessons resonate deeply. Additionally, engaging undergraduates expands the institution's bandwidth. As Hamman explains: *"If it wasn't that way, my colleagues and I simply wouldn't be able to do very much because we're pretty limited... But if our students are doing it, I can help coach the students. If we have ten students that are involved in wanting to lead these initiatives, now we can do ten things as opposed to just one thing. You get that multiplication effort."*

Cedarville launched an after-school program designed specifically for middle school students. The structure of the program was intentionally designed to minimize administrative and logistical friction:

- **Strategic Timing:** The program took place on four consecutive Tuesdays in February. February is historically a "shoulder season" for youth sports when basketball is winding down, and spring soccer has not yet begun, so the scheduling minimized scheduling conflicts.

- **Accessible Logistics:** Sessions ran from late afternoon to early evening at the university, allowing local students to easily walk across the street or be dropped off by parents.

- **Tactile Hardware Challenges:** Rather than staring at traditional computer monitors, students used interactive hardware components. The program purchased Micro:bits—inexpensive, pocket-sized programmable microcomputers—to give middle schoolers a physical, tangible gateway into hardware hacking and coding logic.

- **The Cyber City Capstone:** On the final evening, families were invited to join their children. Over pizza, the parents watched as the middle schoolers put their new skills to the test in a collaborative capstone challenge: hacking a physical "Cyber City" model to safely trigger a simulated emergency shutdown (complete with realistic smoke emerging from a toy nuclear reactor).

The impact of this outreach goes beyond K-12 exposure: the university students who design and execute these lessons also experience profound personal and professional growth. They gain:

- **Autonomy and Courage**: Designing lesson plans, organizing logistics, and managing classrooms builds immense professional confidence.

- **Career Readiness:** Students can showcase these leadership experiences directly on their résumés and discuss them in technical job interviews, giving them a distinct competitive edge.

- **Community Good Will:** The university establishes itself as a supportive, generous neighbor that actively invests back into the local municipality, creating invaluable public relations and strengthening regional ties.

CASE STUDY: Florida State University

(interviewee: Dr. Xiuwen Liu)

While Cedarville's academic outreach focuses on local, student-led after-school programs for middle schoolers, Florida State University's (FSU) youth programs are designed to inspire and prepare high school students for advanced academic research and professional pathways.

For the past five years, FSU has hosted Saturday summer bootcamps during June and July. To keep participation completely accessible and reduce socio-economic barriers, FSU provides free breakfast and pizza lunches to all participants. The bootcamps typically serve 10 to 15 students at a time, ensuring a low student-to-instructor ratio. The curriculum centers on Capture the Flag (CTF) exercises that transform complex cybersecurity concepts into interactive, gamified challenges. Under the guidance of faculty and student instructors, participants gain hands-on experience in:

- **Cryptography and secure communications:** Learning how to encrypt, decrypt, and protect sensitive data.
- **Digital forensics and cyber investigations:** Recovering hidden or deleted data to reconstruct digital timelines.
- **Reverse engineering of software:** Deconstructing compiled code to understand its underlying behavior and identify vulnerabilities.
- **Binary exploitation:** Discovering and leveraging software vulnerabilities in a controlled sandbox environment.
- **Web security:** Analyzing and defending against common web application weaknesses.

The bootcamp series concludes with a collaborative mini-CTF competition where students apply their newfound skills in a team-based, real-time defensive scenario.

In addition to the Saturday bootcamps, FSU's cyber faculty also contribute to the university's highly competitive Young Scholar Program (YSP). YSP is an intensive, eight-week summer residential experience for outstanding 11th and 12th-grade students from across the state of Florida. Each year, 40 select scholars are brought to FSU's campus to live in the residence halls and work alongside university researchers. In the cyber track, faculty and student mentors introduce these advanced students to cutting-edge research topics, including Artificial Intelligence (AI) security and machine learning defenses.

By exposing students to academic research at an early stage, FSU successfully bridges the gap between high school STEM interest and advanced collegiate research.

As with many CAE-designated institutions, both Cedarville and FSU host GenCyber camps during the summer.

Key Considerations

1 / Leverage a "Near-Peer" Model to Maximize Scale

Do not attempt to run K-12 outreach entirely on the shoulders of your faculty. Instead, treat your undergraduate cybersecurity major or student club as the operations team. Empower them to take ownership of curriculum design and classroom instruction. The faculty's role should be that of a supportive coach, handling high-level administrative tasks, securing funding, making initial administrative phone calls to school principals, and providing pedagogical feedback.

2 / Implement Tiered Safety Policies and Begin with Low-Risk Formats

Navigating youth protection policies can be a major hurdle. To launch programs quickly, start with non-residential, short-duration formats (such as after-school programs or day camps) for older age groups (middle or high school). These typically fall under less restrictive child-safety tiers than elementary-aged or residential programs. Ensure all participating university students and faculty undergo criminal background checks and implement standard boilerplate safety waivers early in the planning cycle.

3 / Focus on Physical, Tangible, and Gamified Learning

Avoid heavy lectures and dry command-line prompts. Middle schoolers and early high schoolers respond best to gamified challenges and physical

hardware. Incorporate affordable devices like microcontrollers (Micro:bits or Raspberry Pis) and build highly visual challenges, such as controlling LED light sequences or communicating via radio signals. These tangible outputs make the abstract concepts of cyber understandable and exciting.

4 / Design Collaborative Capstones that Engage the Whole Family

A successful youth program should celebrate its graduates publicly. End your multi-week programs or day camps with a showcase event and invite parents, siblings, and teachers. Providing a low-cost meal, like pizza, encourages high family turnout. Letting younger students show their parents exactly how they secured a system or solved a cryptography puzzle builds pride, reinforces learning, and turns local parents into active advocates for your institution's program.

5 / Align Outreach Formats with Strategic Institutional Milestones

K-12 outreach should not exist in a vacuum; it should directly support your department's strategic goals. Relating your community engagement directly to institutional initiatives makes it easier to secure internal funding, dedicated lab space, and administrative approvals from leadership.

"What started 15 years ago as a conversation about designation has led to a culture of innovation and excellence in Cybersecurity and the greater campus. Who knew that a regional university could have a hand in developing a national cyber camp program, a national community of colleges and universities, creating a culture of student community involvement that has reached 60,000 people in our region. When people ask about the impact of the CAE program, I say "you have no idea!"

Dr. Tony Coulson,
California State University San Bernadino

Developing regional hubs can:

- Build tightly-knit communities through regional meetings, collaborative working groups, and localized newsletters.
- Synchronize an ecosystem of urban and rural, large and small institutions. By serving as a central point of contact, they can allow smaller schools to access the same federal grants, industry partnerships, and curriculum resources as major research institutions.
- Provide a collaborative space to mentor graduate students, transitioning military personnel, and industry professionals who want to teach and inject new ideas into the faculty pipeline.
- Create seamless, skills-based pipelines that transition students, veterans, and military spouses into critical local defense and industry roles and help solve regional skills shortages.

Regional Hubs

Introduction

A regional hub serves as a collaborative, geographically-focused network that unites academia, local businesses, military commands, and government entities to strengthen collective digital defenses. Rather than operating in isolation, regional hubs act as localized engines that synchronize diverse institutions. They establish an essential bridge between national strategic directives and grassroots execution, building cohesive pipelines from high schools, community colleges, and universities into active national security and defense careers. By decentralizing administration, these hubs provide a physical and virtual infrastructure where members share resources, co-author grants, align curricula to frameworks like the Department Cyber Workforce Framework (DCWF) , and provide professional development to sustain the next generation of cyber educators.

CASE STUDY: University of Colorado Colorado Springs

(Interviewee: Gretchen Bliss)

The University of Colorado Colorado Springs (UCCS) provides an example of how a regional hub can move beyond simply connecting academic institutions to help build a broader cyber ecosystem. From 2020 through 2023, UCCS led one of the regional hubs funded by the NSA to strengthen connections across the rapidly growing National Centers of Academic Excellence in Cybersecurity (NCAE-C) community.

When Gretchen Bliss joined UCCS as Director of Cybersecurity Programs in 2020, the university was already designated as a CAE-CD. The opportunity, in her view, was to make greater use of that designation by strengthening connections among UCCS faculty and leadership, other CAE institutions, government, industry, and the surrounding community. UCCS organized much of this work around its POWER cyber strategy: Partnership, Outreach, Workforce Development, Education, and Research.

The 2020 regional hub grant provided a structure for putting that approach into practice on a much larger scale. UCCS was responsible for a geographically dispersed region of CAE institutions across the western United States. Rather than treating the hub primarily as an administrative network, UCCS used it as a mechanism for building relationships, sharing information, identifying collaboration opportunities, and connecting academic institutions with government, industry, K-12 education, and workforce-development partners.

A central element of the UCCS approach was consistent engagement. Regular meetings gave participating institutions opportunities to introduce their cyber programs, share emerging initiatives, identify common challenges, and learn what other institutions across the region were doing. These interactions helped move relationships beyond occasional national meetings and created a network in which institutions could more readily exchange ideas, pursue partnerships, and connect one another with resources and opportunities.

UCCS also leveraged the hub to connect the academic community with the region's substantial cyber, military, federal, and industry presence. Activities included strengthening government and industry relationships, supporting articulation and academic partnerships, sharing grant and program opportunities, and expanding cybersecurity outreach and workforce-development activities. During this period, UCCS significantly expanded its community engagement, ultimately conducting more than 100 localized outreach activities reaching more than 18,000 participants across K-12 education, higher education, industry, government, and the broader community.

The hub experience also highlighted the value of developing people as well as programs. Regional and virtual activities created opportunities for faculty, graduate students, and industry professionals interested in teaching to build professional networks, share innovative approaches, and learn from more experienced members of the CAE community. This was particularly valuable for institutions where workload, travel costs, or limited professional-development funding made participation in national activities difficult. In this way, the hub became not only a mechanism for institutional collaboration but also a means of strengthening the pipeline of future cybersecurity educators and leaders.

Several lessons emerged from the UCCS experience. First, regional hubs are most effective when they function as active communities rather than simply communication channels. Regular interaction helps participants understand one another's capabilities and creates the relationships necessary for collaboration. Second, geographic proximity and regional knowledge matter. Institutions often face similar workforce, employer, government, and educational challenges, making regional collaboration particularly useful. Third, successful hubs need dedicated coordination. Relationships, meetings, outreach, information sharing, and partnership development require sustained leadership and administrative capacity.

The 2020–2023 experience also demonstrated that a hub can provide infrastructure for a much broader ecosystem. It can become a central point for connecting institutions to partnerships, grants, working groups, workforce initiatives, professional development, and information that individual institutions may have difficulty accessing on their own. It can also provide a mechanism for gathering information from the region and communicating regional needs back to the larger CAE community.

For UCCS, the value of the hub grant extended beyond the grant period itself. The relationships, outreach infrastructure, and collaborative practices developed through the hub strengthened the university's ability to connect cyber education with community and workforce needs. The experience reinforced a central lesson from UCCS's work: a regional hub creates the greatest value not simply by connecting institutions, but by creating the conditions for those institutions and their partners to work together.

Key Considerations:

1 / A coalition of the willing
Before launching a regional hub, identify your core group of motivated academic, industry and federal leaders who have a desire to collaborate.

2 / Right-sizing the geographic scope
Balance scale against engagement depth. A smaller hub (e.g., 50–60 institutions) allows for frequent, high-touch interactions and faster learning compared to massive hubs (over 100 institutions). Tailor your boundaries to match local defense and civilian demand.

3 / Secure sustainable funding
Establish dedicated infrastructure support. Funding is vital to support the continuance of the hub, manage regional events, run annual reports, and measure economic return-on-investment (ROI) to key stakeholders like the Department of War.

4 / Establish clear ROI metrics
Ensure you establish data-gathering mechanisms early. Without a clear way to measure the economic impact and workforce pipeline value of your hub, securing long-term funding from government and defense sponsors becomes extremely difficult.

5 / Synchronize diverse ecosystems
Bridge the gap between urban and rural schools. Act as a centralized access point for the entire community. Use shared toolkits, virtual platforms, and centralized application systems so smaller schools can leverage the resources of larger institutions.

6 / Align academic pathways with regional employers
By mapping existing coursework to standardized frameworks like the NICE/DCWF work roles, hubs create seamless, skills-based pipelines that quickly transition students, veterans, and military spouses into critical local defense and industry roles.

"As a former student at a CAE institution and now a professor at one, I've come full circle. The resources that shaped me, such as scholarships, hands-on research through grant-funded work, competitions, and clubs, came not just from my own institution, but from the wider CAE community. This collaborative, hardworking network is what pushed me toward teaching cybersecurity and being engaged with the cybersecurity education community. Now, as the program continues to evolve, I get to shape those same opportunities for my students."

Paige Flores, PhD.
California State University San Bernadino

An effective SSOC:

- **Simulates or operates live, realistic defense workflows:** Bridges classroom theory and professional practice by immersing students in authentic cyber defense tasks—such as live-alert monitoring, hypothesis-driven threat hunting, incident response, packet capture analysis, and enterprise intrusion investigations.
- **Maps directly to Industry & Workforce frameworks:** Aligns curriculum and daily responsibilities with established workforce standards like the Department Cyber Workforce Framework (DCWF) (e.g., Cyber Defense Analyst [511] and Cyber Defense Forensics Analyst [212]), ensuring technical skills and deliverables match employer expectations.
- **Fosters tiered mentorship & student leadership:** Establishes progressive responsibility structures (e.g., Tier 1 through Tier 3 analysts) where experienced peers guide junior members, while instilling critical professional standards including ethical conduct, NDAs, teamwork, and incident reporting.
- **Delivers tangible institutional and career value:** Directly strengthens campus security posture through active event remediation while equipping students with demonstrable, on-the-job operational experience that significantly accelerates job offers and hiring momentum.

Student Security Operations Center (SSOC)

Introduction

Student Security Operations Centers (SSOCs) are immersive, hands-on, simulated environments where students serve as cyber defense analysts and threat hunters. SSOCs mimic the high-stakes, fast-paced environment of real-world security teams and provide opportunities for students to learn through responding in real-time to simulated threats and operational challenges.

An effective SSOC provides a bridge between the classroom and professional career tracks through creating an environment in which students can develop the technical confidence and collaboration skills they need to transition smoothly into the cyber workforce. For colleges and universities, the SSOC establishes a scalable training model that builds program prestige and strengthens ties with industry and defense sectors. For students, the SSOC is a safe yet realistic space to monitor live alerts, hunt for threats, and practice incident response, thereby accelerating their careers and boosting their employability. For the faculty who guide them, coordinating an SSOC offers invaluable opportunities to mentor students, support their professional growth, and stay connected to evolving industry demands.

CASE STUDY: Coastline College

(Interviewees: Dr. Tobi West and Professor Andrea Barrios)

The simulated Student Security Operations Center (SSOC) at Coastline College is a virtual, experiential learning space built from the ground up to prepare students for real-world cyber defense careers. Developed in close collaboration with cybersecurity subject matter experts, this innovative program serves as a high-fidelity launchpad into the industry.

Rather than relying on generic academic exercises, students in the SSOC dive into simulated operations that occur regularly in live SOCs. They learn by rotating through the core functions of a live SOC. Students monitor and triage alerts in an enterprise security monitoring platform, leverage endpoint and

network telemetry to conduct hypothesis-driven threat hunting, uncover suspicious or previously undetected activity, and investigate simulated intrusions against a simulated Active Directory enterprise from the initial compromise through malware command-and-control. Hands-on forensics simulations complement these activities, including packet capture, host artifact analysis, malware examination, and formal incident reporting, thereby reinforcing the full case lifecycle and the documentation standards expected of professional Cyber Defense Analysts and Cyber Defense Forensics Analysts. To retain interest and immerse students in the rhythm of live, actual operations, the program incorporates regular SOC meetings and specialized workshops that solidify their understanding of the cyber defense domain and support a clear pathway from classroom to career. To maximize operational relevance, the 1-unit course curriculum is mapped directly to the DCWF, specifically targeting the 511 (Cyber Defense Analyst) and 212 (Cyber Defense Forensics Analyst) work roles.

The initial response was overwhelming: in each of its first two offerings, more than 40 students applied, which far exceeded the program's 15-seat capacity, and the SSOC experience has proven a valuable differentiator for students pursuing cyber careers. Two students who highlighted their SSOC experience during job interviews received employment offers, while another student who included the SSOC on their résumé and discussed the experience during interviews is currently progressing through the hiring process for a cyber position with a DoW contractor. All three students reported that employers were particularly interested in their SSOC experience, with interview discussions focusing extensively on the knowledge, skills, and real-world operational experience they gained through the program.

Following its second successful iteration and favorable student feedback, Coastline is now leveraging these insights to scale the initiative. Plans are already underway to expand seating capacity, introduce progressive second- and third-term course offerings, and integrate cutting-edge AI support tools. But Dr. West and her team are also aware of the challenges in running an effective SSOC, and they continue to seek new and innovative solutions for obstacles they have faced, including asynchronous teamwork that limits coordination and inconsistencies in prerequisite knowledge among student participants.

CASE STUDY: The Citadel

(Interviewee: Dr. Shankar Banik)

In May 2023, the Citadel established a student-led, student-operated Security Operations Center (C-SOC) to provide cadets with a real-world, professional environment for developing advanced cyber skills. By integrating academic principles with live operational responsibility, the C-SOC serves as a best-practice model for creating "SOC-Ready Principled Leaders" who provide tangible security value to the college while achieving an unparalleled level of experiential learning.

As a student-led, enterprise-supported model, the C-SOC is founded on a unique collaborative model between cadets and the Citadel's Enterprise IT Team. The center's mission is twofold: to educate and train principled leaders with the cyber skill sets needed for the modern workforce, and to provide direct, tangible security services to the college. To achieve this, the C-SOC maintains a professional structure comprising tiered Cadet Analysts (Tiers 2 and 3), creating a clear path for progression and mentorship. This structure ensures efforts align with the college's broader security posture while allowing junior analysts to learn from more experienced peers, fostering leadership and a culture of shared knowledge.

The C-SOC is not a simulation; it is an active component of the Citadel's live cybersecurity defense infrastructure where cadets are entrusted with analyzing and documenting real-time network traffic. Immersion in a live operational environment enables students to move beyond theoretical knowledge to practical application. In their core functions, analysts interpret threat intelligence, compile monthly and yearly reports for the Enterprise IT Team, and research and recommend specific remediation plans for security incidents, directly contributing to the college's defense. Throughout these operations, students gain hands-on proficiency with an extensive suite of industry-standard tools, including Rapid7 (SIEM), Palo Alto, Zeek, OpenVAS, Metasploit, and Security Onion, ensuring they are fully prepared for the technological demands of the workplace.

The creation of a student-run SOC navigating a live enterprise network presents inherent challenges regarding security, trust, and consistent operational quality, which the Citadel C-SOC overcame through a deliberate

focus on culture and structure. To clear the trust obstacle and instill the critical importance of confidentiality, all cadets are required to sign a Non-Disclosure Agreement (NDA) as a foundational lesson in professional ethics. To address the skills gap and establish a baseline of competence, the C-SOC implemented a structured training curriculum and a tiered progression system (Tier 1 to Tier 3) that includes Capture the Flag (CTF) events, an operational readiness program, and live-fire exercises. Finally, rather than relying on a top-down approach, the C-SOC tackled the leadership challenge by empowering its students to take the lead on key initiatives, such as composing questions and conducting interviews with prospective new members, thereby fostering a deep sense of ownership.

As evidence of effectiveness, the C-SOC's success as a learning environment is measured by both its operational impact and the demonstrable growth of its student analysts. Since its inception, the center has delivered tangible security impact by assisting with approximately 10 active network attacks, managing over 1,000 endpoints, and closing thousands of investigations (3,059 in 2024 alone), proving that students are actively enhancing the Citadel's cybersecurity posture. This experiential learning is amplified through the Cyberbit Cyber Range, which provides full-scale, emulated enterprise networks for live-fire events such as defending against ransomware, keylogging, and insider threats, giving students a hyper-realistic, hands-on keyboard experience embedded directly into undergraduate coursework. Ultimately, this training program is explicitly aligned with DoD Cyber Security Analyst qualifications, with opportunities for certifications such as Security+, Network+, and CySA+, ensuring graduates are not just SOC-ready but fully prepared to meet rigorous federal and private-sector workforce standards.

By successfully merging academic goals with real-world operational demands, The Citadel's C-SOC serves as an exemplary case study for building a highly effective pipeline for the next generation of cyber leaders.

Key Considerations

1 / Link Education and Workforce Outcomes

Successful experiential learning environments begin with a clear link between education and workforce outcomes. Rather than centering programs on academic content alone, the most effective models are built around the knowledge, skills, and behaviors required in professional practice. For example, aligning the curriculum with established standards, such as the DCWF and targeting recognized roles like Cyber Defense Analyst (511) and Cyber Defense Forensics Analyst (212) ensure that training is immediately relevant to employers. Whether students are working in a high-fidelity simulation or contributing to a live operational environment, the educational value comes from engaging in realistic workflows, using industry-standard tools, producing professional-quality deliverables, and solving problems that mirror those encountered in the workplace. This alignment with workforce expectations creates a bridge between classroom learning and career readiness.

2 / Intentional Design and Opportunities for Progression

High-impact SOC environments are not standalone activities but rather structured ecosystems. It is important that recruitment uses a clear, efficient methodology for ensuring student suitability and motivation so that the best cohort is onboarded for the program's success. Additionally, foundational training, progressive responsibility, and opportunities for specialization are important for success. Students benefit most when they can move through increasingly sophisticated levels of participation while receiving guidance from faculty, practitioners, and experienced peers. Equally important is the integration of leadership development, communication, documentation, teamwork, and professional ethics. These environments succeed not only because students develop technical competencies but also because they learn to operate as professionals within a mission-driven organization.

3 / Student Ownership, Engaged Mentors, and Institutional Buy-in.

As programs grow in complexity, challenges such as skill variability, operational consistency, trust, coordination, and resource limitations become more pronounced. Successful programs address these challenges through structured training pathways, clear expectations, formalized processes, and strong mentorship models. Fostering student ownership strengthens engagement and helps establish a culture of accountability, collaboration, and continuous learning. In practice, the most effective SOC learning environments resemble professional organizations more than traditional academic laboratories.

Strong programs demonstrate measurable outcomes for multiple stakeholders, including students, employers, faculty, and the institution. Student employment outcomes, enhanced workforce readiness, improved institutional reputation, operational contributions, and strengthened industry partnerships collectively provide evidence of impact. The broader lesson is that experiential learning within a SOC should be viewed not as a supplemental activity but as a strategic institutional investment that can advance student success, meet workforce demands, and create meaningful organizational value.

Summary

A Student Security Operations Center (SSOC) serves as a high-impact, experiential bridge connecting academic instruction with real-world cyber careers. By either simulating complex enterprise environments or actively partnering with campus IT to analyze live network telemetry, an effective SSOC moves students past passive learning into hands-on threat detection, triage, and incident remediation. Guided by workforce standards such as the DCWF and supported by structured tiered mentorship, SSOCs provide colleges with measurable institutional security value while transforming students into highly competitive, “SOC-ready” professionals who stand out to defense and commercial recruiters.

“Guided by workforce standards such as the DCWF and supported by structured tiered mentorship, SSOCs provide colleges with measurable institutional security value while transforming students into highly competitive, “SOC-ready” professionals who stand out to defense and commercial recruiters”.

Things to consider when building AI into the curriculum:

- **The "Neither/Nor" Assessment Paradigm:** Modern cybersecurity assignments must be designed around complex, iterate-heavy tasks that neither a human nor an AI can execute effectively in isolation.
- **Redefining "Hireable":** The entry-level hiring baseline has fundamentally shifted. True competency is no longer defined by siloed technical execution, but by a student's ability to orchestrate secure, reliable, and compliant AI workflows.
- **The "Sycophantic Engine" Trap:** Because commercial LLMs are engineered to agree with and please the user, students must develop deep "prompt-skepticism" to identify, audit, and correct hallucinations.
- **Agile Curriculum Pivoting:** As breakthrough agentic tools release, faculty must possess the institutional support and technical flexibility to pivot syllabi mid-semester to match rapid industry shifts.

Using AI in the Curriculum

Introduction

The emergence of large language models (LLMs) and generative AI generates significant questions around pedagogical design and learning processes for many institutions. Over the past few years, academia has learnt that it can neither ignore nor control student engagement with AI. Restrictive plagiarism detectors, prompt-logging, or forcing students to verify every AI-assisted citation within a physical library do not benefit the student's educational success. It is imperative that initial suspicion of AI as a potential cheating engine is replaced by an increased awareness of the practical contemporaneous and future benefits and limitations of AI use. This is particularly important in the academic discipline of cyber where key behaviors can be potentially automated, both in relation to student engagement and future work roles.

The cyber job sector is increasingly impacted by AI. Employers are evidencing a reduction in entry-level jobs focused on basic, repetitive scripting or static system monitoring, and articulating a greater need for candidates who can deploy, secure, and govern AI-driven automations and affordances.

To prepare students for this landscape, educators need to teach students how to treat AI as a collaborative partner and an efficiency tool. This chapter outlines how to establish an agile, AI-integrated cyber curriculum.

CASE STUDY: California State University San Bernardino

(Interviewee: Dr. Vincent Nestler)

During the 2026 spring semester, Dr. Vincent Nestler recognized that the standard "information-retrieval chatbot" model of AI (such as ChatGPT-4) was already becoming obsolete in professional cyber environments. In February 2026, the open-source release of Open Claude (and its agentic framework, Cloudbot) marked a major technological milestone. Unlike static chat interfaces that simply answer questions, cognitive agents operate in an autonomous loop: they can be given high-level goals, autonomously write HTML or script files, execute local commands, audit their own outputs, and

deliver finished projects. When NVIDIA CEO Jensen Huang publicly declared this transition to agentic software as one of the most critical milestones in modern computing history, Nestler did not wait the next annual curriculum review: he pivoted his entire syllabus within a few weeks of the announcement.

Rather than teaching students to write simple code snippets, Nestler re-engineered his curriculum around complex system orchestration, tasking his students with deploying local AI agents, writing custom system-automation loops, and ensuring that those autonomous agents operated within strict compliance and data-security policies. Students graduated from his course with a familiarity with emerging uses of AI and confidence in approaching employers based upon their current needs, rather than having completed a course that had prepared them for an already obsolete work role.

In interview for this chapter, Nestler spoke about the very real impact this rapid redesign of his course had for one student. This student had sent out over 500 résumés without receiving a single callback or interview. When she sought career advice to Nestler, he was frank: *"Your résumé is a dime a dozen. Under standard conditions, you are going straight into the trash. If you want to be noticed, you have to demonstrate a capability that employers desperately need but nobody else knows how to do."* The student threw herself into the newly pivoted agentic AI capstone, learning how to configure secure local private clouds, run autonomous coding loops, and audit AI outputs for system compliance. At her next interview, she bypassed her standard coursework and presented her agentic AI automation portfolio. She walked the recruiters through exactly how she configured secure AI agents in Nestler's class to automate network-hardening tasks while maintaining strict compliance standards. The interviewing panel told her that out of dozens of senior applicants with ten to fifteen years of traditional experience, she was the only candidate who could practically explain and demonstrate how to deploy AI securely. This student acquired a highly competitive employment contract.

Good practices for AI integration in Cyber Education

1 / Establish an Agile Local Academic Sandbox (The "Cyberlab")

To teach advanced AI integration, departments cannot rely on public cloud platforms that charge high subscription fees or raise student privacy concerns.

- Build Private Cloud Infrastructure: Secure local, department-controlled servers (a private cloud) where students can deploy local Virtual Machines (VMs) and host local, open-source Large Language Models (LLMs) like Llama-3 or Mistral.

- Bypass External Restrictions: Having a dedicated "cyberlab" allows students to safely run penetration-testing tools, hook up autonomous coding agents, and automate network attacks without risking external network blacklists or violating public platform Terms of Service.

2 / Design Assignments Around the "Infinite Scale" Principle

If a student can complete an assignment with a single, simple prompt to a public chatbot, the assignment is pedagogically dead.

- **The Neither/Nor Rule:** Design assessments that require outputs of such high complexity that neither a human working alone nor a simple AI prompt could complete them.

- **Require Multi-Step Orchestration:** Instead of asking students to write a short 20-line script, require them to build a fully functional, multi-file software application. Students must use AI to generate the foundational modules, but they must manually stitch the files together, troubleshoot the interface, configure database connections, and run multiple debugging loops. This shifts the grading focus from *syntax memorization to systemic integration and architecture.*

3 / Audit the "Sycophantic Engine" Trap

A critical component of AI literacy is teaching students that AI models are mathematically optimized to please the user, which frequently leads to dangerous cognitive bias.

- Demonstrate User Bias: Teach students how LLMs adapt their answers to match user expectations. For example, if a user prompts an AI with a leading question about a specific, highly controversial topic, the AI will often agree with the user's bias, even fabricating false evidence to support it.

- Teach Prompt-Skepticism: Require students to treat AI outputs as draft-quality work-in-progress. Students must actively audit every line of code, verify technical claims against official documentation, and prove that they understand the underlying logic of the AI's suggestions.

4 / Secure Proactive Leadership Support

Pivoting a course syllabus mid-semester to keep pace with rapid technological breakthroughs can raise administrative concerns regarding course consistency and student complaints.

- Build Departmental Alignment: Faculty must proactively communicate with department chairs, deans, and academic committees. Explain why a mid-semester adjustment is necessary (such as a massive software release that changes industry hiring requirements).

- Protect Academic Integrity: When leadership understands that an agile syllabus directly translates to immediate student placements, they can provide the institutional protection needed to deploy cutting-edge assessments.

Summary

Integrating AI into the cybersecurity curriculum transforms the educational experience from a static "spreadsheet exercise" (measuring classroom hours and inputs) to a dynamic, outcome-based model. By utilizing local private clouds, designing highly complex collaborative assignments, and actively combating the sycophantic bias of LLMs, departments can ensure their graduates are highly competitive.

As the definition of competence continues to shift, academic programs must resist the urge to retreat into retrogressive, pen-and-paper testing. Instead, they must lean directly into the hybrid era, preparing students to confidently manage the systems where human ingenuity and machine intelligence meet.

"The CAE Community is my extended family, and our annual CAE Symposium feels just like our family's Thanksgiving gathering. Watching this community grow over the last two decades through our Communities of Practice (CoPs) and deep faculty members' interconnections has proven that our shared dedication to the National Security Mission is the true bedrock of our success."

Yair Levy, Ph.D., College of Computing, AI, and Cybersecurity (CCAC), Nova Southeastern University, Ft. Lauderdale, Florida.

CAE Resources

CLARK: the Cybersecurity Labs and Resource Knowledge-base



Dr. Blair Taylor was serving as a subject matter expert with the NSA's College of Cyber when she noticed a growing gap between the need for cyber education and the number of faculty available to teach it. Developing new instructors would take years, and Dr. Taylor recognized that neither students nor the national security apparatus could wait that long. Rather than focusing on what was impossible, Dr. Taylor focused on what could be done immediately: if the nation could not produce new cyber faculty overnight, perhaps it could equip existing instructors with high-quality, classroom-ready resources. That idea became the foundation for the Cybersecurity Labs and Resource Knowledgebase (CLARK). Following a competitive process, Towson University was selected to prototype, develop, and host what would become a national resource for cybersecurity education.

From the outset, CLARK was designed to be much more than a file repository. Using Design Science research methods, Dr. Taylor and her team studied why previous curriculum-sharing efforts struggled and discovered a simple truth: quality drives adoption. If faculty members encountered weak or incomplete materials on their first visit, they would be unlikely to return. To build trust, when CLARK began, every submission would undergo a rigorous double-masked peer-review process to ensure both technical accuracy and instructional quality.

Built around a simple but powerful principle of "by-faculty, for-faculty," CLARK provides educators with access to peer-reviewed, classroom-ready learning objects developed by experienced cybersecurity instructors. These resources allow faculty to quickly integrate high-quality content into their courses rather than spending valuable time building curricula, labs, assessments, and instructional materials from the ground up.

CLARK operates with a standardized structure based on instructional time, with content organized into NanoModules (less than one hour), MicroModules (one to four hours), and Modules (multi-day instructional units). Learning objects are aligned with major national frameworks, including the NSA CAE Knowledge Units, the DCWF, and ACM curriculum guidelines. To support faculty who may not have formal training in education, the submission process incorporates Bloom's Taxonomy to help authors create stronger, measurable learning outcomes.

What truly sets CLARK apart is that it is not simply a repository of archived content: it is an active and continually evolving community resource. New materials are regularly contributed, reviewed, and published to ensure that educators have access to timely content that reflects the latest developments in cybersecurity and emerging technologies. As workforce needs evolve, CLARK evolves alongside them. For example, the platform recently introduced a comprehensive Introduction to AI and Machine Learning course developed through a collaborative workshop involving 20 nationally recognized AI experts. The curriculum was created specifically to help institutions address newly established CAE Knowledge Units and rapidly emerging industry demands.

CLARK's impact is reflected in its adoption nationwide: the platform has generated more than 93,000 unique downloads and serves over 19,000 active users. Its resources are being utilized by around 1,000 colleges and universities, which represents roughly one quarter of all higher education institutions in the US. CLARK continues to expand into the K12 community.

Summary

The value of CLARK extends across the entire cyber education ecosystem.

- For institutions, it provides a strategic collection of vetted resources that support NCAE-C validation efforts, curriculum mapping, and long-term program growth.
- For faculty, it offers customizable presentations, laboratories, assignments, and assessments that enable immediate, high-quality instruction.
- For students, it delivers engaging, research-informed learning experiences, including self-paced security injections and hands-on activities designed to strengthen practical cybersecurity and secure coding skills.

At its core, CLARK demonstrates what is possible when the cyber education community works together. By enabling institutions to share proven educational resources, accelerate curriculum development, and rapidly respond to emerging workforce needs, CLARK has become a national model for collaboration, innovation, and academic excellence in cyber education.

Grants

(Many thanks to Alice Smitley for her expert input and guidance to this chapter)

For a newly designated Center of Academic Excellence in Cybersecurity (CAE-C), a federal grant can help translate that designation into action. While the CAE-C designation recognizes an institution's capacity, dedication, and alignment with national standards, federal funding provides the fuel to expand education, support national security workforce pipelines, and pilot innovative academic models. The CAE-C designation recognizes an institution's capacity and commitment, grant funding can help that institution put those strengths to work in visible, measurable ways.

Funding provides the critical resources needed to launch ambitious projects that would otherwise b*e out of reach. The value of a federal grant extends across the entire academic ecosystem and encompasses:*

- For the institution, it enhances prestige, expands research capabilities, and solidifies its leadership in cybersecurity education.
- For faculty and staff, it provides the means to develop groundbreaking curriculum, conduct vital research, and build programs that shape the future of the cyber workforce.
- For students, it creates unparalleled opportunities for hands-on learning, engagement in real-world projects, and access to cutting-edge technology and mentorship.

For a designated institution, this impact is often realized through cornerstone initiatives like the Early College Cybersecurity Credit (E3C) program, which builds dual-credit high school pipelines, or the DoW Cyber Service Academy (CSA), which provides critical student scholarships. Regardless of which specific grant you pursue, the fundamental rules for winning them remain the same.

Successfully navigating the federal grant lifecycle demands a strategic approach, a deep understanding of the process, and a strong internal coalition. This chapter serves as your practical guide to that process. By demystifying the requirements, outlining a roadmap for building an internal support team, and providing clear best practices, it equips you to pursue and manage federal funding with confidence, ensuring your institution can fully realize its mission as a National Center of Academic Excellence.

Build Your Internal Team First

Start with the internal team. Before drafting a proposal narrative, confirm who must be involved, what each office needs, and when they need it. This early coordination is one of the most important parts of grant readiness because it affects compliance, budgeting, approvals, and submission timing.

Specifically, you need to develop deep, collaborative relationships with:

- The Office of Sponsored Programs (OSP) or Grants Office: This office manages your institution's official submissions. OSP reviews proposal requirements, confirms compliance, applies institutional policies, and often submits the final package. For your team, this means OSP is not just a final checkpoint. It is a partner that can help you avoid budget errors, missing approvals, and compliance problems before they become deadline risks.
- The Financial and Accounts Payable Teams: These teams help build realistic budgets, track spending, process invoices, and manage post-award financial requirements. A federal grant is not a blank check. Each cost must follow the award terms and applicable federal rules. By involving finance early, you can confirm which costs are allowable, prepare for reporting requirements, and reduce the risk of disallowed expenses later.

You should not pursue a federal grant in isolation. Build your internal coalition early. Bring the right offices into the conversation as soon as you begin considering a grant opportunity, and share timelines, project scope, and requirements before the deadline pressure builds. Early coordination gives your team more time to identify risks, strengthen the proposal, and avoid preventable problems.

Laying the Groundwork: Your Institution's SAM.gov Registration

Before your institution can receive most federal funds, it must be registered in the System for Award Management (SAM.gov). While a small number of grants may not require it, the vast majority do, making an active registration a prerequisite for any serious grant-seeking institution.

The important detail is that the new SAM.gov registration is not instant. It can take several weeks to a month to move from initial request to active status. This process is handled at the institutional level, typically by your OSP, not by individual applicants.

A lapsed or incomplete registration can prevent submission at the deadline. Before considering any grant, confirm with your OSP that your institution's SAM.gov registration is active and will remain active throughout the application period. This simple early check can prevent a serious but avoidable submission problem.

For more details on the registration process, refer to the Registration Guide for Grants and Contracts (https://fundinglandscape.com/answers/sam-gov-registration-guide-2026).

The Art of the Proposal

Once you have assembled your internal team and confirmed your institution's readiness, the proposal is where you match your project vision to the solicitation. A strong proposal is not just persuasive; it is organized around the requirements reviewers are using to score it. Treat the solicitation as both instructions and a map for your narrative, budget, timeline, and supporting documents.

1 / Sticking to the Evaluation Criteria Makes the Reviewer's Job Easier

Each proposal solicitation will provide evaluation criteria against which all submissions will be judged. It serves as the reviewer's scorecard and your single most important guide. To give your proposal the best chance of success, address all criteria straightforwardly, make the information easy to find, and ensure the connections between the information and the criteria are easy to follow.

Grant reviewers are often subject matter experts evaluating dozens of proposals under a tight deadline. They will not hunt for information. Your job is to make their job as easy as possible. A proposal that is difficult to navigate will be scored lower, even if the ideas are brilliant.

Pro Tip: Use the evaluation criteria to build the outline for your proposal. Create headings and subheadings that mirror the exact language of the criteria (e.g., a section titled "1. Sound & Reasonable Methodology"). This enables the reviewer to easily align your narrative with their scorecard, making it easier to assign points.

Common evaluation criteria often include the following. Here is what is meant in practice:

- **Sound & Reasonable Methodology:** *Do you have a clear, realistic timeline and project plan?*

- **What this really means:** This is the "how" of your project. You need to demonstrate a logical, step-by-step plan for achieving your objectives. Included is the project timeline (like a Gantt chart), clearly defined roles for each team member, specific milestones, and a plan for assessing your progress. "Sound" means your plan is based on proven practices, and "reasonable" means your goals are achievable within the proposed timeframe and budget.

- **Cost Realism:** *Are your requested funds proportionate to what you actually plan to deliver?*

- **What this really means:** This is not about being the cheapest; it's about being the most credible. Every dollar you request must be justified and directly linked to a project activity. For example, if you request funds for a piece of equipment, you must explain why that specific equipment is necessary to achieve your project goals. A budget that is too low can be as damaging as one that is too high, as it signals to reviewers that you don't fully understand the scope of the work.

- **Deliverables:** *Are your project outcomes clearly defined, and will they be made available to the public where appropriate?*

- **What this really means:** Vague promises like "improve cybersecurity education" are not enough. A deliverable is a tangible product. Examples include: a new curriculum module, a series of faculty development workshops, a publishable research paper, or a piece of open-source software. Be specific about what you will produce, how it will be disseminated (e.g., on your website, via a national repository), and how it will benefit the broader community.

- **Clarity:** *Does your proposal cleanly account for every single requirement in the solicitation?*

- **What this really means:** This is about attention to detail. Did you answer every question? Did you include all requested attachments (like résumés or letters of support)? A clear proposal is also free of jargon and acronyms where possible, making it accessible to a wider range of reviewers.

- **Leadership takeaway:** proposal quality depends on more than the project idea. It also depends on institutional readiness, timely approvals, realistic budgeting, and a shared understanding of compliance responsibilities.

2 / Avoid Automatic Disqualification by Reading the Fine Print

The federal review process is strict. Submissions with missing documents, incorrect formatting, prohibited content, or late delivery may be deemed ineligible before the proposal is reviewed for merit.

Double-check that you have addressed all the evaluation criteria, provided any specific details or documentation requested, and that your proposal is formatted correctly. Complying with all restrictions on length, font size, margins, and even file naming conventions is important. Also, make sure you haven't included any prohibited items. Imagine spending a hundred hours on a proposal only to have it rejected because you used the wrong font or your file was too large to upload. These are not minor details; they are the first and easiest way for a federal agency to reduce a large pile of applications. Avoiding these easy pitfalls will ensure your proposal isn't immediately disqualified and can advance to evaluation on its merits.

Pro Tip: Create a compliance checklist based on the proposal instructions. As you complete each formatting and content requirement, check it off. Have a colleague, or someone from your OSP, do a final review of the checklist against the finished document before submission.

Evaluation Dimension	What Reviewers Are Scoring	Practical Execution Strategy
Sound & Reasonable Methodology	Is the timeline realistic, and is the project plan logical and achievable?	Build a detailed step-by-step plan. Include a clear Gantt chart, define team roles, establish measurable milestones, and outline a robust progress assessment strategy based on proven educational or technical practices.
Cost Realism	Are the requested funds highly aligned with and proportionate to the proposed scope of work?	Do not try to write the cheapest budget; write the most credible one. Ensure every budget line-item is directly justified by a corresponding narrative activity. Excessively low budgets signal a lack of scope awareness, while unlinked high costs raise compliance flags.
Tangible Deliverables	What concrete, publicly available outcomes will the project produce?	Avoid vague promises like "promoting cybersecurity." Specify clear, tangible outputs—such as a modular curriculum, faculty development workshops, publishable whitepapers, or open-source software tools—and detail how they will be hosted and shared.
Absolute Clarity	Does the document cleanly and completely account for every single solicitation requirement?	Address all questions directly. Write a clean, highly readable narrative that avoids unnecessarily dense jargon or undefined acronyms, making the text accessible to a multi-disciplinary review panel.

"I have been involved with the CAE program for over a decade, and it has been instrumental in the growth and success of our cybersecurity program at Bossier Parish Community College. The friendships, professional relationships, and collaborative network developed through CAE have provided valuable support, guidance, and opportunities throughout the years.

Participation in CAE-sponsored training and events has helped us stay current with national trends and best practices in cybersecurity education. Combined with feedback from our local industry partners, these experiences have helped ensure that our program remains relevant, aligned with workforce needs, and focused on preparing students for success in the cybersecurity field. The CAE community continues to be one of the most valuable resources in advancing both our program and our mission."

Chris Rondeau, Bossier Parish Community College

New and Early Career Faculty Development

For many new instructors, entering cyber education can feel like stepping into a classroom already moving at full speed. The content is technical, the tools change quickly, and students arrive with different levels of preparation, confidence, and curiosity. As Paige Flores, Lecturer at CSUSB 's School of Cyber & Decision Sciences, observes, *"You don't know what you don't know"* when first navigating the modern cyber classroom. That simple truth sits at the heart of CAE's New and Early Career Community of Practice.

Cyber programs often recruit from two very different talent pools: some faculty are newly minted Ph.D. graduates with deep research training, others are seasoned industry practitioners beginning a second career in teaching. Both groups bring tremendous value, and both also encounter surprises. Research-focused Ph.D. scholars may need support translating abstract concepts to a diverse undergraduate classroom; industry veterans, even after decades of hands-on experience in the technical and non-technical areas of cyber, may discover that turning lived expertise into an effective lesson is *"a completely different ball game."* Some struggle to align their courses with formal academic frameworks such as the CAE Knowledge Units, and others find themselves teaching introductory courses outside the specialized professional networks where they feel most at home.

Flores has seen these challenges firsthand during her time as a student researcher at Towson University and they informed her awareness of the need for an informative, supportive, professional development community for new and early-career cyber faculty. To help create that space, Flores

partnered with Gretchen Bliss from the University of Colorado, Colorado Springs to establish the "New and Early-Career Faculty" initiative under the CAE Community of Practice in Cyber Defense. They gathered a planning committee which includes representatives from multiple CAE institutions to incorporate diverse perspectives and connect new and early-career faculty with similar colleagues.

Rather than focusing primarily on research portfolios or formal institutional networking, the community meetings address the immediate, tactical realities of being a cyber educator. The group brings that mission to life through monthly, interactive workshops on Microsoft Teams and the topics come directly from what faculty say they need most: teaching abstract concepts such as networking, introducing Linux fundamentals, using AI in the classroom, navigating the intensive NCAE-C designation process, and preparing for funding opportunities.

Due to the challenges of early-career faculty life, with its crowded schedules and heavy course loads, the program is deliberately flexible; *"We're meeting them where they're at,"* Flores explains. Sessions are recorded and posted to a dedicated CAE Community YouTube playlist and, after each session, Flores sends a resource-rich follow-up email with links, tools, and discussion highlights.

The initiative also makes time to listen. Each January, the group holds 10-minute drop-in listening sessions to learn what faculty are struggling with and what support would help next. It is a small design choice, but an important one: by letting faculty shape the agenda, the community keeps its topics fresh, relevant, and grounded in real classroom needs.

The impact has been significant. The initiative now has a registration list of roughly 350 people, with a core group of about 100 educators engaging through live attendance, YouTube views, and email exchanges. The initiative has also become a seedbed for broader collaboration. It has helped spark cross-institution grant proposals and the creation of an AI pedagogy working group. What began as practical support for new faculty is now helping the larger CAE community learn together. For CAE leaders, the lesson is encouraging: a successful faculty development community does not have to become an overwhelming administrative burden. Flores estimates that the entire operational commitment requires at most six to eight hours per month. That includes the workshop itself, a brief planning meeting, and light follow-up.

The model works because it leans on guest speakers, uses email well, and accepts the natural "peaks and valleys" of faculty engagement. It also works because the people leading it care about community. As Flores puts it, *"If you have someone who's really interested in building communities... it doesn't feel like work. You get to do it for fun, and then you get to meet up with your friends once a month."*

XP Cyber

The XP Cyber Range is an academic cyber range that enables US-based educators to teach and assess their students' cyber skills and workforce readiness. Using a holistic approach, it also serves to gather data for educators through assessing competency, objective scoring, and documenting students' performance.

There are 77 distinct work roles in the Department Cyber Workforce F ramework, but traditional academic paths often treat "cyber" as a singular, monolithic subject. Students graduate knowing the theory of networking or the abstract concepts of cryptography, but they have never spent a single hour sitting in a high-stress, complex, living network or what to expect in a real-life cyber scenario; they have never had to coordinate with system owners, defend a multi-subnet corporate system under live attack, or patch a critical vulnerability on an active server.

In 2013, a small team at California State University, San Bernardino (CSUSB), under the direction of Dr. Vincent Nestler, studied this widening gap between academia and the workforce and decided to build a bridge: *"We built a cyber range because what we wanted to do required us to make one—not because we were actually interested in making a cyber range to start,"* recalls James Ashley, Director of Research and Development at CSUSB's Center for Cybersecurity and Artificial intelligence.

When Dr. Nestler and his team first secured funding from the Department of Homeland Security (DHS), their goal was simple but ambitious: to create realistic, scenario-based challenges where students could step directly into the shoes of a specific cyber work role. They wanted students to experience the complex and problem-solving centric nature of real cyber work within the scale, scope, messiness, and unexpected chaos of a real corporate network.

At the time, the available hands-on labs were painfully simplistic — sterile "sandbox" environments where a student followed a step-by-step guide to click a few buttons, enter a few commands, and complete a basic task. There was simply no context. No "why." If students were to become competent, they needed hands-on, experiential learning opportunities, and realistic, contextualized problems to solve in networks of scale and complexity. Nestler's team wanted to deliver to students *"the cyber workforce experience before the workforce,"* which would later become their project's tagline.

CSUSB developed their own distribution platform, built cutting-edge virtualization software, automation tools, and enterprise computing hardware. Hosted, purchased, and managed directly out of CSUSB, this infrastructure grew from a modest prototype into a powerful platform originally known as the NICE Challenge Project (named after the NICE Framework) and being rebranded as XP Cyber as its capabilities matured and expanded.

"A cyber range is kind of a silly word that everyone uses to describe roughly a virtualization solution that someone stood up somewhere," says Ashley, before warning that comparing one range to another is like comparing apples to oranges: they are not the same. An instructor can build a virtual corporate network from scratch, script custom attacks, and schedule precise windows of disruption. It sounds perfect on paper, but it harbors a quiet, destructive trap for educators: *"If you have one cyber professor, or a very small set of professors at an institution, you don't have the hours in the day to run a giant virtualization infrastructure, manage it, maintain it, create content, and provide support alongside teaching classes."*

Building and running a cyber range is a massive engineering endeavor, which is why XP Cyber operates with a dedicated, full-time staff of skilled engineers to keep the system online, update content, and provide "train-the-trainer" support to educators. This offloads the infrastructure challenges and gives professors their time back, allowing them to do what they do best: teach and educate.

The XP Cyber Range provides students with a wide variety of cyber work role-based experiences mapped to cyber workforce frameworks and knowledge units, including the Department Cyber Workforce Framework (DCWF), the

NICE Framework, and the NCAE-C Knowledge Units. The experiences provide opportunities for students to identify which work roles align with their career aspiration so that they develop the confidence to know they are ready to enter the cyber workforce.

XP Cyber' scenarios have been developed through engaged partnerships with federal agencies and national laboratories. Rather than guessing what realistic scenarios look like, Nestler's team have, for example, worked together with subject matter experts at the FBI to design it. When they received funding from CISA to build Industrial Control Systems (ICS) and SCADA environments, they collaborated directly with the nation's premier National Laboratories to replicate the highly specialized networks that run our power grids.

James believes that innovations in how we populate the talent pipeline are not coming from some large, massive discovery, but arise from the compounding of small actions. In his eyes, XP Cyber was never meant to be a magic bullet or a replacement for other educational methods, instead it is a critical part of a larger educational ecosystem.

XP Cyber is entirely free for any legitimate educational institution in the United States. By removing the financial and technical barriers to entry, the team at CSUSB have not just built a cyber range, they have built a national utility, an enduring playground of digital defense that empowers the next generation of cyber professionals to walk out of the classroom, step up to the keyboard, and confidently say: *"I know exactly what to do."*

"We used the CAE-CO designation as our blueprint when we decided that we wanted to build a world class cyber program at Cedarville. It was the best decision we could have made. After achieving designation in 2018, our cyber program had well-earned credibility with prospective students and employers. We attracted top students from all over the nation, and started building momentum that has been picking up steam ever since. It thrills me to know that we have a significant number of graduates working for the Department of War and making an impact for our national defense."

Dr. Seth Hamman, Cedarville University

Conclusion

Cyberspace is inseparable from military operations, critical infrastructure, economic strength, and daily life. The competition for talent is real and no single university or college can meet the scale of the requirement alone. The CAE community demonstrates that a distributed and continuously improving network can educate, innovate, and deliver at national scale and with an agility that can respond to emerging threats and evolving technologies.

The early chapters in this volume focus on the journey beyond designation, demonstrating how institutions have furthered their academic excellence through building advisory boards, coaching their career and student services, refining outreach engagements, expanding competitions and clubs, running Student SOCs, and participating in regional networks. The later chapters describe some key initiatives that benefit the entire CAE infrastructure. The practical next steps belong to the reader. I invite you to adapt these practices to fit your institution's mission, students, and region and then share what you learn with others, so that they might emulate your practices in ways that continuously develop their own excellence.

This volume exists because faculty across the CAE community were willing to document their experience for the benefit of others. Their generosity, and the daily commitment of thousands of colleagues who build programs, teach students, write grants, run competitions, and sustain partnerships, often on top of full teaching loads, is the reason the next generation of cyber professionals will be better prepared than any that came before.

The work beyond designation is not finished. It is the ongoing practice of excellence in service to students and to the nation. May the practices, resources, and pathways collected here help every institution advance that work with clarity, urgency, and lasting impact. When institutions learn from one another and share resources, our students, faculty, institutions, and employers gain a strategic advantage. •