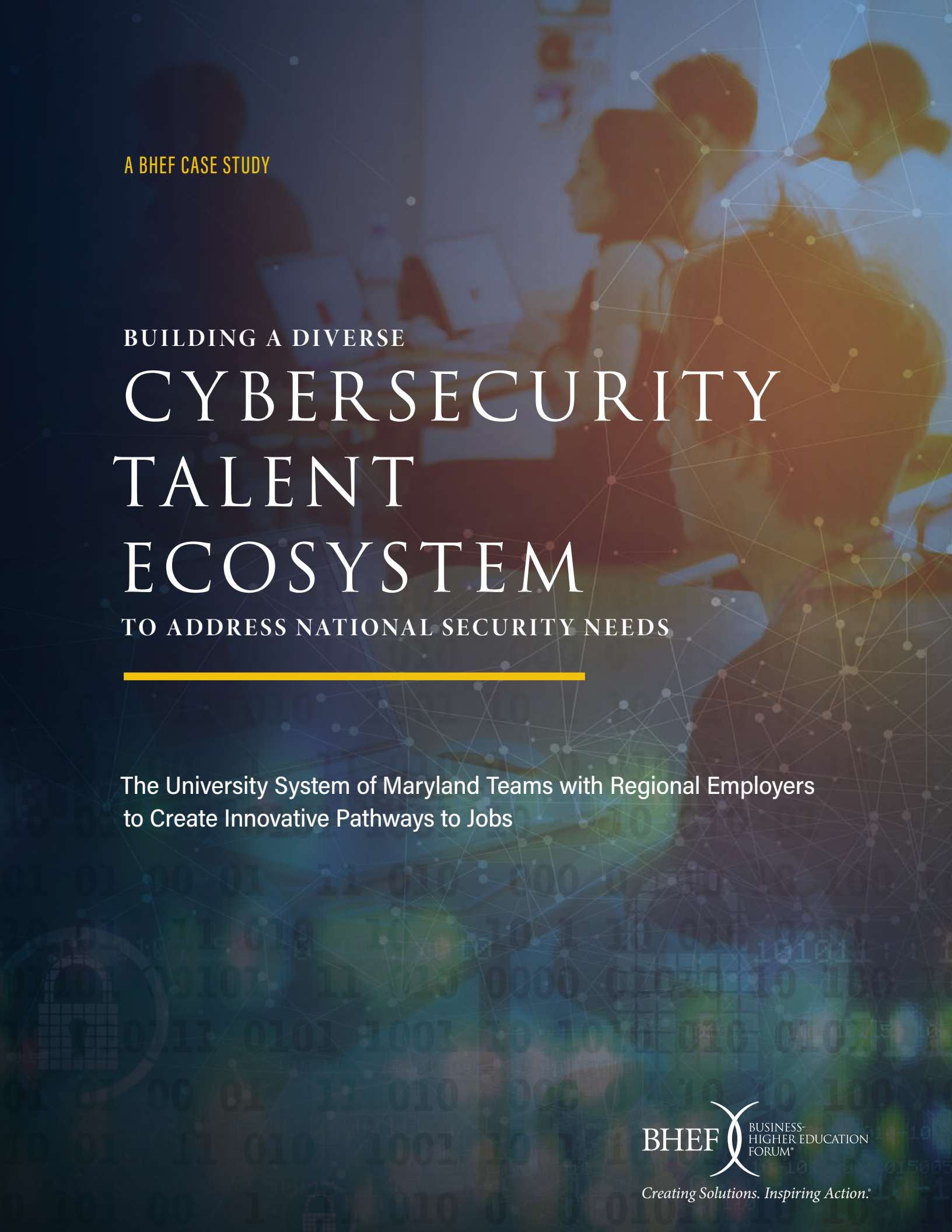


A BHEF CASE STUDY

BUILDING A DIVERSE CYBERSECURITY TALENT ECOSYSTEM TO ADDRESS NATIONAL SECURITY NEEDS

The University System of Maryland Teams with Regional Employers to Create Innovative Pathways to Jobs

BHEF BUSINESS-HIGHER EDUCATION FORUM®

Creating Solutions. Inspiring Action.®

ABOUT BHEF

The Business-Higher Education Forum (BHEF) is the nation's oldest membership organization of Fortune 500 CEOs, college and university presidents, and other leaders dedicated to the creation of a highly skilled future workforce. BHEF members collaborate and form strategic partnerships to build new undergraduate pathways; improve alignment between higher education and the workforce; and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

TABLE OF CONTENTS

INTRODUCTION

AS THE NATION'S OLDEST membership organization of Fortune 500 CEOs, college and university presidents, and other leaders, the Business-Higher Education Forum (BHEF) and its members form strategic partnerships to build new undergraduate pathways, improve alignment between higher education and the workforce, and produce a diverse, highly skilled talent pool to meet demand in emerging fields.

Through the collaboration of its members, BHEF launched the National Higher Education and Workforce Initiative (HEWI) to support business-higher education partnerships that co-design community college and university pathways to careers in fields that are critical to innovation and national security, as well as maximize work-based learning to increase transfers, degree attainment, and connections to living-wage jobs.

This case study examines how BHEF member, the University System of Maryland (USM), collaborated with businesses and government agencies to develop cybersecurity pathways on multiple campuses to build a diverse regional cybersecurity talent ecosystem that can address national security needs. This case study also provides recommendations for stakeholders in government, business, and higher education on developing an ecosystem for cybersecurity skills needs—or one that can serve as a model for other fields.

This case study builds upon BHEF's work to create new undergraduate pathways in high-skill, high-demand fields. As part of HEWI, BHEF received a $400,000 grant from the Alfred P. Sloan Foundation in 2012 to work with USM and the Northrop Grumman Corporation on the development of undergraduate pathways in cybersecurity. In partnership with BHEF, USM pursued a coordinated, system-level effort to create new cybersecurity pathways that would attract diverse students, engage them in cutting-edge learning experiences, and encourage them to build their careers in the region.

This case study examines how BHEF member, the University System of Maryland, collaborated with businesses and government agencies to develop cybersecurity pathways on multiple campuses to build a diverse regional cybersecurity talent ecosystem that can address national security needs.

SYSTEM OVERVIEW

USM OFFERS A VARIETY OF ACADEMIC PROGRAMS that prepare students for careers in cybersecurity. These programs include bachelor's degrees on residential campuses, online programs that largely serve working adults, and competency-based certification programs. All were designed in partnership with government agencies and companies that employ cybersecurity professionals to ensure that the graduates have the skills and knowledge that employers demand. The programs combine coursework and hands-on learning experiences to prepare students to meet the cybersecurity challenges of the 21st century.

> "USM's strategic partnership with BHEF has strengthened the linkages between industry and higher education, driving innovative undergraduate programs to help meet critical workforce needs while engaging the best, brightest and most diverse array of students. **Together, USM and BHEF are helping to position Maryland at the epicenter of cybersecurity.**"
>
> **ROBERT L. CARET** / CHANCELLOR / UNIVERSITY SYSTEM OF MARYLAND

CYBERSECURITY JOB METRICS

209,000

CYBERSECURITY POSITIONS IN THE U.S. WENT UNFILLED IN 2015

84%

OF CYBERSECURITY JOB POSTINGS IN THE WASHINGTON, D.C., METRO AREA REQUIRE AT LEAST A BACHELOR'S DEGREE AND AT LEAST THREE YEARS OF RELEVANT WORK EXPERIENCE

40,000

JOB OPENINGS FOR CYBERSECURITY-RELATED POSITIONS POSTED IN THE WASHINGTON, D.C. METRO AREA IN 2017

THE CHALLENGE

USM is surrounded by a network of businesses and government agencies that urgently need access to a larger pool of highly skilled cybersecurity professionals.

DENIAL OF SERVICE, RANSOMWARE, data loss, and full-on cyberattacks have proliferated in recent years, affecting federal and state governments, credit-rating agencies, and other companies. Approximately 209,000 cybersecurity positions in the U.S. went unfilled in 2015, and 71 percent of employers have incurred damages because of that deficit. The growth of cybersecurity talent is limited by a lack of diversity—for example, according to annual surveys of 18 to 26-year olds conducted by Raytheon, women are less interested and less informed about cybersecurity career opportunities than men.

USM is surrounded by a network of businesses and government agencies that urgently need access to a larger pool of highly skilled cybersecurity professionals. In 2017, employers in the Washington, D.C., metro area posted more than 40,000 job openings for cybersecurity-related positions, and this number is expected to grow. According to survey data, employers in the region consider it particularly difficult to find qualified candidates for cybersecurity jobs compared to other roles within their organizations. This challenge is partly rooted in the level of education and experience that are typically listed as minimum qualifications for cybersecurity positions in the region: 84 percent of cybersecurity job postings in the Washington, D.C., metro area require at least a bachelor's degree, and 84 percent require at least three years of relevant work experience. Few recent college graduates can claim that much work experience, and so this combination of required qualifications effectively drives cybersecurity talent out of the region to seek opportunities elsewhere, exacerbating the region's need for cybersecurity professionals.

Meeting demand at this scale will be impossible unless many more people—including women and members of other underrepresented groups—pursue careers in cybersecurity, but pathways into this relatively young field are not yet clearly defined. This picture is further complicated by rapid evolution in the field: How can institutions of higher education develop academic programs that keep pace with advances in cybersecurity challenges and practices?

THE SOLUTION

Create new undergraduate pathways into cybersecurity that attract students with diverse backgrounds and interests, engage them in meaningful learning experiences that reflect the cutting edge of the field, and encourage them to stay in the region to build their careers.

MARYLAND IS THE EPICENTER of national cybersecurity, and USM's efforts to build a cybersecurity talent ecosystem can serve as a model for response. USM reframed this challenge as an opportunity to create new undergraduate pathways into cybersecurity that attract students with diverse backgrounds and interests, engage them in meaningful learning experiences that reflect the cutting edge of the field, and encourage them to stay in the region to build their careers.

USM's program grew out a series of planning activities, studies, and regional workforce assessments highlighting the need to sharply increase student graduation rates in STEM fields, particularly among women and underrepresented minorities, to meet the state's rapidly expanding STEM workforce needs, notably in information technology and cybersecurity. In 2009, the Maryland STEM Task Force, co-chaired by Brit Kirwan, USM chancellor, and June Streckfus, executive director of the Maryland Business Roundtable for Education, submitted its final recommendations to Governor Martin O'Malley in the report, *Investing in STEM to Secure Maryland's Future*.

The report noted an anticipated surge in STEM-related jobs in the Maryland region, particularly in critical areas such as cybersecurity, and called for greater collaboration between industry and USM to produce 40 percent more STEM graduates in the state by 2015 to fill these jobs. This recommendation echoed USM's own 2010 strategic plan, which noted that its annual production of approximately 4,000 STEM graduates (including STEM teachers) was falling considerably short of filling the region's 6,000 STEM openings each year. The plan called for greater collaboration between business and the

RECENT STATE EFFORTS IN CYBERSECURITY

Governor Larry Hogan has also identified cyber as a major part of Maryland's economic and workforce development strategy. For example, in October 2017 he signed an executive order directing the Task Force on Cybersecurity and Information Technology, as part of the Governor's Workforce Development Board, to **study opportunities to grow the sector of Maryland's economy associated with computer science and the information technology industry**. The task force will focus on developing pathways that meet identified workforce needs in computing fields, addressing the challenges facing Maryland's talent ecosystem, and encouraging employer partners to invest in Maryland's IT workforce. In addition, the task force has been asked to identify innovative, sustainable ways to promote gender and minority equity in the STEM and IT workforce.

THE SOLUTION

P-20 system in the state, as well as for increased efforts to align education with workforce needs.

In 2010, Governor O'Malley designated cyber as the state's primary workforce focus. That same year, the Governor's Workforce Investment Board projected that the greatest job growth would be in high-skill occupations, in particular network systems/data communication, computer software engineering, and systems administration. Following on these efforts, Chancellor Kirwan commissioned a Cybersecurity Task Force in 2010 that brought together university leaders and major employers of cybersecurity talent from nearby government agencies and businesses. Its 2011 report detailed the region's need for highly skilled workers in cybersecurity, provided an inventory of USM resources available for cybersecurity education and research, and explored opportunities for partnerships among USM institutions and business and government stakeholders to produce the cybersecurity workforce of the future. USM's efforts were reinforced in 2012 when the Alfred P. Sloan Foundation awarded the BHEF a $400,000 grant to work with USM and the Northrop Grumman Corporation on the development of undergraduate pathways in cybersecurity.

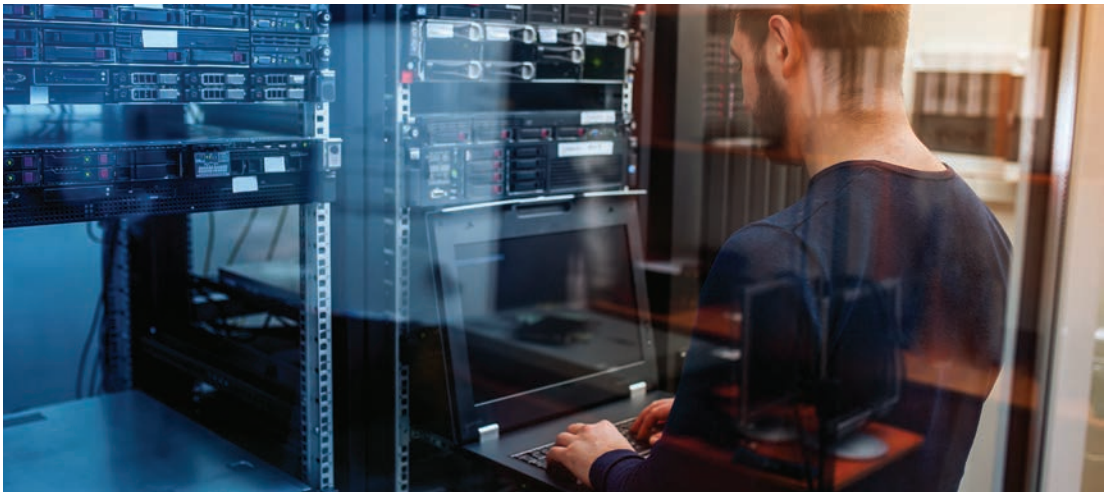
While USM has pursued a coordinated system-level effort, its leadership also saw strength and potential in the diversity of its universities, which have unique missions, resources, and student populations. Aiming not only to grow but also to diversify the region's cybersecurity talent ecosystem, there was a strategic advantage in having each university develop unique pathways, consistent with their existing institutional strengths. At the same time, the universities' approaches had important features in common, including an unwavering focus on quality. The five universities profiled in this case study are all designated as Centers of Academic Excellence in Information Assurance Research by the National Security Agency (NSA) and the Department of Homeland Security. USM and its campuses have also collaborated extensively with local companies

> "Cybersecurity is clearly linked to both our economic vitality and our national security, and at its core lies some of our nation's best and brightest talent. Together with the University System of Maryland we are partnering in a unique way to grow and train a diverse cyber workforce through the Advanced Cybersecurity Experience for Students at College Park and Cyber Scholars Program at UMBC. These hands-on programs are working and will ensure that we are providing already talented students with the right cybersecurity skills to make a real impact in the years to come."
>
> **WES BUSH** / CHAIRMAN AND CHIEF EXECUTIVE OFFICER / NORTHROP GRUMMAN CORPORATION

and government agencies to develop academic programs that align with evolving workforce needs, to provide students with work-based learning experiences, and to connect students to professional networks and opportunities that persuade them to stay in the region after graduation.

One example of a signature system-level effort took place in 2014. USM partnered with the MITRE Corporation, which operates the first Federally Funded Research and Development Center (FFRDC) dedicated to cybersecurity. The National Cybersecurity FFRDC (NCF), sponsored by the National Cybersecurity Center of Excellence, works with industry to identify concerns related to cybersecurity and then documents reference implementations as National Institute of Standards and Technology Special Publications, which it shares freely in the public interest. Through this partnership, MITRE has gained access to USM's cybersecurity expertise, and it engages faculty in its efforts to understand and solve the problems raised by industry. To foster collaboration, USM contracted a new position—cybersecurity academic innovation officer—that matches faculty expertise to NCF projects. NCF also leverages the expertise of USM's students. Before publicly sharing a reference implementation to a cybersecurity problem, the FFRDC undertakes rigorous assessment to ensure its applicability. This hands-on work is ideal for student interns, who directly contribute to advances in the field through these projects. MITRE has brought on numerous interns since the NSF was established, and it plans to grow its internship program in coming years. In multiple cases, these interns eventually transitioned to full time employment.

In addition to signature system-level efforts, each campus leverages its own strengths when addressing the cyber challenge, contributing uniquely to the system-wide response. The following pages detail these efforts on campuses across Maryland.



UNIVERSITY OF MARYLAND, COLLEGE PARK

THE UNIVERSITY OF MARYLAND, COLLEGE PARK (UMD) is the system's flagship research university. UMD attracts many of the region's brightest students, in part because its Honors College offers unique interdisciplinary programs for undergraduates. Building on the success of those programs, the university partnered with Northrop Grumman to develop the nation's first honors program in cybersecurity as a pathway for recruiting top talent into the field. With the support of a $1.1 million gift from the Northrop Grumman Foundation, the Advanced Cybersecurity Experience for Students (ACES) was launched in 2012.

ACES comprises two linked programs: a two-year living-learning program that leads to an Honors College citation on student transcripts and a two-year minor. The programs serve distinct purposes but share several key features. The curricula of both programs assume a multidisciplinary approach to cybersecurity, drawing not only from computer science and engineering but also from economics, public policy, criminology, and other fields. This exposure to both the technical and nontechnical aspects of cybersecurity provides students with a broad perspective on the field. Students in ACES can also choose any major, with the understanding that cybersecurity challenges will be solved most effectively by teams with diverse backgrounds. Both programs also emphasize hands-on learning experiences, requiring students to participate in experiential learning through internships, research, or group projects focused on addressing real-world challenges.

The ACES living-learning program is designed to cultivate a scholarly community during students' first two years at UMD. Students live together in an honors residence hall that is also home to a cybersecurity laboratory funded by Northrop Grumman. This environment encourages students to learn collaboratively and to develop supportive relationships. Students also take classes as a cohort, and their courses facilitate peer learning. For example, students who complete internships take a reflections course in which they share and compare their experiences working for different companies or government

Women of ACES at the University of Maryland

agencies. Through these conversations, students gain insights about meaningful variation in organizational cultures and operations and about the type of work environment they should seek out when they enter the job market.

The ACES minor offers advanced cybersecurity coursework to upper-level undergraduates, with a continued focus on interdisciplinary and experiential learning. Many students in the minor also participated in the living-learning program, and they can stay connected by serving as peer mentors and tutors to students in the living-learning program.

Northrop Grumman has played a vital role in developing and implementing ACES, not only by generously funding the program—the company recently renewed its commitment with a $2.76 million gift—but also by advising on curriculum design and encouraging employee involvement in ACES by serving as adjunct faculty and mentors. ACES also has a unique partnership with the NSA, which provides several instructors for

ADVANCED CYBERSECURITY EXPERIENCE FOR STUDENTS (ACES)

75

STUDENTS JOIN THE ACES LIVING-LEARNING PROGRAM EACH YEAR

370+

STUDENTS HAVE PARTICIPATED IN THE LIVING-LEARNING PROGRAM SINCE 2013

50

JOIN THE ACES MINOR EACH YEAR

90

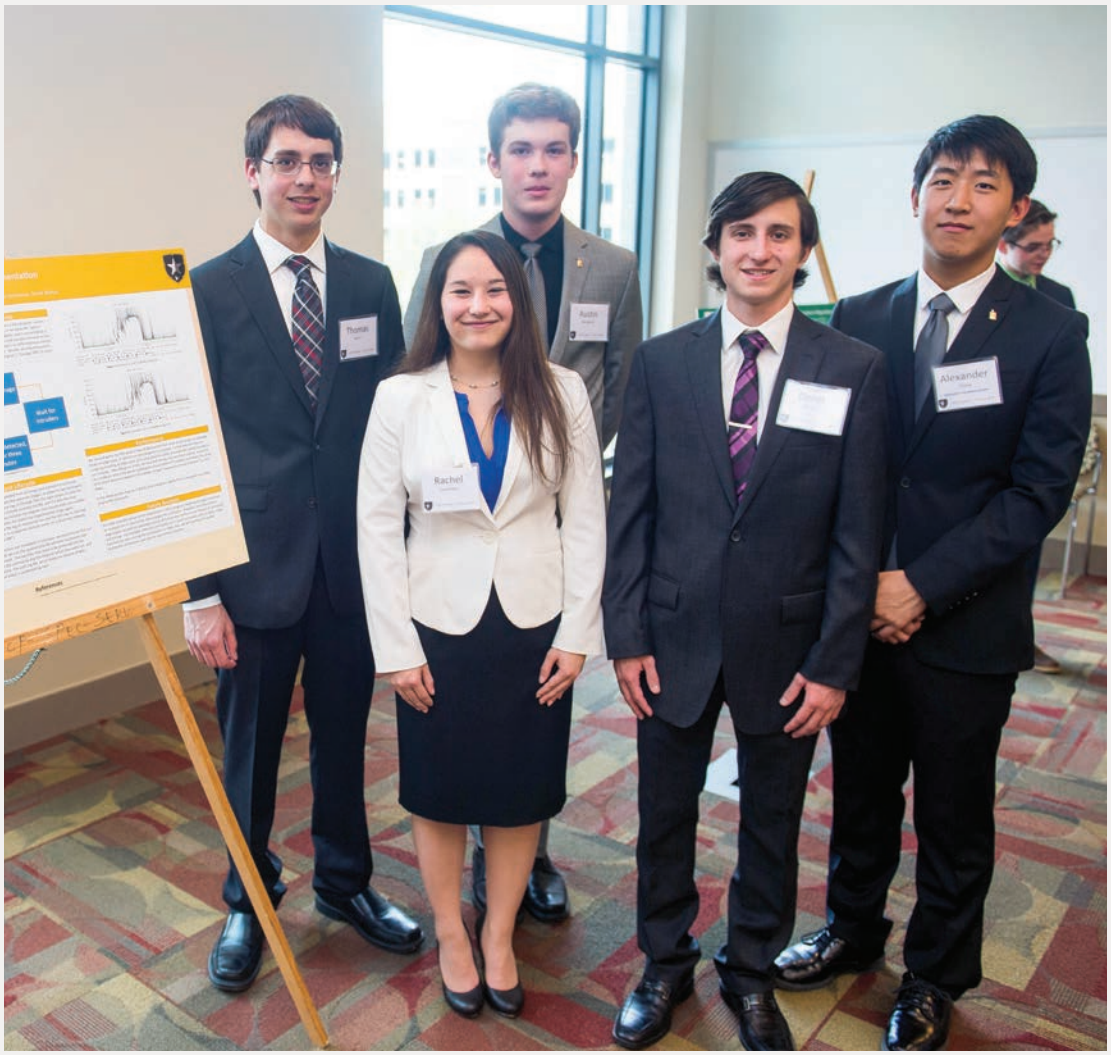
STUDENTS HAVE PARTICIPATED IN THE MINOR SINCE 2015

33%

OF PARTICIPANTS IN THE ACES LIVING-LEARNING PROGRAM ARE WOMEN

three-credit courses, mentors, and uncleared internships for ACES students. ACES has formed additional partnerships with Leidos, Talos, Parsons, and other nearby companies and government agencies, creating a vibrant network of expertise and opportunities. Partners provide feedback about the ACES' curriculum, host internships, and participate in networking events with students. Through their ongoing involvement with the program, partners build relationships with talented students and often recruit them into full-time positions when they graduate.

Each year, about 75 students join the ACES living-learning program and about 50 join the ACES minor. Altogether, more than 370 students have participated in the living-learning program since 2013, and about 90 have participated in the minor since 2015. Thirty-three percent of participants in the ACES living-learning program are women, in contrast to 20 percent and 15 percent in the computer science and computer engineering programs, respectively. Moving forward, UMD hopes to further grow and diversify enrollment in the ACES minor both by attracting more students majoring in fields outside of computer



ACES students presenting their research

science and engineering—such as journalism and psychology—and by recruiting more transfer students. In addition, UMD recently launched the Maryland Global Initiative for Cybersecurity, which will help coordinate and develop the university's government and industry partnerships, with the goal of establishing UMD as a leader in cybersecurity education.

UMD is also home to the Maryland Cybersecurity Center (MC2) an interdisciplinary research center that combines technical and nontechnical approaches to cybersecurity, ranging from economics to policy to computer science and engineering to criminology. Faculty affiliated with MC2 provides a breadth of research and technical exposure to students at UMD interested in the diverse issues associated with cybersecurity.

In addition, the growing entrepreneurial and innovation ecosystem in College Park provides applied and novel learning experiences for students. Cybersecurity companies are establishing offices in the newly rebranded Discovery District, and faculty-led start-ups in cybersecurity are new resources for UMD graduate and undergraduates to have experiential learning.

STUDENT PROFILE / **CHRISTIAN JOHNSON**

"I was one of those kids who applied to every college under the sky," said Christian Johnson a recent alumnus of the University of Maryland, College Park. He was looking for a school with a highly rated computer science program and proximity to professional resources, all of which UMD fit. "But ACES was what actually sealed the deal for me," he said. He saw potential in joining a program in its infancy that was directly related to computer science but would also allow him to expand his knowledge and interests at the same time.

Johnson joined ACES in Fall 2013 and took advantage of all the opportunities that the program offered. In his freshman year, he was asked to be the undergraduate representative for a team compiled by the university president to address security issues. He won many awards throughout his time as a student as well, including the ManTech Cyber Security Scholarship his junior year.

He worked hard to get from ACES all that he wanted. "When I came in as a freshman," he said, "it didn't take more than two weeks for me to know that I was in it to do it for four years." He made that wish a reality as the first student board president. Johnson worked with ACES staff to create the ACES minor.

Beginning in early 2015, Johnson began working as an intern with Northrop Grumman, where he stayed for two years. He worked full time over breaks and stayed on throughout the semester part-time as a cyber software engineer. That experience and his education in computer science and cyber security led him to his current position.

Now Johnson works at Amazon Web Services as a systems development engineer, also known as an operational excellence engineer. He began working part-time the spring before his graduation, beginning full-time once he earned his degree. "Both the computer science education and the cybersecurity education are both extremely valuable in my job," Johnson said.

Johnson cites ACES' strong corporate partnerships as one of the main reasons he is where he is now. "The level of corporate engagement is a unique aspect of the program," he said. **"ACES is really instrumental in providing career development and exposure. In general, ACES provided a level of exposure to the professional world that I have not seen out of almost any program at Maryland before."**

He is looking forward to continuing his career at Amazon Web Services and seeing more ACES students reach success in their academic and professional lives. He said, "I'm very excited going forward seeing the strengthened relationship between the alumni community and the incoming students."

UNIVERSITY OF MARYLAND, BALTIMORE COUNTY

THE UNIVERSITY OF MARYLAND, BALTIMORE COUNTY (UMBC) is a research university with a reputation for inclusive excellence. UMBC's Meyerhoff Scholars program is viewed as a national model for increasing diversity in STEM fields, and the university drew on lessons learned from that model when it launched the Cyber Scholars program in 2013. The program, initially supported by a $1 million grant from the Northrop Grumman Foundation, focuses on preparing women and members of other underrepresented groups to lead the next generation of cybersecurity professionals.

This year, 70 percent of UMBC's Cyber Scholars are women, and 30 percent are underrepresented minorities. The program provides them with a broad set of opportunities and support that is designed to attract and retain talented students from diverse backgrounds. Scholars—who can major in computer engineering, computer science, or information systems—are awarded scholarships of up to $15,000 per year. They are exposed to the leading edge of cybersecurity through a curriculum informed by the program's industry and government partners, as well as through required internships and research experiences. One of the program's signatures is Cyber Practicum, a weekly course featuring hands-on activities and talks by cybersecurity experts from such partner organizations as Northrop Grumman, T. Rowe Price, NSA, the Federal Bureau of Investigation, and the Johns Hopkins Applied Physics Lab. Scholars have additional opportunities to interact with partner organizations through networking events and site visits. Scholars are also paired with faculty and industry mentors, and they meet at least monthly with program staff for one-on-one coaching. To foster an environment of peer learning and support, Cyber Scholars live on the same floor of a residence hall and take courses together. This living-learning community is intended to help students from underrepresented populations feel a sense of belonging in cybersecurity.

In response to growing student interest in the Cyber Scholars program, UMBC

UMBC Cyber Scholars and Affiliates enjoyed a talk on campus from Northrop Grumman Corporation chairman and CEO, Wes Bush

created two new levels of participation. Cyber Associates fully participate in the program but do not receive scholarship support, and Cyber Affiliates are invited to attend events when space is available. Cyber Scholars is a high-touch, resource-intensive program that would be challenging to scale without additional funding. The Associates and Affiliates approach has enabled UMBC to significantly expand access to program elements without dramatically increasing the budget. Last year, the program served more than 100 Cyber Affiliates.

UMBC's commitment to building a diverse cybersecurity workforce extends beyond Cyber Scholars, who earn a traditional four-year degree. The university also offers alternative pathways into the profession, including a master's of professional studies in cybersecurity that primarily serves working adults. In addition, UMBC's training center offers Cyber Academy, an intensive noncredit program that includes competency-based

CYBER SCHOLARS PROGRAM

70%

OF CYBER SCHOLARS ARE WOMEN

30%

OF CYBER SCHOLARS ARE UNDERREPRESENTED MINORITIES

CYBER INCUBATOR

40+

COMPANIES CURRENTLY HOSTED BY THE INCUBATOR

60%

OF COMPANIES OWNED BY VETERANS, WOMEN, OR MEMBERS OF UNDERREPRESENTED GROUPS

assessments, five professional certifications, a capstone experience, and internship opportunities. The Cyber Academy attracts many veterans and active duty military members, as well as other adult learners seeking to change careers. In all cases, UMBC's cybersecurity programs were developed in close partnership with government agencies and companies to ensure that graduates are effectively prepared to enter the workforce.

UMBC is also home to a cyber incubator that provides space, professional services, and networking opportunities for cybersecurity start-ups. The cyber incubator is supported in part by Baltimore County and the Maryland Department of Commerce, which are interested in start-ups' potential for creating jobs. The incubator currently hosts more than 40 companies, and over 60 percent of them are owned by veterans, women, or members of other underrepresented groups. Many start-ups are drawn to UMBC because of the available talent pool: Incubator companies employ about 150 UMBC students as interns and about 150 alumni as full-time employees.

UMBC Cyber Scholars help high school girls learn about cybersecurity basics through the annual Cyber 101 overnight program

Northrop Grumman sponsors several of these companies through Cync, a highly competitive scholarship program that covers space and services provided by the cyber incubator. Cync companies are selected because they are working on cybersecurity solutions of particular interest to Northrop Grumman, which also provides in-kind support, including technical expertise and business development advice. The cyber incubator recently launched another program, the iCyberCenter, for international cybersecurity companies interested in entering the U.S. market. The program includes two components: executive training that introduces the complex issues companies may face in their transition to the U.S. and an incubator program that includes specialized services to meet the needs of international companies. UMBC also views this program as an opportunity to persuade companies to locate their U.S. headquarters in Maryland and to hire from the local talent pool.

STUDENT PROFILE / **LAUREN MAZZOLI**

As a child, Lauren Mazzoli loved science labs, solving math problems at the board, and even leading group projects. She might not have been the best in her class, but she was always eager to learn. However, that all changed once she reached middle school. The adults in her life started telling her that it was okay to get a B in science since "girls don't really need to know that stuff anyway," and that she shouldn't lead her group projects because she was "too bossy." Without realizing it, Lauren slowly lost her confidence and interest in science. Years later, Lauren visited UMBC for a campus tour, and she found a place where she felt safe being herself. The mix of students actively engaging in labs and the professors supporting every student were two of the main reasons why Lauren transferred to UMBC and would ultimately find her passion for computer science and mathematics.

Lauren was one of nine students who comprised the first cohort of Cyber Scholars at UMBC, helping to shape the program into what it has become now, five years later. As a student, **Lauren was a computer science and math double major and worked approximately 20 hours per week in the IT security department of the division of information technology on campus, getting hands-on cybersecurity experience.** She maintained an impressive GPA and still found time to serve as a mentor to younger Scholars in the program. She also had the opportunity to build an important mentoring relationship with her industry mentor, Donna Dodson, chief cybersecurity advisor at NIST. Having a senior cybersecurity professional as a mentor and participating in the majority-women communities provided by the Cyber Scholars and Center for Women in Technology at UMBC helped Lauren to maintain her confidence as she advanced through her degree program and completed an internship at the Department of Defense.

After earning her bachelor's degree in May 2015, Lauren decided to accept an offer from Northrop Grumman as a cyber software engineer and pursue her master's degree in computer science part-time at UMBC. She has earned several internal awards at Northrop Grumman as well as the Rising Star awards through both the Women's Society of Cyberjutsu and the UMBC Alumni Association since her graduation. She earned her master's degree in May 2017 and has recently become a part of Northrop's competitive Future Technical Leaders program. She has also remained highly engaged with the Cyber Scholars Program, serving as a liaison between Northrop Grumman and the university to plan technical talks, hiring events, cyber competitions, and more for the students in the program.

UNIVERSITY EFFORTS

UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE

THE UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE (UMUC) is dedicated to serving adult learners. To strengthen and diversify the cybersecurity talent ecosystem, UMUC focuses on developing high-quality online programs to enable working adults to transition into the field. Building on its pre-existing information assurance programs, the university convened an advisory board composed of senior executives from industry and experts with high-level government experience to help design a cybersecurity curriculum aligned with employer needs. To translate that curriculum into effective online programs, the university adopted a master-course model—developing a set of online courses prepopulated with content and assignments—to ensure high quality across courses and to enable faculty to focus on contributing their unique expertise and experience, rather than building their courses from scratch. The university also invested upwards of $7 million to develop its initial cybersecurity offerings, including a new graduate department, full-time faculty, and the technical infrastructure to permit students to exercise their newly learned skills in a virtual environment.

UMUC cyber student team (Padawans) at a competition

UMUC launched its first online degree programs in cybersecurity in 2010. Its current inventory includes master's degrees in information assurance, cybersecurity management and policy, cybersecurity technology, and digital forensics and cyber investigation; and bachelor's degrees in management and policy, computer networks and cybersecurity, and software development and security. Offering these programs online has enabled UMUC to reach students across Maryland and the U.S. and active-duty members overseas—and to do so on an impressive scale. UMUC has created numerous pathways into its programs through articulation agreements with community colleges, not only in Maryland but also in Virginia, North Carolina, Florida, Arizona, and Hawaii. By broadening access, UMUC has attracted a highly diverse student population to its cybersecurity programs. In fall 2016, UMUC's online cybersecurity programs enrolled more than 10,000 students, including 4,100 Maryland residents.

10,000
STUDENTS ENROLLED IN ONLINE CYBERSECURITY PROGRAMS

4,100
STUDENTS ARE MARYLAND RESIDENTS

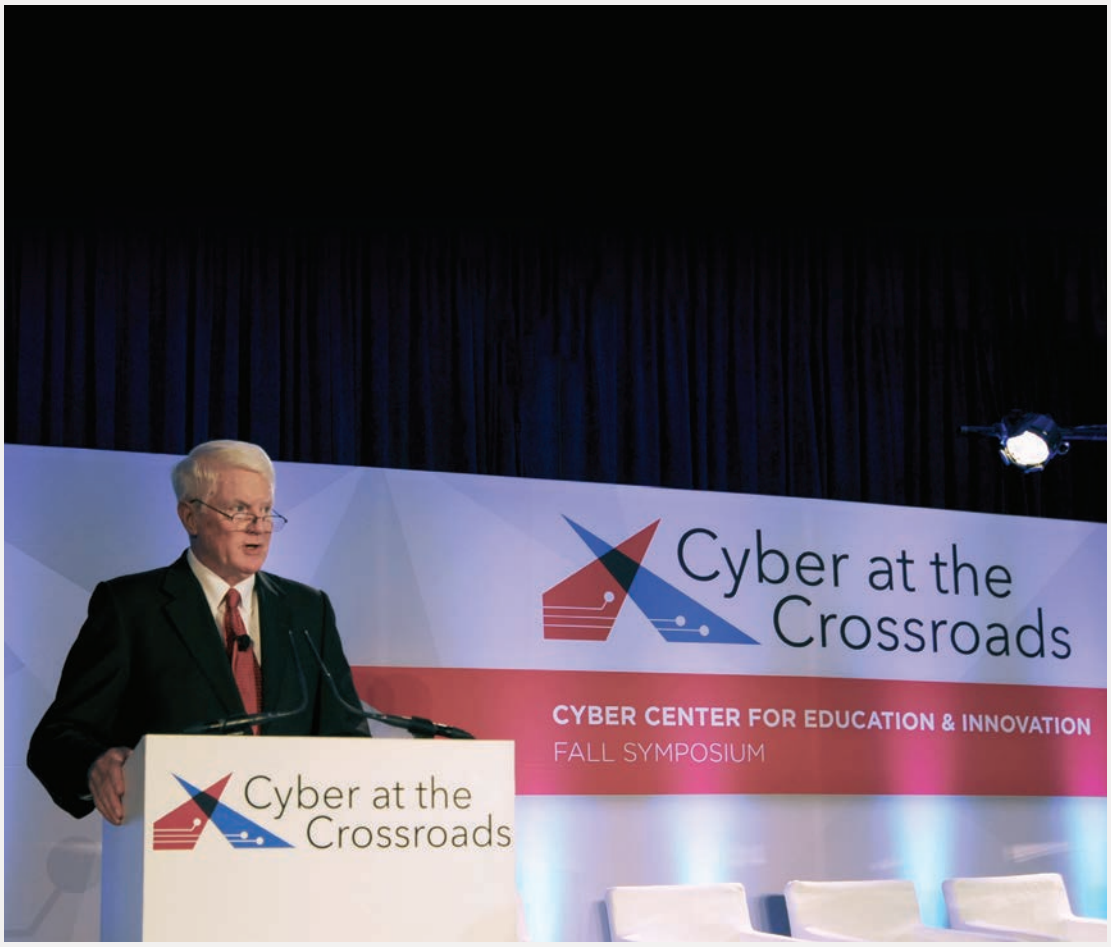
NATIONAL CENTER OF ACADEMIC EXCELLENCE IN INFORMATION ASSURANCE AND CYBER DEFENSE EDUCATION

NATIONAL CENTER OF DIGITAL FORENSICS ACADEMIC EXCELLENCE

STAFFING AGENCY FOR THE MARYLAND CYBERSECURITY COUNCIL

Part of the university's strategy to ensure the currency of its programs and the job readiness of its graduates is to embed itself within the larger state and national cybersecurity ecosystem. These linkages involve program administrators, cybersecurity faculty, and students. Specifically:

- **UMUC participates in periodic external reviews of its cybersecurity curricula by national bodies.** It is designated as a National Center of Academic Excellence in Information Assurance and Cyber Defense Education by the National Security Agency and the U.S. Department of Homeland Security, and as a National Center of Digital Forensics Academic Excellence by the Defense Cyber Crime Center Academic Cyber Curriculum Alliance.
- **The university supports student and faculty opportunities to participate in collegiate and industry-sponsored cybersecurity competitions.** Since 2012, UMUC's team (Cyber Padawans) has competed in nearly 20 state, regional, national, and international events, consistently winning awards.



UMUC is the lead educational programming partner of the Cyber Center for Education and Innovation (CCEI)—Home of the National Cryptologic Museum (NCM). The Center is a private-public joint initiative between the National Cryptologic Museum Foundation and the National Security Agency. Above: Lt. General John Campbell (USAF, Ret.) senior advisor to CCEI, introduces Cyber at the Crossroads, a one-day symposium in October 2017 organized by UMUC and CCEI.

- **UMUC is the designated staffing agency for the Maryland Cybersecurity Council, a statutory entity chaired by the state's attorney general.** This role involves the university in coordinating policy research in cybersecurity for the council and directly connects the university with a broad range of cybersecurity issues at the state level.

- **UMUC participates in cybersecurity workforce development initiatives beyond the classroom.** On behalf of USM, UMUC is the lead partner to develop the educational and training program of the Cyber Center for Education and Innovation (CCEI). A public-private partnership between the National Cryptologic Museum Foundation and the NSA, CCEI's mission is to create an East Coast cybersecurity nexus to integrate industry, government, and academic stakeholder resources, to advance cybersecurity training and education at every level, and to build a facility both to replace the current home of the National Cryptologic Museum and to anchor CCEI's education and training activities. The State of Maryland has appropriated funds to support this initiative.

STUDENT PROFILE / CHIMERE MURRILL

Chimere L. Murrill was raised in Petersburg, Virginia, a small, rural city south of Richmond. The child of a single mother of two, Chimere was encouraged by her mother to excel academically because she understood the importance of education. In addition, Chimere's natural curiosity for computers and technology would propel her to sacrifice the security of small town life to venture into a wider world of opportunities.

In her early education, Chimere was placed in honors classes and her ambition was to attend university. Winning a partial track-and-field scholarship, Chimere entered Morgan State University, the largest historically black university in Maryland. There she eventually earned her bachelor's degree in computer information science and systems.

At Morgan, Chimere joined the campus chapter of the Association of Information Technology Professionals and was elected vice president of her chapter. In 2004, she was given an internship at the global IT division of Black & Decker headquarters in Towson, Maryland. The internship continued for two years while she attended school full time and volunteered in the campus computer labs. Upon graduation, Chimere landed a position with IBM as a global technical consultant, where she acquired a security clearance.

Encouraged by a mentor, Chimere sought employment that would expose her to the most challenging cybersecurity work opportunities. Since then, she has been employed by VikTeck, a firm in Hanover, Maryland, providing cybersecurity and information assurance services to the Department of Defense. In this role, **Chimere has worked on some of the highest-level security and intelligence missions protecting the U.S. from advanced persistent threats. Chimere honed her cyber skill set in the classroom as well as on the job.** She completed her master's degree in cybersecurity at the University of Maryland University College in 2016.

Chimere works with disadvantaged youth to teach them the importance of setting personal goals to achieving success in life. She is also seeking resources that would support her efforts to develop a cyber program to introduce these youth to cybersecurity, network, and other technical concepts starting in eighth grade.

UNIVERSITY EFFORTS

BOWIE STATE UNIVERSITY

BOWIE STATE UNIVERSITY is a historically black university (HBCU) that places a special emphasis on science and technology. The university belongs to a consortium of 13 HBCUs, two national labs, and a public school district that, in 2015, was awarded a $25 million grant by the Department of Energy to develop pathways that increase participation of underrepresented minorities in the cybersecurity workforce. Bowie State has used its share of the grant—$1.2 million over five years—to expand its cybersecurity curriculum and increase its outreach efforts.

Bowie State offers two bachelor's programs that allow students to focus on cybersecurity: the cybersecurity track in the computer science major and the computer and network security track in the computer technology major. The university has developed five cybersecurity courses, based on recommendations from an advisory board that includes experts from industry and government. In addition to creating these clear pathways into the cybersecurity profession, Bowie State has established new opportunities for experiential learning. The university built laboratories that enable students to practice applying their cyber problem-solving skills in a simulated work environment. Many students also participate in internships hosted by Bowie State's industry and government partners, including BAE Systems, the Office of Naval Research, and the National Institute of Standards and Technology.

Graduates of Bowie State's cybersecurity programs are in demand, and many students are offered jobs a year before they graduate. Student interest in these programs is high, so the university plans to offer additional sections of its cybersecurity courses in the coming year. Bowie State also plans to add a capstone course to its cybersecurity programs and is working with the Department of Energy to share its curriculum model with other members of the consortium.

In addition, Bowie State students frequently participate in hackathons, and they have a record of success: Last year, a team of African-American women placed second in a national competition.

Bowie State's Forensic Technology Cyber Squad

To attract students from diverse backgrounds into the field of cybersecurity, Bowie State engages in extensive outreach efforts. Its programs include workshops for African-American middle and high school girls and a five-week summer program for Baltimore youth. These programs feature hands-on learning activities designed to boost interest in cybersecurity, and they are led by African-American faculty and students from Bowie State. In the last three years, about 1,000 young people have participated in the university's outreach programs. Those efforts are beginning to bear fruit, as six participants from the summer program recently entered Bowie State's cybersecurity programs, taking their next steps toward careers in the field.

2

BACHELOR'S PROGRAMS THAT ALLOW STUDENTS TO FOCUS ON CYBERSECURITY: THE CYBERSECURITY TRACK IN THE COMPUTER SCIENCE MAJOR AND THE COMPUTER AND NETWORK SECURITY TRACK IN THE COMPUTER TECHNOLOGY MAJOR

5

CYBERSECURITY COURSES

2ND

PLACE FOR A TEAM OF AFRICAN-AMERICAN WOMEN IN A NATIONAL HACKATHON COMPETITION

1,000

YOUNG PEOPLE HAVE PARTICIPATED IN THE UNIVERSITY'S OUTREACH PROGRAMS

Professor Lethia Jackson works with students in Bowie State's Forensic Technology Cyber Squad on the SWAMP program

STUDENT PROFILE / **CARROLL REED III**

Carroll Reed III, a 2017 Bowie State University graduate, always knew he wanted to study computer science. As a college freshman, he arrived on campus with technology experience gained through high school computer programming classes and an engineering program.

It wasn't until he started working with the university's signature STEM career and college pathways program, Education Innovation Initiative (EI2), that he developed an interest in cybersecurity. "Cybersecurity is a field with so many jobs available, but so few Americans have the skills needed to work in those positions," he said.

As it turns out, Reed had come to Bowie State at the perfect time. He joined a newly formed student group called the Forensic Technology Information Cyber Squad, led by computer science professor Lethia Jackson. The students have played a major role in Bowie State's partnership with 12 other historically black colleges and universities, which received $25 million over five years to build programs for minorities to study cybersecurity from middle school through college.

Reed and his fellow Cyber Squad members collaborated with a Wisconsin-based national cybersecurity facility called the Morgridge Institute for Research to test the Software Assurance Marketplace (SWAMP) before it launched. Through his research with this open-sourced, high-performance computing tool, Reed became an expert at writing code and detecting code weaknesses. "We created the user manual and protocols for SWAMP users," he said. "We also reported errors and bugs within the system." All of those research findings, including errors and corresponding solutions, were shared ahead of SWAMP's launch to ensure that the tool was functioning properly. Today, SWAMP is open to all programmers in any language seeking to confirm the security of their code.

The Cyber Squad has also participated in national contests including the National Security Agency Codebreaker Challenge and multiple hackathons, where they met several industry professionals. **Dr. Jackson also played a key role in Reed's personal and professional development. "She taught me the importance of strong communication skills, and she makes sure you know how to present yourself."**

Like other Cyber Squad members, Reed earned valuable internships, including a job with the NIST. For two summers, he worked on significant NIST projects—one involving security certificates, and the other rewriting the security protocol. With all of his hands-on training and real-world experience, Reed was highly prepared for his current position at the tech company Customer Value Partners. He also has a global view of the cybersecurity field.

Only six months after earning his bachelor's degree, Reed is already looking for ways to make an impact in cybersecurity and positively influence his community. Next, he plans to pursue a master's degree in data science or cybersecurity management. His ultimate goal is to open a technology school for minority youth to increase the number of Americans who are equipped to protect the country against cyber threats.

UNIVERSITY EFFORTS

TOWSON UNIVERSITY

TOWSON UNIVERSITY, one of the nation's top regional public universities, is a leader in cybersecurity education both statewide and nationally. Towson's computer and information sciences department pioneered the first undergraduate cybersecurity track in Maryland, which is also one of the first in the nation, and offers five cybersecurity-focused programs at both the undergraduate and graduate levels: B.S. and M.S. in computer science with computer security, M.S. in applied information technology program with information security and assurance, a post-baccalaureate certificate in information security and assurance, and a post-baccalaureate certificate in computer forensics. Towson received the first and only Center of Academic Excellence in Cyber Operations designation by the NSA in the state and is expected to receive the first of four ABET accreditations for cybersecurity programs in the nation. Towson also has an applied D.Sc. in information technology, whose graduates often stay in academia to train the future of talent in cybersecurity.

FACULTY IN CYBER

Faculty with broad areas of expertise: Secure Coding, Cyber Operations, Cyber Defense, Cyber Pedagogy, Reliable Software Engineering, Data Sciences, AI, Social Networking

Numerous grants both for research and curriculum: Security Injections, Cyber-Physical Systems, Wireless Security, Application Development

In addition, Towson's Center for Continuing Education and Professional Studies offers information technology courses in cybersecurity, including in-person and online cybersecurity specialist courses that offer three CompTIA certifications and a dual enrollment network security course that combines two key certifications, Network+ and Security+, into one program. Serving a wide variety of students from undergraduates to experienced professionals, the center has instructors from industry, encourages hands-on learning, and leverages its Cisco courses and equipment to prepare students with, and to train teachers to teach, the latest skills and certifications for the cybersecurity job market.

In recognition of its leadership in cutting-edge cybersecurity education, the university receives cybersecurity grants from the National Science Foundation, National Security Agency, and several other federal and state agencies. Faculty at Towson is also working on cutting-edge federally funded cybersecurity research on the smart grid, wireless networks, cyber-physical systems, and social networks. In addition, through a National Science Foundation Scholarship grant,

16+

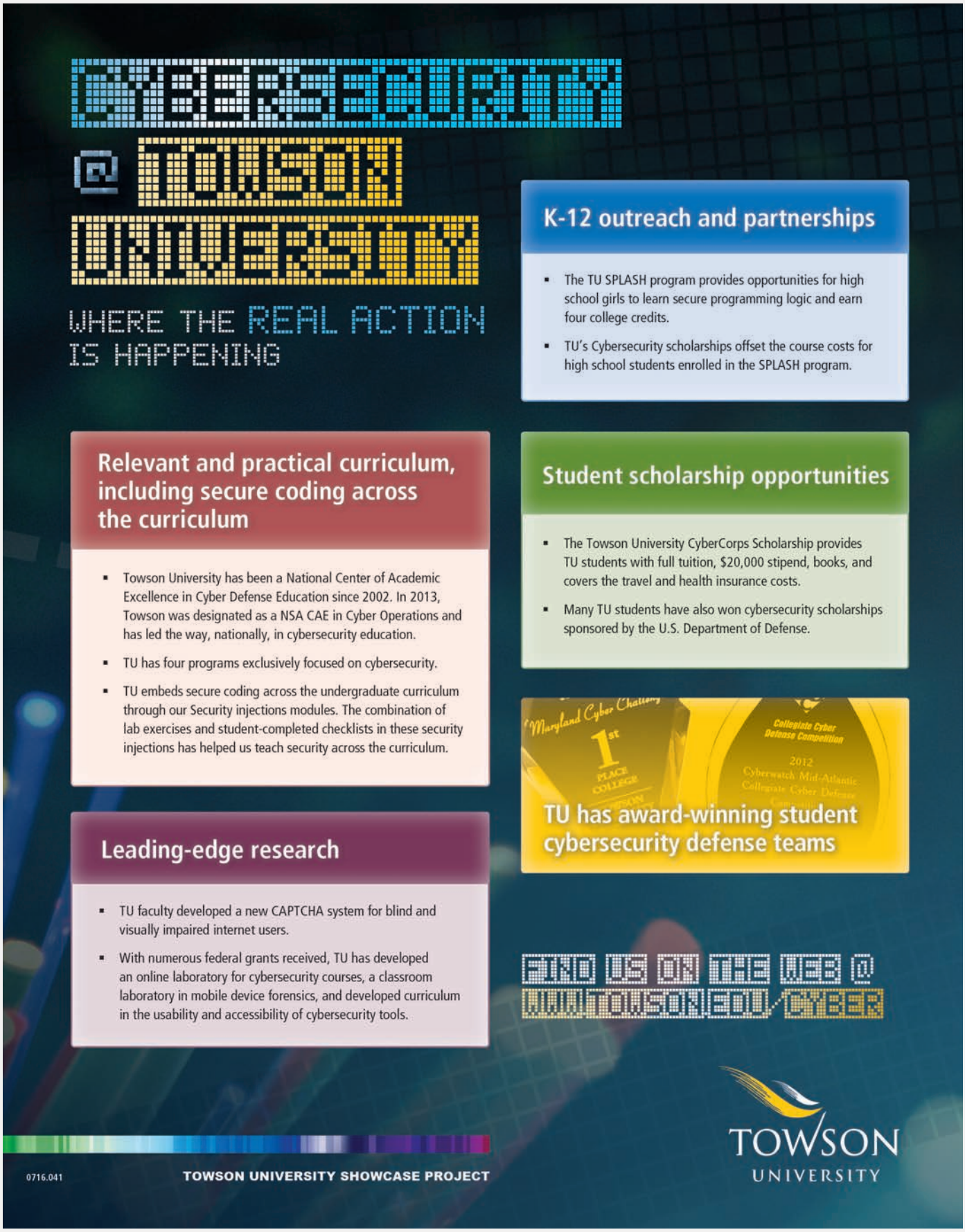
FULL-TIME FACULTY INVOLVED IN CYBERSECURITY AND ADJUNCT FACULTY WITH INDUSTRY EXPERIENCE

5

CYBERSECURITY-FOCUSED PROGRAMS AT BOTH THE UNDERGRADUATE AND GRADUATE LEVELS

1ST

AND ONLY CENTER OF ACADEMIC EXCELLENCE IN CYBER OPERATIONS DESIGNATION BY THE NSA IN MARYLAND


CYBERSECURITY
@ TOWSON
UNIVERSITY
WHERE THE REAL ACTION IS HAPPENING
K-12 outreach and partnerships
The TU SPLASH program provides opportunities for high school girls to learn secure programming logic and earn four college credits.
TU's Cybersecurity scholarships offset the course costs for high school students enrolled in the SPLASH program.
Relevant and practical curriculum, including secure coding across the curriculum
Towson University has been a National Center of Academic Excellence in Cyber Defense Education since 2002. In 2013, Towson was designated as a NSA CAE in Cyber Operations and has led the way, nationally, in cybersecurity education.
TU has four programs exclusively focused on cybersecurity.
TU embeds secure coding across the undergraduate curriculum through our Security injections modules. The combination of lab exercises and student-completed checklists in these security injections has helped us teach security across the curriculum.
Student scholarship opportunities
The Towson University CyberCorps Scholarship provides TU students with full tuition, $20,000 stipend, books, and covers the travel and health insurance costs.
Many TU students have also won cybersecurity scholarships sponsored by the U.S. Department of Defense.
Maryland Cyber Challenge
1st PLACE COLLEGE
Collegiate Cyber Defense Competition
2012
TU has award-winning student cybersecurity defense teams
Leading-edge research
TU faculty developed a new CAPTCHA system for blind and visually impaired internet users.
With numerous federal grants received, TU has developed an online laboratory for cybersecurity courses, a classroom laboratory in mobile device forensics, and developed curriculum in the usability and accessibility of cybersecurity tools.
FIND US ON THE WEB @ WWW.TOWSON.EDU/CYBER
0716.041
TOWSON UNIVERSITY SHOWCASE PROJECT
TOWSON UNIVERSITY

Towson provides two-year CyberCorps scholarships for students studying computer science with a focus in computer security, including tuition, books, a stipend, and allowance for relevant travel and health insurance. This program is intended to develop qualified computer security professionals that will join the federal and state workforce and secure the national information infrastructure.

A core philosophy at Towson is the idea that all students should have some experience in cyber. The university's Security Injections@Towson project strategically places security-related modules into existing undergraduate computer science classes with a combination of lab exercises and student-completed checklists, ensuring that security is taught early across the curriculum and engaging hundreds of instructors and thousands of students across the country. Towson's extra-curricular opportunities include cybersecurity seminars held twice monthly with invited speakers from industry and government, a Cyber Defense Team that has been ranked first four times in mid-Atlantic Collegiate Cyber Defense Competitions and has competed nationally, and a Cyber Defense Club open to any student interested in expanding their knowledge of computer security through activities such as discussions of current events, hands-on labs, and cyber defense competitions. A formal, well-designed internship program and graduate assistantships sponsored by industry also ensure that students engage in critical work-based learning opportunities as well.

Towson's commitment to diversity and broader impact is reflected in its cyber approach as well. In addition to the multiple pathways for a degree or certificate in cybersecurity, Towson's Secure Programming Logic Aimed at Highschool program provides an online introductory programming logic course that prepares high school girls to begin programming in any language and counts for a four-credit college course, which can be transferred to any institution. Towson's diverse faculty, 16 of which are focused on cyber, serve as an example of diversity and the broad knowledge and expertise that is important in the field. Faculty contributions to national efforts, such as the task force for writing the first Association for Computing Machinery Cybersecurity Curriculum and the federally funded Cyber Education Workshop that brings together cybersecurity educators to strengthen cybersecurity education, ensure that Towson remains a leader at the forefront of cybersecurity.

STUDENT PROFILE / **BRANDON MOODY**

Brandon Moody never leaves home without a certain textbook from his cybersecurity case studies class. Well, that's an exaggeration, but he does always have the book on hand at his internship with the U.S. Department of Health and Human Services Office of the Inspector General.

"It almost acts as a bible," jokes the senior, who says the case studies class was excellent preparation for his position as an information technology auditor/specialist at the government agency.

In fact, it was Towson's highly respected computer science program that drew Moody to attend in the first place, despite acceptances from other prestigious institutions. (Towson's in-state tuition and proximity to his family didn't hurt either.)

"Everything relies on computers," explains the west Baltimore native, emphasizing the importance of learning to protect information systems from threats. And Towson's academics are giving Moody the first-class training he needs to be part of the new generation of computer scientists safeguarding information from hackers whose deeds increasingly dominate headlines.

Additionally, engaging with the Cybersecurity Club, Black Student Union, and multiple honor societies is helping Moody jump-start his career through professional networking and exposure to people from a variety of backgrounds.

"I like the diversity at Towson," says Moody. "Being around different types of people prepares you for a professional environment."

Towson University. (2018). *Brandon Moody.* Retrieved from https://www.towson.edu/fcsm/departments/computerinfosci/bmoody.html

EARLY RETURNS

IN THE SHORT TIME SINCE USM'S cybersecurity programs launched, the number of students completing them has increased dramatically. Since 2015, USM has awarded more than 10,000 bachelor's degrees in cybersecurity-related programs, and the programs continue to grow. By offering programs that attract students from different backgrounds, USM has provided opportunities for full-time and part-time students, veterans, active-duty members, women, and members of other underrepresented groups to join the cybersecurity workforce. USM's community college partners have been an important part of this outcome. In the 2016–2017 academic year, more than 3,000 students from Maryland community colleges transferred into UMUC's undergraduate cybersecurity programs.

Student participation in internships and other work-based learning experiences is also on the rise. Seventy percent of rising sophomores in UMD's ACES program complete an internship, and 92 percent of UMBC's Cyber Scholars participate in an internship or research experience.

USM's industry and government partners plan to grow their internship programs to take fuller advantage of the opportunity to engage with the universities' talented students and identify those who are a good fit for their organizations. Partners frequently recruit interns into full-time positions, often making offers well before students graduate or consider other job opportunities. This talent pathway through USM has proven highly valuable to partners, who are especially pleased with the diversity they see, particularly the increased representation of women.

The reputation of USM's cybersecurity programs has attracted interest from many employers in the region, expanding the network of businesses and government agencies pursuing partnerships with the system and its campuses.

Evidence suggests that USM's efforts—particularly the relationships it fosters between students and local employers—are helping address the region's shortage of cybersecurity talent. Graduates of these programs are in demand for high-paying jobs, with the vast majority earning at least $70,000 in their first full-time position after college. These students receive many job offers, but most choose to stay local, having discovered that their home region offers compelling opportunities to build meaningful careers in cybersecurity.

WORK-BASED LEARNING

Internships are a high-impact practice in higher education that provide students with opportunities to apply their emerging knowledge and skills in real-world settings and gain work experience that is critically important to local employers looking to hire full-time cybersecurity professionals. They also serve as opportunities for students to explore potential employers—and for employers to evaluate potential full-time employees. **USM and its campuses frequently communicate with partner organizations about internships to learn whether students are demonstrating the expertise that employers expect and to use that feedback to make any needed adjustments in the curriculum.** For employers, internship programs are a valuable strategy for recruiting future full-time employees. Interns build relationships with colleagues and become familiar with the organizational cultures at their internship sites. USM cybersecurity graduates are in demand when they enter the job market; positive internship experiences with partner organizations can nudge them to stay local and continue working with employers where they feel at home.

PRIMARY RECOMMENDATION

Expand and Improve Student Cyber Work-Based Learning Experiences

As noted above, entry-level cyber jobs in the Washington, D.C., region carry heavy academic and experiential requirements, with the most openings demanding at least a bachelor's degree and three years of relevant work experience. These requirements place students in a bind: How do they get the experience to qualify for their first jobs in cyber? Policymakers, businesses, higher education leaders, and other stakeholders are concerned that students will take their degrees and training from Maryland institutions to other regions in search of entry-level positions.

A need exists to significantly expand student cyber work-based learning experiences in Maryland, particularly at the post-secondary level where many students have reached a level of proficiency in technological fields, are close to making career decisions, and can make real contributions to employers' work needs. Work-based learning models—such as internships, co-ops, and research courses already in place at USM and other institutions in the state—should be expanded, particularly to include underrepresented groups.

Further, the State of Maryland could significantly scale student work-based learning experiences and spur greater student interest in cyber careers and engage business and postsecondary institutions through matching grants. The funds would go primarily to students, but companies and participating federal agencies would be asked to provide some portion of a student's stipend/cost of living expenses and the state would contribute the rest, thereby stretching public funds and getting buy-in from the business and federal sectors. The amount of the match could be based on the size of the company: Bigger companies would be asked to cover more of the costs, thus encouraging small and midsize companies to participate.

Companies from nondefense sectors (e.g., financial, health care, retail) would be especially encouraged to participate. Participating organizations could come together to establish industry-recognized credentials, such as badges, that would satisfy work requirements for students who undertake work-based learning through this proposed initiative.

ADDITIONAL RECOMMENDATIONS **FOR POLICY MAKERS**

Continue to formally assess workforce needs at the state level in order to rapidly respond to new opportunities to create in-demand programs. The cybersecurity efforts in Maryland have been driven by research-based workforce assessments that identified opportunities and challenges facing the region. These assessments drew on the complementary expertise of government officials, local employers, and higher education leaders. This body of evidence has proven vital to formulating workforce development strategies that effectively leverage available resources, seize ready opportunities, and address or account for foreseeable constraints.

Use convening power to set a workforce-development agenda in motion. Over the years, the State of Maryland and USM have had considerable success in convening stakeholders around cyber workforce development and building a community of interested employers, academics, and public servants to lead on this issue. Policymakers committed to seeing workforce development sustained over the long-term should continue to convene interested parties and enable them to spearhead the movement.

Prioritize cybersecurity in state government. State policymakers have an immense opportunity to demonstrate their leadership and understanding of 21st-century challenges by establishing cybersecurity as a critical priority in state government. To support that commitment, states could actively engage in the National Governors Association's initiative, *Meet the Threat: States Confront the Cyber Challenge*, which places states at the center of finding solutions to the country's cyber threats. Such initiatives can help states develop a systematic statewide response to cybersecurity threats and talent needs.

Fund public higher education to enable strategic workforce development. USM is producing thousands of cybersecurity graduates each year, but it could be producing many more. Because of resource constraints, the universities' cybersecurity programs are operating at capacity and are turning away interested students. The full potential of these programs to grow Maryland's cybersecurity workforce could be realized with additional public investment. In addition, these funds could be used to support regional economic development initiatives on campus such as business incubators.

ADDITIONAL RECOMMENDATIONS **FOR HIGHER EDUCATION LEADERS**

Accelerate program development by leveraging institutional strengths and existing partnerships. USM campuses have been able to design and launch new programs on an unusually short timeline by identifying and deploying relevant institutional assets. Rather than starting from scratch, they have looked for opportunities to build on established program models and use existing resources creatively. Likewise, rather than spending time cultivating new relationships with industry and government, campuses built momentum quickly by calling on their long-standing partners.

Create programs that reflect and reinforce the institution's niche. Each university profiled in this case study has a unique mission, history, and student body, and the cybersecurity programs developed on these campuses reflect that diversity. Instead of trying to replicate programs that worked on other campuses, each university created a distinctive cyber pathway consistent with its institutional identity. As a result, each program attracts different students into the cybersecurity talent ecosystem, rather than competing for the same pool of students.

Ground program curricula in practitioner expertise. To ensure that cyber programs are tightly aligned with workforce needs, USM and its campuses have worked closely with government and industry partners to co-develop curricula. In addition, these institutions have found that hiring practitioners as adjunct faculty is an

effective strategy for ensuring that courses stay current. Integrating the expertise of cybersecurity practitioners has enhanced the value proposition of these programs by assuring prospective students—and employers—that program graduates will be equipped with the skills, knowledge, and experience to successfully enter the cyber workforce.

Promote meaningful engagement between students and business and government partners. Students enrolled in USM's new cybersecurity programs have rich opportunities to interact with the businesses and government agencies that partner with their universities. Partners sponsor internships and cybersecurity contests; encourage their current employees to serve as adjunct faculty, guest speakers, and mentors; and invite students to tour their facilities. Sponsored by the National CyberWatch Center, the National Cybersecurity Student Association provides further educational and professional development of students through activities, networking, and collaboration. Through all of these interactions—which are often formal components of cybersecurity programs—students build professional networks that frequently lead to job opportunities at partner organizations.

Ensure partnerships are mutually beneficial. USM and its campuses ask their industry and government partners for a variety of resources, including financial contributions, internship positions, and personnel to teach courses and mentor students. They want their partner organizations to see a return on these investments. Many partners engage with USM because they are interested in hiring its graduates. USM helps them achieve that goal by providing partners with opportunities to network with students and by sharing information about where their graduates are accepting jobs and why so that partners can more effectively compete for prospective employees. Providing a home for business incubators with access to an institution's talent pool also ensures mutually beneficial relationships with partners.

Invest in efforts to attract and retain students from underrepresented groups, especially women. USM has adopted a variety of strategies for increasing diversity in its cybersecurity programs, including outreach to students as early as elementary school, recruiting faculty and mentors from underrepresented groups to ensure that students see diverse role models, designing interdisciplinary curricula that appeal to students who might feel they do not belong in fields that are purely technical, and working closely with cohorts and individuals to foster students' feelings of support on campus. Targeted marketing materials, capture-the-flag competitions, and involvement in the National Youth Cyber Education Program represent opportunities to cultivate interest in cybersecurity and career opportunities to all students, especially women, from K–12 and beyond. Many of these strategies are resource-intensive, but these efforts are crucial to changing the face of the cybersecurity workforce.

Identify and remove barriers to collaboration. In some cases, businesses or government agencies were eager to partner with USM or its campuses, but obstacles within the institutions made collaboration difficult or impossible. USM and its universities have worked to modify bureaucratic processes that obstruct collaboration. In essence, these institutions have become more entrepreneurial in order to respond more nimbly to partnership opportunities.

ADDITIONAL RECOMMENDATIONS **FOR BUSINESS LEADERS**

Commit to deep engagement with academic partners. For many companies that partner with USM, the most valuable return on their investment in cybersecurity programs is the talented graduates they hire as full-time employees. Because graduates of these programs are in demand on the job market, companies that see the best return on their investment are those who give more than money: They give time and personnel. These companies consistently seize opportunities to build relationships with students by encouraging employees to serve as adjunct faculty or mentors, by sending representatives to networking events, and by sponsoring activities that spark students' interest.

Be open to talent from nontraditional pathways. Many job openings in cybersecurity specify that applicants should have a degree in computer science. This requirement excludes candidates who could be excellent matches for open positions and could also bring greater diversity into the workforce. For example, someone with an economics degree might have great potential as an analyst, and a veteran who completed a noncredit cybersecurity certification program might be better prepared than a freshly minted computer science graduate to contribute on day one. Given the scale of demand for cybersecurity professionals, employers may benefit from looking beyond a specific credential and considering job applicants' backgrounds in a holistic way.

Engage all sectors in cyber workforce development. Cyber jobs in the region focus largely on the defense sector, but employers from other sectors, such as financial, healthcare, retail, and critical infrastructure, should be brought to the table to convey their particular workforce requirements to the education community in order to grow and retain talent suited to their needs.

Cultivate and recruit a diverse workforce. Employers should actively engage in efforts to develop and recruit a diverse workforce. They may consider partnering with HBCUs and minority-serving institutions on cybersecurity programs or pathways and encouraging company representatives to mentor underrepresented minorities. Engaging in such efforts benefits not only the companies themselves but also the cybersecurity workforce as a whole.

> "No state is better equipped or better positioned than Maryland to address the rapidly emerging and evolving cybersecurity challenges facing our nation."
>
> **LARRY HOGAN** / GOVERNOR / STATE OF MARYLAND

Office of Governor Larry Hogan. (2017). Governor Larry Hogan Issues Executive Order Enhancing Maryland's Cybersecurity Preparedness [press release]. Retrieved from http://governor.maryland.gov/2017/10/05/governor-larry-hogan-issues-executive-order-enhancing-marylands-cyber-security-preparedness/

ABOUT THE UNIVERSITY SYSTEM OF MARYLAND

The University System of Maryland (USM) is the state's public higher education system. USM's 12 institutions, two regional higher education centers, and system office work closely together to leverage their collective expertise and resources, share best practices, increase the system's effectiveness and efficiency, and advance USM's mission to improve the quality of life in Maryland. Benefiting students, as well as Maryland and its citizens, USM offers expansive access to affordable, high-quality educational opportunities, performs groundbreaking research, instills a culture of innovation and entrepreneurship, promotes economic growth and workforce development, provides vital services to communities and individuals, and partners with business, governmental, nonprofits, and organizations to improve quality of life.

ACKNOWLEDGEMENTS

BHEF would like to thank all the interviewees from the University System of Maryland, its campuses, and its partner organizations—including the Greater Washington Partnership, The MITRE Corporation, the National Institute of Standards and Technology, the National Security Agency, Northrop Grumman Corporation, and the State of Maryland—for providing detailed information and insights related to the ongoing development of undergraduate cybersecurity pathways throughout the University System of Maryland. BHEF would also like to thank our writing consultant, Maya Weilundemo Ott, for her contributions to this case study and the Alfred P. Sloan Foundation for their support for this work.

This work was funded by the University System of Maryland and five of its campuses: Bowie State University, Towson University, University of Maryland, Baltimore County, University of Maryland, College Park, and University of Maryland University College. It is a part of a partnership between the University System of Maryland and the Business-Higher Education Forum.

SYSTEM CONTACTS

Ms. Mary M. Morris
Assistant, Vice Chancellor for Economic Development
University System of Maryland
mmorris@usmd.edu

Mr. J. Thomas Sadowski
Vice Chancellor for Economic Development
University System of Maryland
tsadowski@usmd.edu

www.usmd.edu

 / 2025 M Street NW, Suite 800 / Washington, DC 20036
202.367.1189 / info@bhef.com / www.bhef.com