**Institution: Brookdale Community College PR# R116R180044**

*Building a Virtual Lab Environment to Provide Cybersecurity Students with Improved Hands-on Skills*

Brookdale Community College requests $95,334 from the US Department of Education’s Pilot *Program for Cybersecurity Education Technological Upgrades for Community Colleges* grant competition to enhance the college’s existing Networking and Cybersecurity offerings. The funds will be used to purchase, install and populate a virtual lab environment using Network Development Group’s NETLAB+ Virtual Edition with 32 active pods (VE 32), along with the required server infrastructure, on-site support and miscellaneous hardware.

Brookdale Community College will leverage expertise and resources from the Center for Systems Security and Information Assurance (CSSIA), one of the National Science Foundation’s Advanced Technological Education (ATE) Centers that supports the improvement of cybersecurity education. A letter signed by Dr. John Sands, Principal Investigator for CSSIA, certifying their center will provide Brookdale with technical assistance on this project, is included in the application. A description of the role CSSIA will play is detailed in the narrative.

Brookdale has been teaching networking courses since 2000 and introduced security into the program in 2003. A 2013 grant from the National Science Foundation enabled Brookdale to add courses in Computer Forensics, Perimeter Security and Ethical Hacking and develop an18-credit certificate in cybersecurity. For Fall 2018, this certificate has been integrated into the existing Networking program as a Cybersecurity track. Program enrollment has grown consistently year-to-year, with 29 students graduating with a Cybersecurity certificate in May 2018. A consistent challenge in growing our cybersecurity offerings is providing students with a safe, robust and customizable environment to learn apply and master hands-on skills.

Faculty has explored a variety of alternative methods of to enable students to learn hands-on skills. These include using physical hardware in existing classrooms, a solution limited by the college’s security policy and requiring significant effort to update and maintain. Additionally, the program has provided access to cloud-based virtual lab environments or simulations through 3rd-party vendors and publishers, such as Infosec Learning, Jones and Bartlett Learning or TestOut.com. These solutions not only add financial burdens to students already struggling to pay for tuition and books, the methods also have limited customizability, are dependent on vendor updates, and in the case of simulations, do not provide real-world experiences.

This proposed solution of Virtual Labs will provide students with no-cost access to a dedicated platform to learn and master the hands-on skills that are so important in Cybersecurity. Additional benefits include the ability to quickly ramp up new labs and courses developed by the CSSIA center and their network of partners, to develop our own custom labs, to host on-site and regional competitions and to provide lab capacity for other community colleges and high schools.

**Institution: The Research Foundation of the City University of New York on behalf of Bronx Community College PR# R116R180039**

**The Cybersecurity Laboratory Upgrade (CLU) Project**

The Research Foundation of the City University of New York (RFCUNY) is pleased to submit this proposal on behalf of Bronx Community College (BCC), an eligible institution that is collaborating with the National CyberWatch Center at Prince George’s Community College. A signed statement from the National CyberWatch Center is attached, certifying it will provide technical assistance or other aid to BCC’s proposed **Cybersecurity Laboratory Upgrade (CLU) Project.**

BCC is requesting **$98,170 over two years** to support the technological upgrades of our cybersecurity computer lab. In November 2017, our 60-credit Cybersecurity and Networking Associate in Applied Science (AAS) degree program—which includes a 30-credit certificate program embedded within it—was approved and registered by the New York State Education Department, making it the first Cybersecurity degree program at the community college level within the City University of New York (CUNY). The program, which will be offered through the College’s Department of Engineering, Physics and Technology, will launch in Fall 2018 with 25 students enrolled to date.

Upon establishing the Cybersecurity and Networking Program on our campus, a baseline computer lab was configured. Although the current lab can support the program’s initial implementation, as students begin enrolling in higher-level courses beginning in Fall 2019, its technological limitations, particularly as it relates to providing a virtual work environment, will become glaringly apparent and detrimental to the quality of the instruction provided. The proposed upgrades, coupled with technical assistance from the National CyberWatch, will address these inefficiencies, resulting in a program that provides BCC students—the majority of whom are significantly low-income—with the robust hands-on training they need to be competitive in the job market and secure meaningful, self-sustaining employment. Further, strong student outcomes and their overall satisfaction will serve to stabilize the program, resulting in increased rates of student persistence and enrollment annually.

**Institution: Central Piedmont Community College** **PR# R116R180047**

NETLAB Expansion Project

Central Piedmont Community College (CPCC) is a public, two-year college located in Charlotte, North Carolina. CPCC is one of the largest community colleges in the state serving over 70,000 individuals in Mecklenburg County and the region through its curriculum programs, continuing education, college readiness offerings and special events. The College operates multiple campuses and educational sites, and offers over 300 certificate, diploma, and associate degree programs that provide high-quality, relevant education across multiple industry sectors. Since its establishment in 1963, CPCC has strived to be a resource for its community, providing high-quality educational options for students consistent with their needs, interests and abilities.

Cybercrime has been on the rise for several decades and advances in computer technology have increased the sophistication of digital crimes at a rapid rate. In 2009, CPCC developed an Associate of Applied Science (AAS) degree in Information Technology with a specialty in Information Assurance and Digital Forensics to meet the growing demand for cybersecurity professionals. This specialty program is complemented by a NETLAB that supports remote access for a hands-on training environment, however, CPCC’s current NETLAB is out of date and in need of critical technological upgrades.

CPCC’s planning for the Cybersecurity Education Technological Upgrades Pilot Program involved reaching out to the National Science Foundation (NSF) funded National CyberWatch Center, located at Prince George’s Community College in Largo, Maryland. CPCC obtained a signed statement of support from the National CyberWatch Center, and in doing so, has met the absolute priority for the Cybersecurity Education Technological Upgrades pilot program. CPCC will welcome any advice or mentorship that any of the NSF Centers can offer, and looks forward to contributing to the national conversation on cybersecurity education and workforce development.

CPCC requests funding from the US Department of Education to purchase equipment and supplies for a new NETLAB and modify a current remote lab to be used as a redundant backup site. NETLAB is an online lab solution that provides students access to live IT infrastructure to perform technology-related experiments from any web-based computer. The NETLAB is important to the study of cybersecurity because it creates a hands-on training environment in which students can use professional forensic software. The purchase of new, advanced equipment, will allow the College to upgrade existing technology and offer training that is relevant to actual field applications of evidence collection and preservation, and forensic analysis.

The technological upgrades will allow CPCC to increase the capacity of the cybersecurity program to enroll more students and expand online course offerings. Students will have 24/7 remote access to software and hardware that would otherwise be cost-prohibitive. This increase access through a complete online degree will allow the College to enroll students from anywhere and expand opportunities for more students to enter into the field of cybersecurity. The NETLAB will provide CPCC with access to the most advanced technology and ensure that graduates of the cybersecurity program are equipped with the in-demand technical skills required by employers.

**Institution: Forsyth Technical Community College PR# R116R180001**

Forsyth Technical Community College will use the $99,830.55 in Department of *Education Pilot Program for Cybersecurity Educational Technological Upgrades for Community Colleges* funding to develop a Cyber Security Operations (SOC) Laboratory in collaboration with NSF-ATE Whatcom Community College and Cyber Watch West. This project addresses the ABSOLUTE PRIORITY by directly collaborating with one of the three designated NSF-ATE centers to expand existing cyber education programs and increase enrollment in cyber related majors. This collaboration and the development of the SOC Lab will create an engaging and immersive educational experience that will result in higher rates of enrollment, retention and completion of students in three identified IT programs. Other programs, including Biotechnology, will utilize the lab to expand cyber skills. Outcomes will be measured by an internal evaluator along with formative and summative assessments.

**Institution: Hostos Community College PR# R116R180013**

**Project Title**: Cyber Security Education Opportunity Program (CSEOP)

Hostos Community College seeks to receive funds as part of the Cyber Security Education Pilot Program in order to build upon its success as an anchor higher education institution for social mobility. Serving one of the poorest congressional districts in the country, the South Bronx, Hostos has been a beacon of hope and socio-economic progress for generations of traditionally disenfranchised populations. As an award winning institution, for its degree and workforce development programs, advanced technology and community focus, Hostos is requesting $91,600 to help upgrade a classroom with audio visual instructional capability and provide the necessary technology infrastructure to enable anytime/anywhere access to cyber security training curriculum and lab environments. In support of its commitment to the focus of improving technology workforce development, the college will contribute over $127,000 in personnel, equipment, supplies and other services towards the implementation, expansion and ongoing support of the CSEOP. Initially as a Cisco Cybersecurity Operations certificate program - which will ultimately articulate for credits in our Cyber Security degree program - Hostos is establishing a pathway for students to acquire work-ready skills and then attain an Associate and ultimately a Bachelor’s degree via our agreement with John Jay College of Criminal Justice. With a target of 20 students within the first year of the program and a combined 60 across the certificate and degree programs by the third year, Hostos is ensuring that maximum impact is realized with the assistance of these federal funds and support from our ATE partner, Prince George’s Community College.

**Institution: Lake Superior College PR# R116R180002**

Lake Superior College (LSC) will use Cybati Works IoT (Internet of Things) kits to integrate cyber-physical security into their current cybersecurity program. This would be a very beneficial technological upgrade for our school and curriculum. Currently, students do not have the resources to investigate the growing security risk generated by IoT devices. These devices are appearing in everything from barbeque grills to washing machines and are connected to our homes and businesses. Unfortunately, very few of them have cybersecurity controls in place. These devices are also found throughout the power, fuel and transportation infrastructures. IoT attacks have already been implemented and will become more prevalent in the future because of the exponential growth of IoT devices.

As a result of a Cybersecurity Workforce Education grant (provided by NSA), Lake Superior College already has a lab comprised of various mini organizations. The organizations include finance, transportation, manufacturing, education, government and healthcare. The IoT lab equipment includes mini power grids, traffic lights and a conveyor belt. Cybati Works also includes training and curriculum for students, so it will easily integrate into our lab comprised of mini workplaces.

There are very few people trained in IoT security and little IoT curriculum. Faculty and CIS (Computer Information Services) student workers will work together to integrate the equipment into our current Cybersecurity Workforce Education lab. Many of our students are taking positions in the government, so they could make an important contribution to the government.

Lake Superior College summer cybersecurity camps and support for several CyberPatriot teams that could learn from our new resources. College of St Scholastica students will benefit because they use our curriculum for their Bachelor’s degree. We will share our project and curriculum with other educational institutions.

**Institution: Rose State College PR#** **R116R180032**

As one of the premiere community college programs in cybersecurity in the Midwestern part of the United States, and as the only recognized cybersecurity certificate program in a top-30 city in U.S. population, the Rose State College (RSC) cybersecurity program is experiencing exponential growth. That growth has brought a strain on college resources including laboratory space, especially for student use before, between and after classes. Current labs are used virtually non-stop during the day for classes in the cybersecurity curriculum and a need has arisen for a self-paced lab that will be open to students whenever the building it is housed in is open. An ideal space for this lab already exists on the Rose State College campus, so there is no need for construction or remodeling. The entire cost of the lab is less than $100,000.

Many RSC students have fulltime jobs and need a fully-equipped cybersecurity lab at non-class hours to complete their assignments. Others have opted to take the entire program online—including one option that can be completed in twelve months. Others need additional time to complete assignments—possibly because of physical or intellectual challenges. Still others may wish to accelerate and work on independent projects between classes. For all of these reasons, Rose State College proposes to build a Self-Paced Cybersecurity Laboratory with extended hours and equipment that mimics the equipment used in the classroom to allow both the traditional and non-traditional students of Rose State College to complete their assignments between classes without the burden of inconvenient hours or have to self-purchase expensive equipment in order to be able to work at home.

This grant will truly “level the playing field” in cybersecurity education and pedagogy at Rose State College for the working student, the student who lacks the funds to purchase his or her own training equipment and the student whose challenges cause them to need more time to complete class assignments.

**Institution: St. Petersburg College PR#** **R116R180012**

**Project Title:** *St. Petersburg College Cybersecurity Education Technological Upgrades* **Abstract:** Cybercrime costs have skyrocketed, reaching nearly $2 trillion per year; Tampa Bay metro area is the 10th most cyber insecure community in the U.S. due in part to the large presence of defense and financial service firms, including 19 global corporate headquarters. Florida is the fourth largest cyber employment market behind only California, Virginia, and Texas, and projects a 28% increase in employment of information security analysts through 2026. Located in Tampa Bay, St. Petersburg College (SPC) strives to remain on the forefront of cutting-edge curriculum and technology to meet regional and global workforce demand. SPC’s College of Computer Information and Technology offers a Certificate and A.S. Degree in Cybersecurity, and is currently applying for the Two-Year Education (CAE2Y) designation in Cyber Defense for the A.S. degree. These offerings enrolled over 400 students in the 2017-2018 academic year alone, nearly doubling enrollment since 2015. However, many employers require a bachelor degree as the minimum standard for hire in cybersecurity. SPC was the first two-year college in Florida to offer baccalaureate degrees, and currently offers a Bachelor of Applied Science (B.A.S) in Information Technology Management. However, cybersecurity has emerged as a distinct discipline, necessitating a more technically focused, and standalone cybersecurity baccalaureate degree. In response to rising workforce and student demand, SPC will collaborate with CSSIA and industry advisors to upgrade and innovate the existing cybersecurity program, ultimately leading to a new B.A.S. in Cybersecurity degree. Once developed, this online B.A.S. in Cybersecurity will be the first of its kind at the community college level in Tampa Bay and only the second in Florida. The goal of this project is to increase the number of students pursuing a cybersecurity credential to meet workforce needs in the Tampa Bay region and beyond. This goal will be accomplished over a two-year period through the following objectives and activities: 1) Redevelop existing B.A.S. in Information Technology Management’s Cybersecurity subplan curriculum to increase training opportunities for students, including development of 4 new

subplan courses, integration of Capture the Flag virtual competitions, and industry certifications such as CompTIA PenTest+; 2) Develop a new B.A.S. degree in Cybersecurity aligned with NSA/DHS National Centers of Academic Excellence in Cyber Defense Education, including approval of academic plan and development of 6 new program courses; and 3) Improve faculty training and ability to offer industry-linked certifications in cybersecurity. By meeting these objectives, the project will serve approximately 200 students in the year immediately following the project end. This initiative will also strengthen regional and national partnerships with institutions in cybersecurity education, sharing resources and best practices for other community colleges seeking to develop B.A.S. programs. Funding will support faculty and staff efforts for curriculum development, new equipment for virtual training activities, and faculty certification training.

**Institution: Suffolk County Community College PR#R116R180010**

**CYBERSECURITY LAB EXPANSION**

New York State had 14,394 cybersecurity job openings as of March 2018 and is struggling to find properly credentialed professionals to fill them (Wall Street Journal, 2018). On Long Island, these professions are expected to grow by double digits through 2024, in occupations ranging from Information Security Analysts (+16.7%), Computer Network Architects (+14.3%) and Computer User Support Specialists (+13.7%; labor.ny.gov). Grant funding will support the extension of Suffolk County Community College’s existing collaboration with the National CyberWatch Center and expansion of its cybersecurity degree program onto its Michael J. Grant Campus within a newly-constructed 1,624 square foot laboratory space.

This $99,990 investment from the U.S. Department of Education will increase the College’s instructional capacity in the critical field of cybersecurity and information assurance, increase degree production in STEM disciplines; and help meet the NY metro region’s need for qualified cybersecurity employees. Equipment purchases will include pod components containing routers, switches and firewalls, servers, router racks, and multi-boot PCs for use by students, which will support instruction within the newly-expanded program. This configuration will help ensure improved student learning outcomes through a full range of real-world experiences and applications, which will maximize benefits to students and position Suffolk’s cybersecurity program for long-term vitality and growth.

**Institution: Whatcom Community College PR# R116R180030**

Whatcom Community College (WCC), in Bellingham, WA. This project will partner with the NSF ATE CyberWatch West center, housed at WCC, and has the full support of both the NSF ATE National CyberWatch Center and the National Center for Systems Security and Information Assurance.

**Project title:** Whatcom Community College’s Program for Cybersecurity Upgrades

Whatcom Community College (WCC) is proposing a cybersecurity upgrade program that will significantly and rapidly expand its training resources and instructional tools for industrial control systems (ICS) and SCADA education. In addition – through the NSF ATE CyberWatch West housed at WCC – WCC will support other colleges applying to this grant program. No funds are requested for this latter effort, which are part of the ATE center’s duties. Hence, this project has two goals:

Goal 1: To provide the industrial control systems (ICS) and SCADA training resources necessary for WCC faculty to provide state-of-the-art instruction to students, preparing them for modern workforce needs. Currently, only one faculty member has received training to teach ICS / SCADA and she is overextended given the popularity of WCC’s program. The need to train additional faculty to teach these courses cannot be addressed without the training resource requested. The College houses a nationally recognized cybersecurity center and is home to the NSF ATE CyberWatch West grant, but as a community college with few resources and a tight budget, it has very limited funds to purchase costly training systems and equipment for its programs. WCC’s computer information systems / cybersecurity program faculty lack training and use inadequate and outdated curriculum to teach ICS and SCADA security. Through funds requested in this grant, WCC will purchase six Marcraft industrial cybersecurity training systems to best prepare students for the strong growth forecast for industrial control systems market. Each training system includes curriculum and student labs, an industrial control systems trainer, SCADA software, programmable logic controller, and more. In order to increase faculty members’ SCADA expertise specifically, WCC also requests funds for cutting-edge, in-house SCADA training. As a result of this grant, WCC faculty will be trained, students will reap the educational benefits, and employers will hire program graduates with the skills needed to prevent cyberattacks and threats to control networks.

Goal 2: The NSF ATE CyberWatch West housed at WCC will support colleges applying to this grant program by providing technical assistance. WCC houses the NSF ATE CyberWatch West center and has a tremendous opportunity through this grant to help support colleges applying to the grant program. This grant presents an opportunity for the ATE center at WCC to provide technical assistance to colleges who are planning upgrades to their cybersecurity education technology. Because the consultation and personnel time required to do this is part of the ATE center’s regular duties, the College is *not* requesting funding for CyberWatch West to provide the technical assistance that colleges need to secure the right technological upgrades for their cybersecurity programs. As a result, colleges and their hundreds of program students will benefit from state-of-the-art upgrades.

**Institutions: San Antonio College PR# R116R180040**

San Antonio College (SAC)’s Cybersecurity Technology Upgrades Project will improve

cybersecurity education by increasing retention and success in gatekeeper cybersecurity

courses by enabling Computer Information Systems (CIS) faculty to move from a traditional,

lecture-based approach to teaching the often difficult and abstract concepts using simulated

work environments and real-world, IT-related workplace scenarios. Funding will establish a

dedicated laboratory that will allow IA/Cybersecurity majors to participate in simulated

scenarios that are modeled on real-world, workplace-based application of programming,

networking and cybersecurity concepts. Objectives include increasing the percentage of

students who pass the gatekeeper courses by at least 5%, maintaining existing retention rates

at 100% and raising those with less than full retention by at least 7%, and demonstrating

collective improvement, particularly in the area of “soft” workplace skills, via employer

evaluations conducted during mandatory student internships.

SAC will collaborate on this project with CSSIA at Moraine Valley Community College and

Cyber Watch West (CWW) at Whatcom Community College. This effort will expand our

existing relationship with the Center at Moraine Valley and establish a new one with CWW

at Whatcom. The Centers’ cybersecurity curriculum resources and VOIP security

information and toolkits that are designed specifically for community colleges will assist

SAC CIS faculty with revising curriculum for our four targeted courses and implementing an

authentic approach to instruction in the workplace simulation lab.