CYBERSECURITY WORKFORCE DEVELOPMENT

THE LONG GAME: A REGIONAL MODEL FOR THE NATION

THE CYBER INNOVATION CENTER
RESPONSE TO THE NIST RFI

bossier parish community college
EMBRACING • EDUCATING • EMPOWERING

cyber innovation center®
Collaboration • Research • Technology

NICERC™
AN ACADEMIC DIVISION OF THE CYBER INNOVATION CENTER

Cybersecurity Workforce Development

The Long Game: A Regional Model for the Nation

The Cyber Innovation Center greatly appreciates the opportunity to provide input to the critical area of growing and strengthening the cyber workforce. Exactly 10 years ago this month, leaders in Bossier City, LA set off on an aggressive journey to create a new economy for the local area focused on the cyber industry. The end state was to create new cyber positions in the local economy resulting in higher paying/quality jobs for the citizens in and near Bossier City, LA.

Most of the specific RFI questions will be answered in the below narrative. The questions which are not specifically answered are addressed at the bottom of this document. Our story is not a one size fits all; instead it serves as a model for other communities to create their own cyber workforce. From the men and women at the Cyber Innovation Center; we hope you enjoy our story!

In the 20th century, Louisiana's economy and workforce relied heavily on the oil and gas, agriculture, and gaming industries. Ten years ago, community leaders in Northwest Louisiana determined that for the region to be prosperous in the information age of the 21st century, we needed to transform our economic and education opportunities around cybersecurity. This pivot to a technology driven, knowledge-based economy began with a massive cooperative effort across government, industry, and educational institutions to revamp educational offerings at multiple levels and to lay the groundwork for a cyber-based workforce development pipeline instrumental to increasing the availability of talented cyber-professionals and providing pathways for entry into cyber careers. After ten years of work, while continuously adapting to the changing economic and technological landscape, Louisiana is beginning to reap the rewards of that groundbreaking vision.

In 2007, The Cyber Innovation Center (CIC), the now anchor of the National Cyber Research Park, was created in Bossier City, LA. The CIC was built on farmland where cows and crops have been replaced by technology infrastructure, miles of cables, computers, and high tech professionals employed by cyber-related companies, government as well as institutions of higher education. An area that members of a previous generation would have left without a second thought, today, is the campus of a significant cyber workforce.

The CIC acts as a "hub" between the cyber industry and higher educational institutions with the aim to develop a curriculum which allows the company to hire an employee at an entry level position and then grow that employee as he/she progresses through a career. The CIC recognized in the development of this pipeline that the traditional, linear process requiring a student to obtain a degree before entering the cyber workforce is no longer the only, or necessarily the preferred, method for achieving this goal. In many instances, it may prove more beneficial to provide a student with a customized training plan.

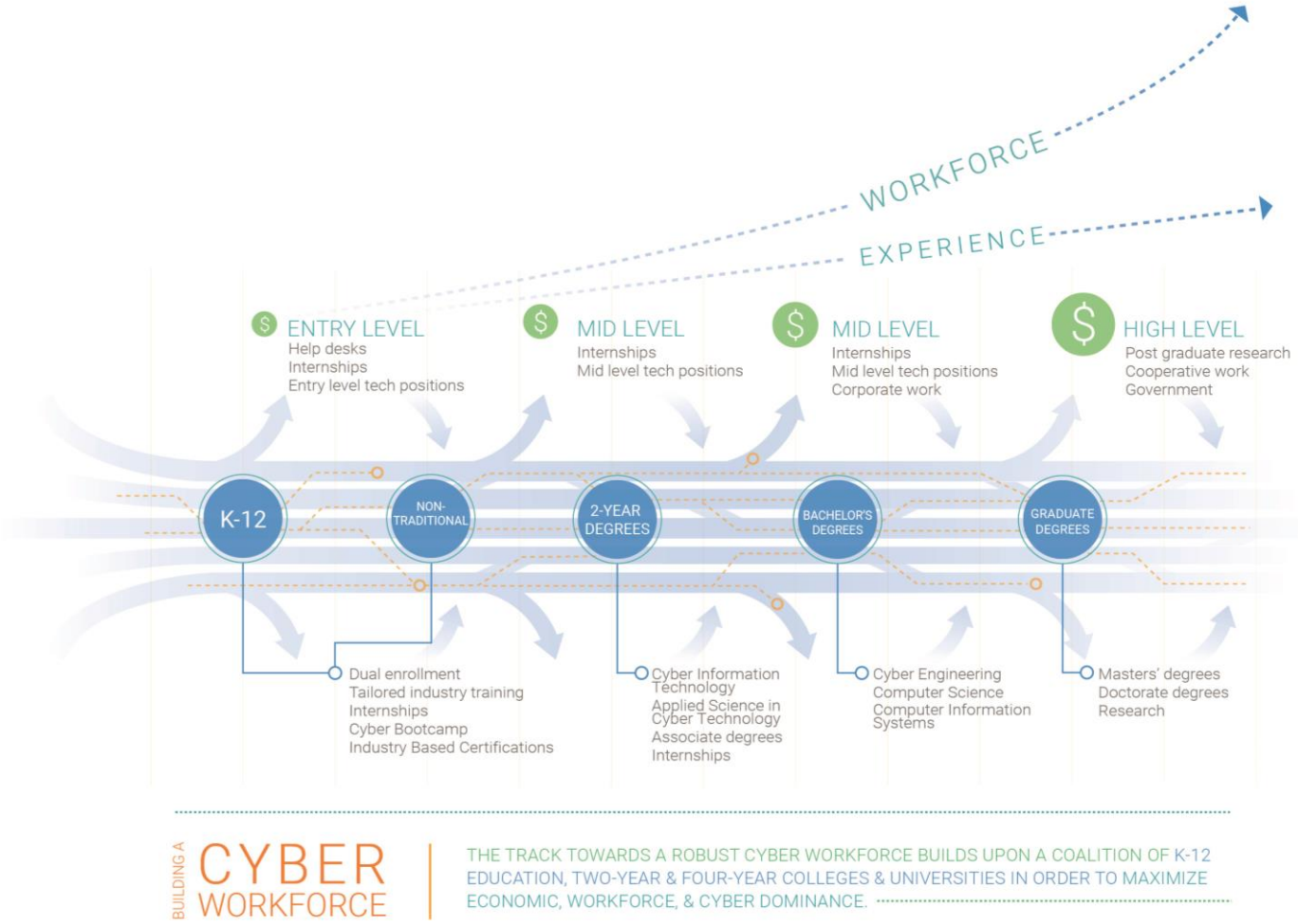

Figure 1. A Cyber Workforce Development Interstate

To acknowledge the possibility of multiple life paths leading to cyber workforce entry, the CIC has reimagined the traditional end-to-end workforce training pipeline as more of an interstate, populated with many points of entry, exit, and re-entry. Like the interstate system has parallel service roads that feed traffic onto high-speed limited access highways, the cyber workforce interstate has feeder institutions that work synergistically to direct students and candidates to appropriate levels of training and education, and ultimately into the workforce. Industry, universities, and community colleges all work together at different levels to contribute to this goal.

How did we get there?

In order to support the newly diversified 21st century career opportunities in northern Louisiana, the CIC recognized the need to organically grow a cyber-skilled workforce. This growth was to be done with collaboration among two- and four-year higher education institutions, industry, government, and K-12 school systems.

There are a variety of education and workforce development pathways available to meet the demands of industry. Some potential employees follow the traditional path of a two- or four-year university, others start school and return later to finish, and yet other experienced workers seek to be retrained in a new industry. The one thing all of those workforce options have in common is that the individual attended a K-12 institution. As such, the CIC established as one of its primary objectives early on, the mission of creating and providing educational opportunities for our K-12 students, the next cyber workforce.

A comprehensive K-12 curriculum

In order to build a sustainable knowledge-based cyber-skilled workforce that can support the needs of government, industry, and academia, the CIC developed a robust Academic Outreach and Workforce Development Program, the National Integrated Cyber Education Research Center (NICERC). NICERC and the educational programs it distributes benefit K-12 teachers by providing dynamic cyber-based curricula resources for the classroom as well as extensive professional development opportunities for educators. These resources benefit students by exposing them to innovative, project-driven learning environments that increase student engagement and content retention. As a result of this program, the community and the nation benefit from a new cyber and STEM (science, technology, engineering, and mathematics) literate workforce that will ensure America's competitiveness and strengthened national security.

In 2012, the Department of Homeland Security's Cybersecurity Training and Assistance Program (CETAP) identified NICERC as their lead technical institute for developing and delivering cyber-themed classroom resources to teachers across the country. NICERC's innovative, cyber-based curricula is available at no cost to any K-12 educator within the United States and its territories.

Over the last 4 years, NICERC content has been made accessible to more than 6,200 teachers in all 50 states and two U.S. territories. Nineteen state departments of education have enlisted help from NICERC to create or implement curriculum frameworks, course standards, or graduation career pathways. Also in that time, NICERC's impact has reached 1.6 million students, many of which have gone on to study cyber engineering in college, obtained workplace-ready credentials and certifications, and even transferred directly into the workplace from high school.

The Cyber Interstate™, illustrated below, outlines NICERC's extensive library of curricula that provides opportunities for students starting in kindergarten through post-secondary education to gain an understanding of cyber issues, engage in cyber education, and provide a foundation for entering cyber-base degree programs and career fields. Cyber Interstate curricula supplies schools with a rigorous program that showcases a systems-level understanding of real-world applications of STEM and builds the foundation for an expansion of cybersecurity knowledge. These project-driven, application-based courses engage students in primary, secondary and post-secondary education.

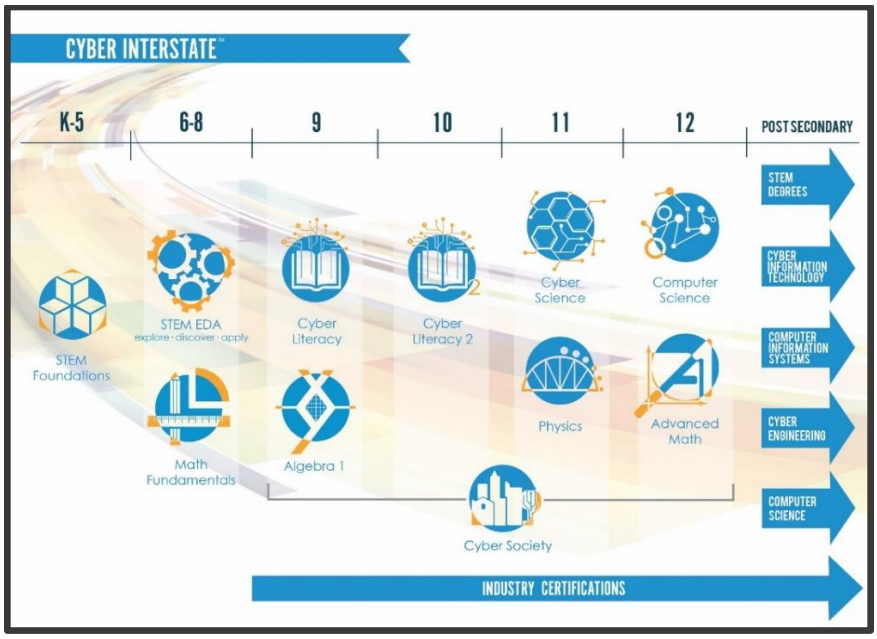

Figure 2. The Cyber Interstate™ K-12 Curriculum

In early 2016, the National Initiative for Cybersecurity Education (NICE) published an updated Cybersecurity Workforce Framework (CWF) aimed at tackling "the challenges of guiding cybersecurity career development and workforce planning" (National Institute of Standards and Technology website, July 7, 2017). Since the release of that document, NICERC has been identifying content area topics from their Cyber Interstate that meet up with the categories, specialty areas, and work roles from the CWF. Of the more than 2000 work roles accounted for in the CWF (work roles consist of job tasks and knowledge, skills, and abilities (KSAs) required to perform tasks), NICERC has content within the high school stage of its Cyber Interstate that touches on almost 300 specific work roles. This means that by introducing high school students to the curriculum provided by NICERC's Cyber Interstate, teachers are taking a proactive approach to preparing the future cyber workforce.

NICERC's professional development opportunities span are available in various cities, nationwide. Teachers gain hands-on experience with projects and technology that provides new, innovative ways to engage students in the classroom. These workshops deliver a hands-on, context-based approach to math and science while incorporating components from the humanities and liberal arts, which allows those teachers to embed the curricula across multiple disciplines and empowers them to prepare students to become the next generation of engineers and cyber professionals. The professional development offered through NICERC delivers a collaborative and comprehensive solution that fosters systemic and sustainable change in the educational environment, thus enhancing the expansion of knowledge among students. NICERC utilizes master teachers, university faculty, and doctoral-degreed educators from regions across the country to support the sustainable and scalable distribution of curricula and professional development. Through NICERC's teacher professional development model,

more students are ultimately impacted (over a greater period of time) than would any program aimed at students alone.

Community Colleges/Universities

Bossier Parish Community College

The mission of Bossier Parish Community College (BPCC) is to promote attainment of educational goals within the community and strengthen the regional economy. This mission is accomplished through the innovative delivery of quality courses and programs that provide sound academic education, broad vocational and career training, continuing education, and varied community services. BPCC provides a wholesome, ethical, and intellectually stimulating environment in which students develop their academic and vocational skills to compete in a technological society.

To achieve its mission of instruction and service, BPCC is committed to the following:

- Offering associate degree programs, one- and two-year occupational certificate programs, and specialized career training.
- Delivering education and training/retraining through technical programs, workforce development, community education, and non-credit courses to serve citizen, business, and industry needs.
- Providing opportunity to earn academic college credits for articulation to other institutions of higher learning.
- Providing developmental studies and remedial programs that enable students to acquire basic skills.
- Utilizing a comprehensive program of student services.

The BPCC Cyber Technology Program aligns with the mission of the College by offering associate degree programs consisting of industry-driven course content that prepares graduates for work in a broad choice of occupations. The program content is experiencing continuous improvement and evolution to keep pace with requirements from cyber business partners. Initiatives by federal and state government, industry sponsors, and other sources contribute to updated lab equipment as well as the completion of other program improvements.

In 2012, the National Security Agency and the Department of Homeland Security named BPCC as a National Center of Academic Excellence in Information Assurance 2-Year Education. BPCC is one of the first 13 schools across the nation awarded this honor. BPCC earned this designation by being a leader in information security education, curriculum development, faculty training, in Northwest Louisiana. BPCC works to foster and create opportunities for interdisciplinary activities, continues to develop and support both credit and continuing education academic programs, facilitates efforts to obtain extramural funding, and serves as a link between the academic and professional communities.

Louisiana Tech University

Louisiana Tech University (LA Tech) is a comprehensive, four-year public research university offering an impressive array of undergraduate and graduate degree programs for citizens of the 21st century and beyond. This includes unique strengths in cyber-fundamentals and cybersecurity education and training. LA Tech also continues to innovate at the intersection of education and training through ongoing cybersecurity curriculum development efforts.

It offers the nation's first four-year undergraduate Cyber Engineering degree, which provides graduates with technology design skills supported by interdisciplinary knowledge of engineering fundamentals, history and ethics, computer science, policy and legal issues, electromagnetic sciences, and mathematics. During the Cyber Engineering program's development, LA Tech faculty and administrators worked in partnership with representatives from multiple federal agencies to understand agency needs and learning objectives for future government employees. The result was an interdisciplinary curriculum, drawn from University's strengths in Computer Science, Electrical Engineering, Mathematics, Physical Sciences, with strategic collaboration with Liberal Arts, Social Sciences and Humanities programs, designed to produce candidates to serve as the future cyber workforce for the nation. LA Tech awarded its first Cyber Engineering degrees in spring 2015. LA Tech's Bachelor's of Science (BS) in Computer Science (CS) can be paired with a concentration in Cybersecurity. The CS program provides a foundational study of the practical and theoretical aspects of computing, and the cybersecurity concentration prepares students to solve network security problems. LA Tech's College of Business offers a BS in Computer Information Systems (CIS) with a concentration in Information Assurance. The CIS curriculum prepares students to conduct work in information technology within the business environment, and the Information Assurance track lays the foundation for work in cybersecurity covering network design and implementation, principles of information assurance, incident response, computer forensics, disaster recovery and business continuity, information systems assurance risk analysis, and cryptography. Figure 1 shows the growth associated with each of the above undergraduate degrees from 2013-2016.

Undergraduate Enrollment				
	2013-Actual	2014-Actual	2015-Actual	2016-Actual
Computer Science (BS)	165	197	275	349
Cyber Engineering (BS)	75	135	149	168
Computer Information Systems (BS)	120	108	104	125
Total	360	440	528	642

Figure 3. Undergraduate enrollment in LA Tech's three BS computing disciplines.

LA Tech also offers innovative graduate programs leveraging interdisciplinary learning and skills development. The College of Business offers an MBA with a concentration in Information Assurance (IA). The graduate IA concentration covers similar topics to the undergraduate IA course sequence at an advanced level. These topics give graduates security skills to take into the business sector with which to improve cybersecurity practices in their organizations of hire. The Ph.D. in Computational Analysis and Modeling (CAM) integrates involvement from the

College of Engineering and Science and the College of Applied and Natural Sciences to produce professionals capable of implementing, analyzing, and evaluating mathematical models using state-of-the-art computing environments and advanced visual data techniques. The CAM program prepares graduates to work in network science, cybersecurity, and big data with a unique foundational knowledge of mathematics and computing. LA Tech's Ph.D. in Engineering with a concentration in Cyberspace Engineering prepares graduates to design and engineer cybersecurity systems, tasks not typically included in traditional cybersecurity degree programs. With the emphasis on design, Engineering Ph.D. graduates are prepared to address the challenges with cybersecurity in design, as well as to contribute to the design of control systems security and more.

Education Program Development

LA Tech is continually looking for innovative, new offerings to increase educational and training opportunities for students in the areas of technology, cybersecurity and cyber engineering. As an example of such pursuits, LA Tech has an Education Partnership Agreement (EPA) with the Defense Cyber Crime Center (DC3) in recognition of the importance of education to the future and economic well-being of the nation. The agreement supports the DC3's goal to encourage the study of cyber and digital forensics science all education levels in the US, and to bring scientific, mathematical and technological experience to universities such as LA Tech. LA Tech is thus exploring the development of tailored educational opportunities to provide students, active service members at the Barksdale Air Force Base and beyond, and veterans, access to high quality cyber education to prepare them for future careers in different intricacies of the discipline.

Centers of Excellence

Along with the BPCC and LA Tech cybersecurity programs mentioned above, the two institutions hold three "Center of Excellence" designations supporting student development and research.

BPCC was named by the National Security Agency and the Department of Homeland Security as a National Center of Academic Excellence in Information Assurance 2-Year Education. BPCC earned this designation by being a leader in information security education, curriculum development and faculty training in Northwest Louisiana. BPCC works to foster and create opportunities for interdisciplinary activities, continues to develop and support both credit and continuing education academic programs, facilitates efforts to obtain extramural funding, and serves as a link between the academic and professional communities.

BPCC also holds the designation as a Center for Workforce Excellence in Cyber Technology issued by the Louisiana Community and Technical College System and the Louisiana Board of Regents. The Center of Workforce Excellence in Cyber Technology has the following noted strengths:

- Fourteen courses align directly to industry-based cyber certifications;

- New content or courses are being added to the curriculum to keep the program current with technology trends;
- Computer information system and cyber programs are Association of Technology, Management, and Applied Engineering (ATMAE) accredited;
- Foundation classes are well-established and faculty and staff are willing to accept change and expand the program;
- Strong industry and community support as evidenced through advisory board participation, new course and program development, and
- Location near several large academic and employer partners.

At LA Tech, the **Center for Information Assurance** is an interdisciplinary research center formed to facilitate research, training, and awareness in Information Assurance in business for Northwest Louisiana and for the United States. NSA and DHS designated LA Tech a National Center of Academic Excellence in Information Assurance Research for academic years 2012-2017. While not formally recognized, LA Tech's **Center for Secure Cyberspace** is an interdisciplinary and interinstitutional entity that assists the faculty members in their research and supporting federal, state, and private sector cybersecurity needs in collaboration with the Cyber Innovation Center. These two centers provide students with an exposure to research addressing real-world problems during the course of their education and contributes to LA Tech's longitudinal approach to student development.

Non-Traditional Student/Veterans

A key ingredient to the workforce which has, and continues to be developed in this region, is training the "non-traditional student/worker." A non-traditional student/worker ranges from someone who never completed their degree to an oil field worker who no longer has a job due to a strained economy, to someone who simply is interested in a career change. Additionally, some of the non-traditional students/workers we encounter do not have the luxury of quitting a job to become a full-time student. Often the goal of the non-traditional student/worker is to become trained as quickly as possible, which means providing the student with multiple access paths to education materials and the minimum requirements to become part of the workforce.

Our region is blessed to be home to Barksdale Air Force Base. Barksdale is not only home to two-thirds of the nuclear triad but also home to many active duty, reserve, and veteran members. Working with our academic partners and Barksdale Air Force Base, the CIC has created a process in which we identify active duty service members prior to the end of their enlistment and align them with a regional cyber company. Some of these service members also have security clearances which meet the needs of some of our local cyber companies. Identifying them prior to their separation date allows us to ensure they have the required certifications and training to enter the cyber workforce immediately upon separation. We also work with Barksdale Air Force Base to engage dependents transferring to Barksdale to determine if their background and interests align with the cyber industry. Finally, the CIC

provides robust support providing veterans with opportunities to obtain appropriate training and education required by the regional cyber companies.

Bossier Parish Community College also has a long-standing partnership with Barksdale Air Force Base and has been named for six consecutive years to the coveted Military Friendly Schools® list (*GI Jobs Magazine*), which honors the top 15 percent of colleges, universities, and vocational schools, that provide outstanding service to military students. Local service members, family members, and veterans continually look to our BPCC for their educational advancement. BPCC's Veteran Educational Services assist students by processing of military education benefits and act as a resource for academic and wrap-around services.

Summary

Despite starting out in a national recession, the CIC over the past 10 years has been able to expand its K-12 cyber curriculum from a program or two that ran only part time in a handful of northern Louisiana schools to content that spans the entire K-12 spectrum and can be found in classrooms from coast to coast. The CIC has expanded the local workforce similarly, creating more than 1,000 high-quality cyber jobs, train a traditional and non-traditional workforce, and assisted in creating the nation's first cyber engineering degree.

By developing an organic cyber workforce, we not only increase tax revenue, lower the unemployment rate, and keep the jobs here, but we also increase the demand signal for more cyber related jobs. In order to successfully replicate these results and growth to other areas of the country, our experience has taught us that to be successful, a region needs the committed support of all local and regional stakeholders. Over the past few years, leadership in cities such as Bossier City and Monroe have purposefully and successfully created opportunities to entice high quality cyber related companies to the region. This has promoted the development of modern facilities and infrastructure as well as continued, compounding support from additional local industry and government.

General Information

1. Are you involved in cybersecurity workforce education or training (e.g., curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides " funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)?

See the above narrative.

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

Teachers are the key to a systemic and sustainable change in cybersecurity education at the K-12 level. NICERC's teacher focused programs allow for the rapid expansion and distribution of cyber-based knowledge, skills, and abilities to K-12 students across the country. One teacher, on average, will educate 122 students in an academic year. By focusing on the development and empowerment of educators, we see an exponential impact among students.

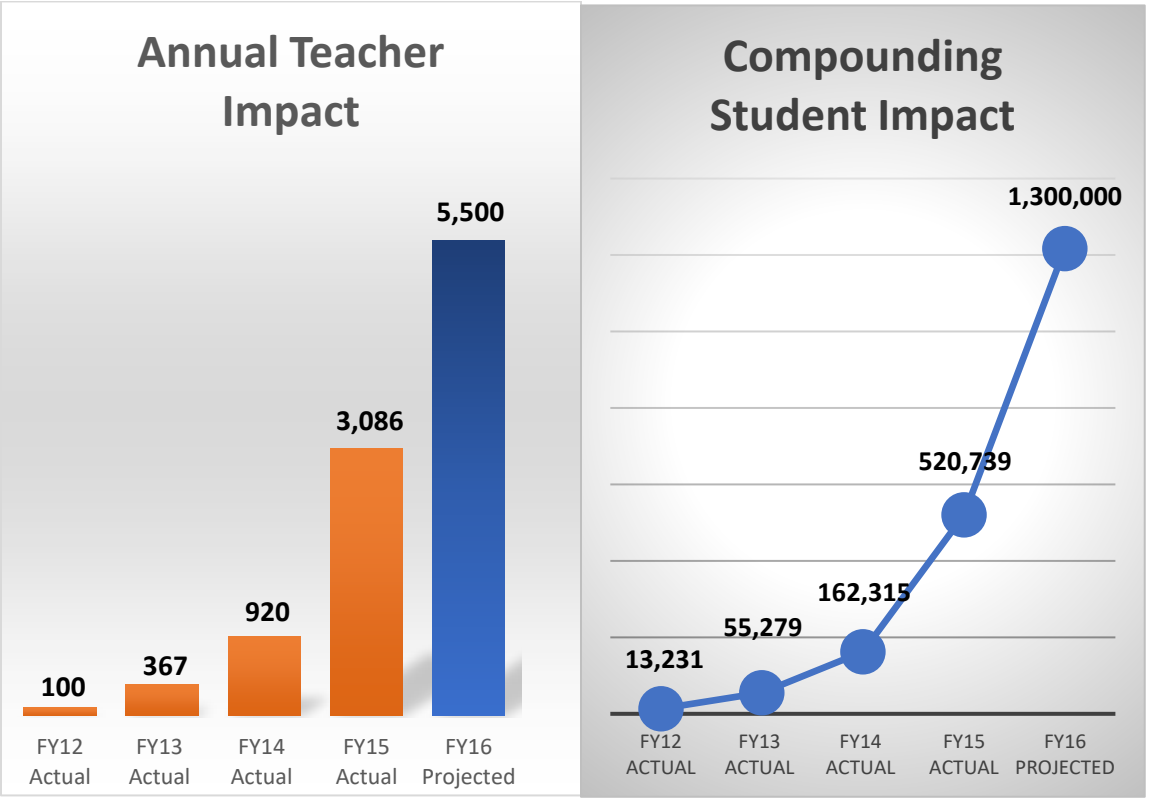

Figure 4. Teacher Impact and Compounding Student Impact

This work is just the beginning of a greater impact needed in cybersecurity education. 52 million K-12 students in the United States and they need to be introduced and brought on to the Cyber Interstate. This foundation provides for the expansion of two- and four-year degree programs, internships, and subsequent decrease in cyber-based job vacancies.

Total Annual Enrollment	2013	2014	2015	2016	2017
AAS Cyber Technology (Net. Sec. & Prog. Analyst)	43	137	165	157	178

Figure 5. Cyber Technology Enrollment

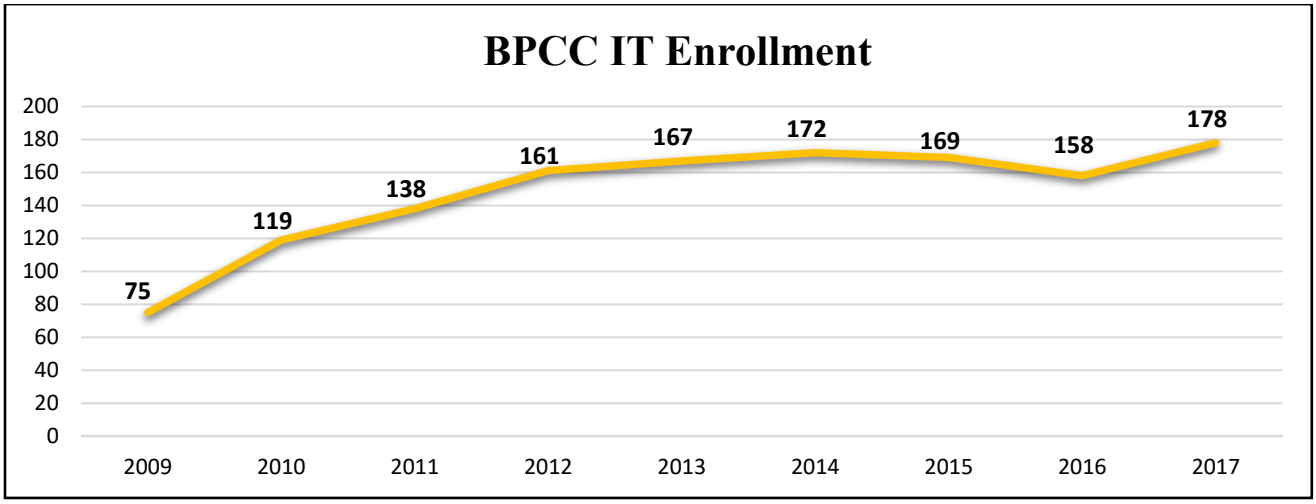

Figure 6. BPCC Information Technology Enrollment

The Associate of Applied Science in Systems Administration was born out of a collaboration with industry partner. The new degree program was recently approved by the LCTCS System and the Louisiana Board of Regents. This program offers two concentrations.

- Concentration in DevOps program provides students with a broad, overarching knowledge of a variety of IT subject areas that brings together development, operations, and testing. DevOps is an interdisciplinary program that requires communication, collaboration, and a broad knowledge so that students understand the full-scope of software delivery.
- Concentration in Enterprise Information Technology & Development program provides students with the skills needed to manage an organization's computer systems. The program prepares individuals to function as entry-level systems administrators and covers analyzing system logs, applying system updates, updating user accounts, troubleshooting problems, and ensuring uptime.

Internships and Employment Rates

For all degree programs in the IT fields, an internship is a requirement for graduation. Using one example, CSRA, since the inception of the Louisiana Economic Development (LED)/CSRA grant on January 2014, a total of 62 BPCC students have either interned or have been hired by

CSRA. Of those 62 BPCC students, 10 students started as interns and were hired by CSRA, 42 were employed by CSRA without interning, and another 10 have interned or are currently interning with CSRA.

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

In Northern Louisiana, the Cyber Innovation Center (CIC) works with its educational partners, local and regional employers to ensure the workforce supply is quantified, met and trained with the current and future needs of the employers. However, understanding and agreement on workforce categories and roles across industry and academia still needs improvement. Since the release of the NICE Cybersecurity Workforce Framework (CWF), NICERC has been identifying content area topics from their curricula that map to the categories, specialty areas, and work roles from the CWF. NICERC has content within the high school stage of its curricula that touches on almost 300 specific work roles within the CWF (work roles consist of job tasks and knowledge, skills, and abilities (KSAs) required to perform tasks). By introducing high school students to the curriculum provided by NICERC's Cyber Interstate, teachers are taking a proactive approach to preparing the future cyber workforce.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

As an organization dedicated to improving the cybersecurity workforce, the CIC and NICERC have established policies that ensure its employees receive regular cybersecurity training. These policies and the associated training focus both on cyber hygiene/awareness of evolving threats and the implementation of IT security procedures and systems designed to improve cybersecurity posture and effectively mitigate risk.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

The CIC, the Bossier Parish Community College (BPCC), North Louisiana Economic Partnership, and industry partners like CSRA have worked to identify the types of cyber jobs employers need and have encouraged the promotion and marketing of our existing high-tech cluster to foster and cultivate a knowledge-based economy. These partnerships have led to increased employment rates for BPCC students as they possess the cybersecurity knowledge and skills valued by employers. The following table outlines some of the promising IT careers in our region:

Current and Future Employment Projections for NW Louisiana					
Job Titles	**SOC Code**	**NAICS Code**	**Demand 2016**	**Expected 2018**	**2 Year Growth**
Cyber Technology					
Software Developers, Applications	15-1132	541511	1,250	1,370	120
Computer Network Support Specialists	15-1152	541511	1,240	1,290	60
Computer User Support Specialists	15-1151	541513	3,810	3,990	190
Information Security Analysts	15-1122	541513	540	590	50
Computer Systems Analysts	15-1121	541513	3,490	3,730	240
Computer Programmers	15-1131	541513	2,700	2,820	120
Database Administrators	15-1141	541513	440	460	20

Figure 7. Employment Projections for Northwest Louisiana

5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

In 2012, the Department of Homeland Security's Cybersecurity Training and Assistance Program (CETAP) identified NICERC as their lead technical institute for developing and delivering cyber-themed classroom resources to teachers across the country. NICERC's innovative, cyber-based curricula is available at no cost to any K-12 educator within the United States and its territories. Over the last 4 years, NICERC content has been made accessible to more than 6,200 teachers in all 50 states and two U.S. territories. Nineteen state departments of education have enlisted help from NICERC to create or implement curriculum frameworks, course standards, or graduation career pathways. Also in that time, NICERC's impact has reached 1.3 million students, many of which have gone on to study cyber engineering in college, obtained workplace-ready credentials and certifications, and even transferred directly into the workplace from high school.

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

The cyber landscape is constantly shifting which requires cyber industries to stay at or above pace of the shifting landscape. This, of course, trickles down to cyber education and training programs. Educational intuitions must stay in constant engagement with their industry partners to ensure the education and training programs are aligned with this ever-changing industry and workforce needs.

7. How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

While it is not possible to accurately predict the specific labor needs that will accompany the development of a sector as broad and innovative as security of cyber physical systems, the solution is to rethink the approach such that the innovation driving that sector is increased rather than hindered. The implementation of NICERC curricula is one example of how driving broad, cyber-based fundamentals throughout grades, levels, and institutions can broaden the pipeline as wide as possible and educate a citizenry that helps and does not hinder cybersecurity efforts. Curriculum development needs to evolve and become agile, to react quickly to industry needs based on innovation and tech disruption such as AI, IoT etc…. As technologies, techniques and practices emerge, curriculum needs to align and provide education on standards, technologies and best practices to facilitate student engagement and success.

Content provided by NICERC's Cyber Interstate is available to teachers through a digital learning management system (LMS). When a teacher gains access to the LMS, they have the ability to log in at any time to observe changes to, additions to, or deletions from the content. The use of this digital LMS was predicated on the fact that the content being presented will be focused on current and emerging technologies, and as a result, if it were prepared in print format, would most likely be out of date before it ever got to the classroom. Consequently, by employing a digital distribution service, NICERC authors and subject matter experts are able to update the content as technology and real-world applications evolve. They can revise projects based on emerging knowledge or alter lesson materials to include relevant current events. Simply put, even the technology in our hands is out of date soon after becoming available. By providing materials to teachers that can be distributed digitally and immediately, NICERC makes every attempt to ensure that the educated workforce resulting from interaction with Cyber Interstate content is the most well-prepared applicant for each job or degree program.

One role of advancing technology will be to spur a shift in the areas of greatest economic activity, meaning that as technological advances are applied in society, prominent labor categories will shift, and jobs that were reliable will disappear. The key to a successful transition will be taking advantage of this opportunity to drive innovation in new sectors, rather than trying to sustain support for those that are being made obsolete by technological advances. As these shifts manifest, the need for a large adaptable cyber workforce will not disappear. Adapting the early education to prime students for cyber careers as well as creating training programs/educational opportunities to help workers transition in to a cyber career will widen the cyber workforce pool, contribute to the adaptability of the workforce, and bring broad perspectives and skillsets from other sectors into the cyber workforce. The added richness of experience of workers re-training to cyber careers can act as an additional driving force for innovation in the sector.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

The cybersecurity workforce development that the CIC and specified entities have been building for the past decade has hinged on their ability to explore collaborative solutions to this multifaceted, long term issue. No one specific program has been key in turning the tide for cyber workforce development, but continual partnership across government, industry, and academic institutions was required to build the web of supporting structures that provide accessible entry pathways for individuals to join the cyber workforce. For one individual to successfully enter the cyber workforce, they must possess skills required by government and industry, and so must have received training and education that address those specific requirements. Communication between government, industry, and educational institutions is required to design those training and educational programs. A high level of interoperability and coordinated efforts between these entities is required to achieve a setting where achieving computer literacy in K-12 is the standard, postsecondary STEM programs are accessible and entry is encouraged, and jobs in technology are available locally. The goal of cybersecurity workforce development is the creation of life pathways that flow naturally into a cyber career, and this is achieved with the development of an environment where as much as possible the bars to educational access and workforce entry are removed.

i. At the Federal level?

At the Federal level, partnership between agencies involved in government cybersecurity and academia will be necessary. Currently, DoD has its own training programs in cybersecurity, and they are focused heavily in practical applications. While this is effective for preparing workers for specific roles, it is missing the component of cutting edge scientific research. Cyber security is at its core an evolving and innovative sector, and training programs could increase effectiveness if they were able to integrate scientific exploration and to push the boundaries for latest methods. The practical methods that have been codified into training programs grow out of date quickly.

Establish a national initiative to focus on cybersecurity education that would expand programs like the DHS Cybersecurity Education and Training Assistance Program (CETAP) to ensure every community has access to cyber curricula, classroom resources, and teacher professional development. By next year, the CETAP program will have successfully reached approximately 2M of the 52M K-12 students in the U.S. To effectively address our national cybersecurity workforce shortages, we need to significantly increase the cyber focus and investment in our K-12 student pipeline. Programs like CETAP provide a scalable, effective model that can build the cybersecurity workforce foundation we need to ensure our economic and national security in the 21st century.

ii. At the state or local level, including school systems?

Encourage state and local Departments of Education to develop pathways, frameworks, and standards that recognize the importance of cyber across all educational disciplines and minimize administrative/bureaucratic barriers limiting educator's ability to incorporate cyber related lessons in the classroom.

Additionally: !

· Computer science needs to be included as a standard part of the core curriculum, beginning early and being treated as one of the basic sciences. !

· Computer literacy needs to be established in K-12, and STEM education needs to prepare students to pursue further education and then work in technical fields. !

iii. By the private sector, including employers?

Participation from industry in cooperative efforts for workforce development is a key component in the successful operation of public-private partnerships in the manner we have described in the narrative. Much expertise in cybersecurity is developed in, and to a large extent contained within, the private sector. One challenge is finding a way to share that knowledge and the skill of industry professionals with the public sector in a way that stimulates economic development to the benefit of both parties. This process requires a tremendous level of communication between parties, and it involves openness and respect for differing, though compatible, missions, purposes, and visions across the partner entities.

Another area where the private sector can play a large role in improving the security environment is in the sustained practice of responsible cybersecurity stewardship in the creation of systems designed with security ingrained. This is a significant issue with the growing internet of things (IoT), and one that will not be resolved until industry addresses the intrinsic security and privacy needs that accompany the smart devices so interwoven with the human and physical world.

iv. By education and training providers?

Provide cyber curricula that is mapped to national and state standards, developed with pedagogical rigor, is multi-disciplinary, and delivered via project based learning. The curricula and related hands-on projects should also be frequently updated to ensure the educational outcomes keep pace with today's rapidly evolving cyber landscape.