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

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;

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.