Cybersecurity Education Management Council

Status Report to the Louisiana Senate Education, Senate Finance, House Education and House Appropriations Committees

FEBRUARY 2025

REGENTS

BOARD *of* REGENTS
STATE OF LOUISIANA

Table of Contents

Executive Summary

Act 57 of the 2020 Regular Legislative Session, authored by Senator Mark Abraham, commissioned the Cybersecurity Education Management Council and created the Louisiana Cybersecurity Talent Initiative Fund. Under the auspices of the Louisiana Board of Regents, the Cybersecurity Education Management Council is tasked to do the following:

- Advise and make recommendations to the Louisiana Board of Regents with respect to distributions from the Fund;

- Annually review the list of degree and certificate programs upon which the distribution is based and the final distribution amounts; and

- Provide updates on the work of the Council, recommendations, distribution of funds, and the distribution impact on the workforce.

The Council is comprised of 11 members including the Commissioner of Higher Education, two members appointed by the Governor, a representative from the Louisiana Department of Education with expertise in science, technology, engineering, and mathematics education appointed by the state superintendent of education, president of the Louisiana Chemical Association, president of the Louisiana State University System, president of the University of Louisiana System, president of the Southern University System, president of the Louisiana Community and Technical College System, secretary of the Louisiana Workforce Commission, and secretary of the Louisiana Department of Economic Development. Vacancies in the membership of the Council are filled in the same manner as the original appointment.

The purpose of the Louisiana Cybersecurity Talent Initiative Fund is to provide a mechanism for donations and/or appropriations of funding for degree and certificate programs in cybersecurity fields offered by public postsecondary education institutions in order to meet the state's workforce needs. Cyber threats persist across every industry sector and domain and cyberattacks are a national security concern. Incidents like recent high-profile attacks on several Louisiana educational institutions underscore the real impacts and importance of cybersecurity to the state. Confronting these threats demands a well-trained, skilled workforce; however, the nation faces a critical shortage of security professionals for current and near-term challenges. Through programmatic support to public postsecondary institutions, the goal of the fund is to develop, train, produce, and retain Louisiana's workforce-ready cybersecurity professionals and improve cyber literacy across industry sectors.

A major milestone in 2024 was the establishment of the Louisiana Cyber Academy, a collaborative effort among six institutions to expand cyber instruction accessibility statewide. While this initiative, along with seven funded awards totaling $1,000,000, represents significant progress, more work remains to meet the growing workforce demands. Current data show over

3,000 cyber job openings in Louisiana, highlighting the continued need for expanding cybersecurity education and training capacity.

The Cybersecurity Education Management Council advises and makes recommendations to the Louisiana Board of Regents related to the distribution of monies appropriated to the Louisiana Cybersecurity Talent Initiative Fund and approved funds are transferred by the Regents to the receiving institutions. Eligibility for funding requires each participating institution to secure matching support equal to at least 25% of the amount of state funding to be distributed. The match provided may include, but is not limited to cash, in-kind donations of technology, personnel, construction materials, facility modification, corporeal property, internships, scholarships, sponsorship of staff or faculty, and faculty endowment proceeds.

As required by Act 57, this report provides an update on the work of the Council, emerging initiatives, distribution of funds, workforce impacts from distribution, and recommendations.

Since its first meeting in September 2020, the Council has reviewed the landscape of existing and emerging cybersecurity initiatives, created a workgroup, and proposed a plan with milestones for current and future fiscal support. In 2024, seven awards were made and the full $1,000,000 allocation distributed to launch new or support existing cybersecurity programs.

List of Acronyms

BOR   Louisiana Board of Regents

CEMC   Cybersecurity Education Management Council

LDOE   Louisiana Department of Education

LED   Louisiana Economic Development

NICE   National Initiative for Cybersecurity Education

NIST   National Institute of Standards and Technology

RFA   Request for Applications

Part I: Introduction

This report, filed pursuant to Act 57 of the 2020 Regular Session of the Louisiana Legislature, highlights the significant progress made by the Cybersecurity Education Management Council (CEMC) in 2024.

The CEMC mission and primary objective guided the work of the Council during the creation and implementation of a distribution process for the Louisiana Cybersecurity Talent Initiative Fund.

- **Mission:** Increase cybersecurity talent output for Louisiana industries.

- **Objective:** Accelerate cybersecurity talent development by initiating measurable, targeted, and practical program support for postsecondary institutions.

In 2020, the Council set an ambitious and intentional timeframe to implement a distribution process. This process included creating a Request for Applications (RFA) to solicit innovative cybersecurity initiatives, awarding available funds on a merit basis to eligible institution(s), and implementing approved projects following funding approval by the Board of Regents. The 2024 funding cycle utilized this process in selecting the seven funded projects. The following section will focus on the successes achieved by the CEMC in 2024.

Part II: Advancing Louisiana's Cybersecurity Ecosystem: 2024 Progress and Achievements

Council Meetings

During its 2024 quarterly meetings, the CEMC continued to consider the charges of Act 57, assessing the success of previous funding and implementing the next competitive cycle. The primary focus of the Council was to ensure that the Louisiana Cybersecurity Talent Initiative Fund continues to work as intended and produce the needed results.

Recap of 2024 Meetings:

- **February 19, 2024**: Dr. Tristan Denley was elected as chair and new Council members were introduced. The Council also discussed implementing additional reporting requirements for future funding cycles.

- **April 9, 2024**: The Council approved recommendations to fund in 2024 one sustained program and six new programs for a total of $949,777. Remaining funds of $50,223, available after all recommended projects were funded at the amount requested, were provided to the Louisiana Cyber Academy initiative at Bossier Parish Community College.

- **December 4, 2024**: Additional reporting metrics were approved for awarded institutions, along with the 2024-25 RFA and deadlines. The FY 2024-25 RFA was published on December 19, 2024. The Council received updates on new cyber training opportunities, including GOHSEP-funded regional cyber academies and a Board of Regents grant from the National Association of System Heads, in partnership with Google, to deploy micro-credentials for faculty, staff, and students at Louisiana public institutions. Industry partnerships were highlighted, including Splunk Academy access for participating institutions and AWS credentials available through Louisiana Tech.

Additional information, including meeting minutes, can be found on the Cybersecurity Education Management Council's **website**.

Cybersecurity Activities and Accomplishments

The following sections highlight the progress of the Council, stakeholders, and stakeholder agencies.

Fund Distribution Process

The creation of the Cybersecurity Talent Initiative Fund distribution process resulted from Council discussions, relevant feedback, and ongoing collaborations. It began with group assessments of cybersecurity data from multiple sources along with reports including the NIST Cybersecurity Framework (nist.gov), the Cybersecurity and Infrastructure Security Agency's NICE Cybersecurity Workforce Framework (cisa.gov), and the ISC2 Cybersecurity Workforce studies for 2019 and 2020. The result was a request for applications (RFA) process to solicit innovative solutions from Louisiana's public postsecondary institutions and provide funds on a competitive basis, using a rubric published in the RFA. Key elements of the RFA are project requirements, metrics and reporting, project tracks, eligibility, and the application review process.

Project Requirements

Project requirements inform interested parties that applications must:

- Focus on professional development of new and/or incumbent cybersecurity workforce participants;
- Detail pathways to employment with industry, including specific employers and roles/competencies where possible;
- Detail monitoring and reporting of any students, graduates, or participants who secure internships, apprenticeships, or jobs;
- Include validation of at least 25% private or non-public funds provided as match;
- Detail all tracks for students (minors/majors), graduates, and learners;
- Align closely to industry and cybersecurity practitioner-recognized standards such as professional certifications or certificate programs;
- Detail alignment to the NIST Cybersecurity Framework and/or NICE Cybersecurity Workforce Framework (e.g., Categories or Work Areas);
- Support directly the participation and success of underrepresented groups (i.e., African American, women, Spanish/Hispanic/Latino, and other students of color) in pathways and employment opportunities; and
- Articulate potential follow-on grant opportunities and/or federal, private, or other support to ensure sustainability.

Metrics and Reporting

Applications also must detail and subsequently report the following metrics and methods:

- The number(s) of potential candidates at the end of the project including students, graduates, or participants in mentorships, internships, externships, apprenticeships, job offers, or jobs;
- Other indicators of hireability or possible employment including, but not limited to, letters from industry confirming workforce readiness;
- Measures of student or learner engagement with industry such as hiring events, interviews, total time (hours) of training programs, and any/all indicators that further illustrate student-industry connection;
- Student/learner demographics or other indicators of support of or participation by historically underrepresented groups (i.e., African Americans, women, Spanish/Hispanic/Latino, and other students of color); and
- The degree, certificate, or certification programs supported by the project, and credentials awarded, if applicable.

Projects supported by the Fund should be cybersecurity-relevant, enhance degree programs or be closely aligned with recognized industry cybersecurity practices, like certifications or certificates, be measurable and practical, encourage close coordination with industry to ensure alignment, and emphasize cybersecurity talent development and retention across all postsecondary education and beyond, providing opportunities for reskilling, upskilling, and skills refinement. For guidance, applicants are strongly encouraged to refer and adhere to the principles of both the NIST Cybersecurity Framework (nist.gov) and the Cybersecurity and Infrastructure Security Agency's NICE Cybersecurity Workforce Framework (cisa.gov), which reflect current and evolving best practices in cybersecurity.

Project Tracks

Two tracks for project work were identified in the RFA: (1)

- Track 1: Student Projects
- Track 2: Incumbent Workforce and Education Projects.

Track 1 projects build awareness and foundational cybersecurity skills by translating industry cybersecurity challenges, needs, and opportunities into impactful programs to prepare students and graduates for cyber-related job opportunities. These projects may address any industry dimension of cybersecurity (e.g., from business to technical) and may include:

- Adding measures of competency to existing programs;
- Supporting third-party professional or association certifications and undergraduate certificates;
- Developing work-based and other experiential learning opportunities;
- Creating new programs targeted to cybersecurity and related disciplines;
- Preparing students for and recruiting students into cyber-related jobs and industries;
- Enhancing and refining channels of industry engagement around cyber-specific skills;
- Supporting research and/or faculty with direct and measurable impact on the production of cyber-fluent, workforce-ready candidates;
- Developing innovative approaches to directly support the participation and success of underrepresented groups (i.e., African Americans, women, Spanish/Hispanic/Latino, and other students of color) in pathways and employment opportunities;
- Developing innovative approaches to directly support the participation and success of military veterans in pathways and employment opportunities; and/or
- Providing pathways for graduates with higher-level degrees (master's and above) to transition into cybersecurity education and instruction.

Track 2, Incumbent Workforce and Adult Education Projects, translate industry cybersecurity challenges, needs, and opportunities into programs to establish and enhance skills for current and emerging opportunities in cybersecurity. These projects may address any industry dimension of cybersecurity (e.g., from business to technical) and may include:

- Reskilling/upskilling/skills refinement or competency-based programs;
- Establishing or accelerating certification or certificate opportunities for incumbent workers and adult learners transitioning to cybersecurity careers;
- Establishing or accelerating certification or certificate opportunities for incumbent workers and adult learners to pursue degrees in cybersecurity-related fields;
- Creating new business opportunities for existing employers through skills enhancement;

- Building new measurable pathways from one industry to another in areas of cybersecurity;
- Working with industry partners on new or enhanced workforce-ready programs;
- Establishing or improving wraparound service models to maximize participant or candidate engagement;
- Developing innovative approaches to directly support the participation and success of underrepresented groups (i.e., African Americans, women, Spanish/Hispanic/Latino, and other students of color) in pathways and employment opportunities;
- Developing innovative approaches to directly support the participation and success of military veterans in pathways and employment opportunities;
- Identifying and (re)engaging candidates who left the workforce to underscore job opportunities in cybersecurity fields; and
- Providing pathways for graduates with higher-level degrees (master's and above) to transition into cybersecurity education and instruction.

Application Review Process

The application review process requires that all submissions be assessed by the members of the Cybersecurity Education Management Council (CEMC). Each member individually assesses the projects, then the Council collectively ranks applications and develops final funding recommendations. After recommendations from the Council are submitted, the Board of Regents determines which applications will be funded based on the competitive review process and funds available.

2023-24 Funded Programs

The following programs were approved for funding in 2024:

Sustained Programs (Track I):

- Northwestern State University (Central Louisiana Cybersecurity Talent Enhancement Program): $30,000

New Programs (Track II):

- Bossier Parish Community College – Establishing the LA Cyber Academy – $260,223
  - Bossier Parish Community College serves as the fiscal agent for the Louisiana Cyber Academy, a collaborative initiative among Louisiana institutions focused on expanding the accessibility of cyber instruction statewide. The six institutions involved in the

Academy collaborative are Baton Rouge Community College, Bossier Parish Community College, Grambling State University, LSU Shreveport, Nicholls State University, and Southern University at New Orleans. The Academy coordinates shared curriculum development and delivery to increase cybersecurity education access across Louisiana.

- Nicholls State University – Maritime Cybersecurity at Nicholls State University – $94,125
- Southern University A&M – Empowering Cybersecurity Leaders by Establishing an Executive Master's Program in Cybersecurity, and Offering Mentorship Programs and Industry-Partnered Certificates – $185,810
- University of New Orleans – Development of an Advanced Cybersecurity Certificate Program – $95,773
- Fletcher Technical Community College – Enhancing Experiential Learning to Increase Workplace Readiness of Cybersecurity Students – $220,000
- McNeese State University – To Create Bachelor of Science Degree in Computer Science with Cybersecurity Concentration at McNeese State University – $114,069

Results to Date

In response to the significant demand for cybersecurity talent across Louisiana, cyber program offerings continue to expand throughout the state, driving increased student enrollment and workforce entry. The December 2023 Board of Regents approval of 24 Universal Transfer Pathways, including a dedicated Cybersecurity pathway, has streamlined students' progression from two-year associate's degrees to four-year baccalaureate programs while preserving earned credits. Since the establishment of the Cybersecurity Education Management Council and Cybersecurity Talent Initiative Fund, completions of cyber-related credentials have surged by more than 80%. New degree programs have begun at Fletcher Technical Community College, and Southern University at New Orleans. Building on this momentum, in 2024 the Louisiana Cyber Academy was established through a formal cooperative academic arrangement among six Louisiana institutions, focused on expanding cyber instruction accessibility statewide. The Academy's curricular oversight committee has already identified its inaugural course offerings that will begin in Spring 2025, including Information Technology Principles and Problem Solving and Programming Techniques, with plans to expand both course offerings and institutional partnerships. These coordinated initiatives, coupled with growing job opportunities and industry interest, are accelerating the development of Louisiana's cybersecurity talent pipeline.

Part III: Policy/Funding Recommendations and Summary

Recommendations and Summary

Act 57 of the 2020 Regular Session of the Louisiana Legislature established a foundation to address the growing demands for a robust Louisiana cybersecurity workforce. This law established the Louisiana Cybersecurity Talent Initiative Fund and the Cybersecurity Education Management Council (CEMC) to create a process that guides public postsecondary institutions as they respond to the cybersecurity needs of the state and the demand for workforce.

As stipulated in Act 57, CEMC will continue to build on its success and advance cybersecurity education efforts in Louisiana. Its achievements in raising awareness and promoting cybersecurity in Louisiana would not have been possible without the collective and collaborative efforts of Council members, other stakeholders, and institutions establishing and growing responsive credential programs.

The impact of these efforts is evident in the data. Since 2020, the Board of Regents' strategic investments have driven a more than 80% increase in cyber graduates, improving the supply/demand ratio for cybersecurity professionals from 60% in 2020 to 81% today (Cyberseek.org). However, with over 3,000 current cyber job openings and 2,700 unfilled positions in computer science in Louisiana, continued investment in and expansion of cybersecurity education and training programs remain critical.

Since the first CEMC meeting in September 2020, the Council has worked to ensure the Louisiana Cybersecurity Talent Initiative Fund generates the highest return on investments in cybersecurity education and training. The competitive process designed to solicit, assess, and fund applications has led to significant advances in programs and campus capabilities. In 2024, the Council strengthened its impact through enhanced reporting metrics for funded institutions and continued to receive funding requests for both new and sustained programs, demonstrating the persistent demand for cybersecurity education and training across higher education institutions.

A major milestone was achieved with the establishment of the Louisiana Cyber Academy, a formal cooperative arrangement among six institutions focused on expanding cyber instruction accessibility statewide. This initiative, combined with new partnerships including GOHSEP-funded regional cyber academies and industry collaborations with Splunk and AWS, has expanded training opportunities throughout Louisiana. Additionally, the Board of Regents' partnership with the National Association of System Heads and Google is enabling the

deployment of innovative micro-credentials for faculty, staff, and students at Louisiana public institutions.

The Cybersecurity Talent Initiative Fund continues to prove its value in improving and expanding program offerings and cybersecurity training opportunities for both students and incumbent workers. The establishment of a Cybersecurity Universal Transfer Pathway, paired with CTIF's sustained investments and growing industry partnerships, is strengthening the educational pipeline, meeting critical workforce demands, providing meaningful 21st-century opportunities for Louisiana students and residents, and solidifying Louisiana's position as a national leader in cybersecurity education and workforce development.