CYBERSECURITY EDUCATION MANAGEMENT COUNCIL

STATUS REPORT TO THE LOUISIANA SENATE EDUCATION, SENATE FINANCE, HOUSE EDUCATION AND HOUSE APPROPRIATIONS COMMITTEES

LOUISIANA BOARD OF REGENTS

JANUARY 2023

TABLE OF CONTENTS

Executive Summary

Act 57 of the 2020 Regular 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 members of the Council elect the chair, vice-chair, and other officers as they consider necessary. 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 shall be 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. Cyber attacks on critical infrastructure are a national security concern. Incidents like the high-profile cyber attacks on several Louisiana educational institutions underscore the real impacts and importance of cybersecurity to the state. Confronting these threats demands well-trained individuals; however, the nation faces a critical shortage of security professionals for current and near-term challenges. By providing 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.

The Cybersecurity Education Management Council advises and makes recommendations to the Louisiana Board of Regents related to the distribution of the Louisiana Cybersecurity Talent Initiative Fund. Funds are distributed by the Board of Regents to the receiving institutions via contracts. Eligibility for funding requires the campus to secure matching funds of no less than 25 percent of the amount of 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, or faculty endowment.

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. The Cybersecurity Education Management Council is required to meet quarterly each year. Since its first meeting in September 2020, the Council has reviewed the current landscape of existing and emerging cybersecurity initiatives, created a workgroup, and proposed a plan with milestones for current and future fiscal support. In 2022, four awards totaling the full $1,000,000 allocation were provided 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 the Cybersecurity Education Management Council (CEMC) achieved in 2022.

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 2022 funding cycle utilized this process in selecting the four funded projects. The following section will focus on the successes achieved by the CEMC in 2022.

Part II: A Successful Year of Engagement in Cybersecurity in Louisiana

Council Meetings

During its 2022 quarterly meetings, the CEMC continued to consider the details of Act 57 of the 2020 Regular Session, in assessing the success of the first funding year and planning for the second competitive cycle. The main focus of the Council was to ensure the distribution process for the Louisiana Cybersecurity Talent Initiative Fund had worked as intended in the first year.

Recap of Quarterly Meetings:

- **January 25, 2022**: Presentation by Dr. Susie Schowen on Louisiana Economic Development's Good Job Challenge grant submission; progress reports from three 2021 CEMC recipients (University of Louisiana at Lafayette, Southern University and A&M College, and Northwestern State University); and review of the RFA for the 2022-23 grant cycle.
- **May 5, 2022**: Approval of 2022 funding recommendations; update from Dr. Schowen on Good Job Challenge grant submission.
- **August 9, 2022**: Participation in the Louisiana Office of Technology's and Louisiana National Guard's Cyber Incident informational session.
- **November 9, 2022**: Reviewed 2023 RFA content, provided feedback, and approved content to finalize the RFA, pending available funds.

Additional information 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 resources along with reports such as the NIST Cybersecurity Framework (nist.gov), the Cybersecurity and Infrastructure Security Agency's NICE Cybersecurity Workforce Framework (cisa.gov), and the ISC^2 Cybersecurity Workforce study for 2019 and 2020. The result was a request for applications (RFA) approach that solicits innovative solutions from Louisiana's public postsecondary institutions and provides 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. Match may include, but is not limited to, cash, in-kind donations of technology, personnel, construction materials, facility modification, or corporeal property, internships, scholarships, sponsorship of staff or faculty, or faculty endowment;
- 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 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 hire-ability 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 American, 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) Student Projects and (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. Track 1 projects may address any industry dimension of cyber (e.g. from business to technical) and may include:

- Adding measures of competency to existing programs;
- Supporting 3rd-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 American, 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 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. Track 2 projects may address any industry dimension of cyber (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 American, 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 Veterans in pathways and employment opportunities;
- Identifying and (re)engaging candidates that left the workforce to underscore job opportunities in cybersecurity fields;
- Providing pathways for graduates with higher-level degrees (Masters 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 will individually assess, collectively rank applications, and then provide 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.

2021-22 Funded Programs

Per recommendations of the CEMC, as approved by the Board of Regents, the following programs were approved for funding in 2022:

- Louisiana Tech University (Cybersecurity Talent Expansion Program): $331,623
- Louisiana State University and A&M College (FIREStarter 2L Developing Cyber Talent with Hands-on Experiences in Digital Forensics and Industrial Control Systems): $344,397
- Southern University System (Cybersecurity Talent Initiative Program SUS-CyberTIP): $242,181
- Bossier Parish Community College (Accelerated Cyber Technology Training ACTT): $81,799 ($66,040 requested plus additional $15,759 to support Fletcher Technical Community College's adoption/adaptation of the BPCC program)

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 meet the growing demands of Louisiana's cybersecurity workforce. This bill established the Louisiana Cybersecurity Talent Initiative Fund and the Cybersecurity Education Management Council (CEMC) to create a process that guides public postsecondary institutions possessing innovative and effective cybersecurity solutions in expanding their reach and responding to the needs of the state.

As stipulated in Act 57, the Cybersecurity Education Management Council will build on its success over the past two years and continue to 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 all Council members and other stakeholders.

Since the first CEMC meeting in September 2020, the Council has worked to ensure the Louisiana Cybersecurity Talent Initiative Fund is distributed in a way to bring the highest returns for the investments provided in terms of cybersecurity education and training. The competitive process designed to solicit, assess, and fund applications has worked well and led to significant advances in the programs and on the campuses affected. In 2022, funding was provided to assist one institution in creating a modified version of another campus's program: a significant sign of the scalability and sustainability of these efforts. The Cybersecurity Talent Initiative program has proven to be a success and promises to help Louisiana improve and expand its program offerings and cybersecurity training/retraining opportunities for both students and incumbent workers. The program's continued investments will strengthen educational and business/industry partnerships, meet the remarkable workforce demand in the field, provide significant 21st-century opportunities for Louisiana students and residents, and elevate Louisiana as a national leader in cybersecurity.