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

LOUISIANA BOARD OF REGENTS

JANUARY 2021

TABLE OF CONTENTS

Executive Summary......3

List of Acronyms......5

Part I: Introduction......6

Part II: A Successful Year of Engagement in Cybersecurity in Louisiana......7

Council Meetings......7

Cybersecurity Activities and Accomplishments......7

Fund Distribution Process......8

Part III: Policy/Funding Recommendations and Summary......13

Recommendations and Summary......13

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 chairman, vice-chairman, 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, representative appointed by the state superintendent of education from the state Department of Education with expertise in science, technology, engineering, and mathematics 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 demand 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 as it pertains to the distribution of the Louisiana Cybersecurity Talent Initiative Fund. This fund will be distributed by the Board of Regents to the public postsecondary education management boards on behalf of the receiving institution. Distribution of available funds requires a match 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, or 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 impact 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 reviewed the current landscape of existing and emerging cybersecurity initiatives, created a workgroup, and proposed a plan with milestones for 2021.

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 Application

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 since its establishment.

The CEMC mission and primary objective guide 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.

The Council set an ambitious and purposeful timeframe to implement a distribution process. Part of this process includes creating a Request For Application (RFA) to solicit innovative cybersecurity proposed initiatives, award available funds to public postsecondary institution(s), and begin implementing approved projects during 2021. The following section will focus on the great success that the CEMC has achieved since its first meeting in September 2020.

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

Council Meetings

During the 2020 quarterly meetings, the CEMC reviewed and discussed the details of Act 57 of the 2020 regular session. Since the first CEMC meeting was held in September 2020, the main focus of the council was to establish and maintain a distribution process for the Louisiana Cybersecurity Talent Initiative Fund. Two additional quarterly meetings were held that helped pave the way for the creation of an RFA and an established distribution process.

Quarterly Meetings

- **September 17, 2020**: Council member introduction, review of Act 57, and election of Mr. Greg Trahan as chair and Mrs. Susie Schowen as vice-chair
- **November 17, 2020**: CEMC mission and objective, approach to identify cybersecurity needs and development of an RFA
- **January 26, 2021**: Reviewed RFA content, provided feedback, and approved content to finalize an RFA, pending available funds

2021 Upcoming Meetings

- **2nd Quarter:** Tuesday, April 13, 2021
- **3rd Quarter:** Wednesday, July 14, 2021
- **4th Quarter:** Tuesday, October 12, 2021

Additional information can be found on the Cybersecurity Education Management Council **website**.

Cybersecurity Activities and Accomplishments

The following sections will highlight the progress of the Council, stakeholders, and agencies vital to its success.

Fund Distribution Process

The creation of the Cybersecurity Talent Initiative program was a result from Council meetings, relevant feedback, and ongoing collaborations. It began with group assessments and discussions involving cybersecurity data from multiple resources and 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. Following the first CEMC meeting of September 2020, the Council determined to begin drafting an RFA to solicit innovative solutions from Louisiana's public postsecondary institutions. Key topics identified within the RFA include 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 development of new and/or incumbent cybersecurity workforce;
- 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 as match to include, but 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, or learners for reporting;
- Align closely to industry and cybersecurity practitioner-recognized standards such as professional certifications or certificate programs;
- Detail alignment to NIST Cybersecurity Framework and/or NICE Cybersecurity Workforce Framework (e.g. Categories or Work Areas);

- 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;
- Articulate potential follow-on grant opportunities/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 connectivity;
- 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).
- The degree, certificate, or certification programs supported by the project, and any 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 to 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 were identified in the RFA as (1) Student Projects and (2) Incumbent Workforce and Education Projects. Track 1, Student Projects, should 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; and/or
- 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;
- Providing pathways for graduates with higher-level degrees (Masters and above) to transition into cybersecurity education and instruction.

Track 2, Incumbent Workforce and Adult Education Projects, should 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; and/or
- 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 applications submitted will be reviewed by the Cybersecurity Education Management Council (CEMC). Each member will individually assess, collectively rank applications, and then provide final recommendations for funding submissions. After recommendations from the Council are submitted, the Board will make final determinations of which applications will be funded based on the competitive review process.

Proposed Timeline

The proposed timeframe for soliciting applications, reviewing, approving, and distributing funds is as follows:

- February 8, 2021 - Request for application issued
- April 23, 2021 - Last day that applicants may ask questions about the RFA
- April 16, 2021 - RFA submission deadline
- April 17 – 22, 2021 - Applications reviewed by CEMC
- April 26, 2021 - Reports and recommendations of CEMC provided to the Board
- April 30, 2021 - Final action by the Board
- May and June 2021 - Contracts negotiated and executed

Part III: Policy/Funding Recommendations and Summary

Recommendations and Summary

As part of Act 57 of the 2020 Regular Session of the Louisiana Legislature, the ongoing work of the Cybersecurity Education Management Council will continue to advance cybersecurity efforts in Louisiana. The achievements in raising awareness and promoting cybersecurity for Louisiana would not have been possible without the collective efforts of those involved and the Council's coordination.

Act 57 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.

Since the first CEMC meeting in September 2020, the Council began working to create a distribution process for the Louisiana Cybersecurity Talent Initiative Fund. This process began with the creation of an RFA, providing guidance to institutions submitting applications. The Council created, reviewed, and approved content for the RFA during the January 2021 quarterly meeting. This content encompassed project requirements, metrics, reporting, project tracks, eligibility, and the application review process. The distribution process for soliciting, recommending, and implementing cybersecurity programs is referred to as the Cybersecurity Talent Initiative program.

Many accomplishments occurred since the first council meeting in September 2020. An aggressive timeline is in motion to address cybersecurity workforce gaps beginning in 2021. However, these solutions will be limited by the resources provided. The evolving expansion of the Cybersecurity Talent Initiative program will grow in its effectiveness and need for additional support. It is recommended Louisiana invest in this initiative to meet the growing demands of cybersecurity. These efforts will strengthen educational and business/industry partnerships, meet the needs of tomorrow's workforce, and elevate Louisiana as a leader in cybersecurity. It is the hope and desire of the Cybersecurity Education Management Council that all stakeholders understand and support the value and impact of the cybersecurity initiatives for Louisiana in 2021 and beyond.