CYBERSECURITY EDUCATION MANAGEMENT COUNCIL

Guidelines for the Submission of

Louisiana Cybersecurity Talent Initiative
Fund Applications

Applications Due: April 17, 2023
5:00 p.m. Central

FISCAL YEAR 2022-23

P. O. Box 3677
Baton Rouge, Louisiana 70821-3677
(225) 342-4253

REQUEST FOR APPLICATIONS

Important Notices

I. GENERAL INFORMATION

A. BASIS OF AUTHORITY

R.S. 17:3138.9 established the Louisiana Cybersecurity Talent Initiative Fund (hereinafter referred to as the Fund), created within the State Treasury as a special fund for the purpose of supporting degree and certificate programs in cybersecurityfields offered by public postsecondary education institutions in order to meet the state's workforce needs. The Fund creates the Cybersecurity Education Management Council (hereinafter referred to as the Council), comprised of representatives of the Louisiana Board of Regents, Louisiana public postsecondary education management boards, Louisiana Department of Education, Louisiana Workforce Commission, Louisiana Economic Development, and Louisiana Chemical Association, along with members appointed by the Governor, to advise and make recommendations to the Board of Regents with respect to distributions of monies for the expansion of cybersecurity programs.

B. PURPOSE OF THE LOUISIANA CYBERSECURITY TALENT INITIATIVE FUND

The Fund is established for the purpose of supporting and sustaining degree and certificate programs in cybersecurity fields offered by public postsecondary education institutions in order to meet the state's workforce needs in cybersecurity and related sectors.

C. PROGRAM ADMINISTRATOR; QUESTIONS ABOUT THIS REQUEST FOR APPLICATIONS (RFA)

Written inquiries concerning this RFA and the requirements set forth herein must be directed to Dr. Clint Coleman, Louisiana Board of Regents' (Regents') Cybersecurity Program Administrator (clint.coleman@laregents.edu). Questions will be accepted only in writing and must be received no later than April 3, 2023. All questions asked about this RFA and all answers provided in response to these questions will be posted on Regents' RSI website (https://rsi.laregents.edu/ufaq-category/cdmc-talent-initiative/) throughout the Q&A period. In order to ensure that all interested parties receive the same information, no questions will be accepted after the deadline date.

II. THE CYBERSECURITY TALENT INITIATIVE PROGRAM

A. PURPOSE AND PROGRAM OBJECTIVES

Cyber threats now 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 qualified to address 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.

Projects supported by the Fund should be cybersecurity-relevant, enhance degreeprograms where appropriate or be closely aligned with recognized industry cybersecurity practices like certifications or certificates, be measurable and practical, encourage close coordination with industry or government to ensure alignment, and emphasize cybersecurity talent development and retention across all levels of postsecondary education and beyond, including reskilling, upskilling, and skills refinement opportunities. 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 cybersecurity practices.

B. PROJECT REQUIREMENTS AND CONSIDERATIONS

Projects supported by the Fund 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 plans for monitoring and reporting of any students, graduates, orparticipants who secure internships, apprenticeships, or jobs;
- Provide validation of at least 25% private or non-public funds as match for the requested CEMC funds, including 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 for reporting purposes all tracks for students (minors/majors), graduates, or learners;
- Align with industry and cybersecurity practitioner-recognized standards such as professional certifications and certificate programs;
- Detail alignment to the NIST Cybersecurity Framework and/or NICE Cybersecurity Workforce Framework (e.g., *Categories* or *Work Areas*); and
- Directly support engagement and success of underrepresented groups (i.e., African American, women, Spanish/Hispanic/Latino, and other students of color) in pathways and their participation in employment opportunities;
- Articulate potential follow-on grant opportunities/Federal/private support to ensure sustainability or build upon and continue growing a previous Cybersecurity Talent Initiative Fund project.

Applications 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, Spanish/Hispanic/Latino, and other students of color, and women);
- Degree, certificate, or certification programs supported by the project, and numbers of credentials awarded, if applicable; and
- If the application is a continuation of a previous Cybersecurity Talent InitiativeFund project, year-over-year or project-length growth across appropriate metrics and indicators.

C. PROJECT TYPES / TRACKS

To address cybersecurity gaps across the workforce continuum, the Cybersecurity Talent Initiative Program supports two separate proposal tracks: Student Projects and Incumbent Workforce and Adult Education Projects. In each track, applicants must specify whether they are seeking support for **New** or **Sustained** projects. Sustained projects are those supported in earlier Cybersecurity Talent Initiative Program funding cycles.

1. Student Projects (*New* or *Sustained*)

Projects within this track 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 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 projects 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, Spanish/Hispanic/Latino, and other students of color, and women);

- 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.

2. Incumbent Workforce and Adult Education Projects (*New* or *Sustained*)

Projects within this track should translate industry cybersecurity challenges, needs, and opportunities into programs to establish and enhance skills for current and emerging employment opportunities in cybersecurity. Track 2 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 American, Spanish/Hispanic/Latino, and other students of color, and women);
- Developing innovative approaches to directly support the participation and success of veterans in pathways and employment opportunities;
- Identifying and (re)engaging candidates who left the workforce to provide awareness of job opportunities in cybersecurity fields; and/or
- Providing pathways for graduates with higher-level degrees (master's and above) to transition into cybersecurity education and instruction.

D. ELIGIBILITY

Public two-year and four-year institutions of higher education, including community and technical colleges, are eligible to compete.

For applications that propose to share resources among several institutions, the following rules/guidelines apply:

1. The application must be submitted by a single lead institution. Partnering institutions must be referenced under the heading "Additional Institutions" on the cover page of the application.
2. Documentation that defines the role(s) of the partner institutions must be submitted as an appendix to the application.
3. Only one comprehensive budget page may be submitted for the award year. Sub-awards for partnering institutions must be described in the budget justification and referenced in the work plan.
4. Funds will be provided to, and managed by, the lead institution, which will be responsible for executing and managing any sub-contracts with partnering institutions.

III. APPLICATION REVIEW PROCESS

All applications will be reviewed by the Cybersecurity Education Management Council (CEMC). Each member will individually assess the applications, then the Council will collectively rank applications and provide final funding recommendations to the Board of Regents.

A. FINAL SELECTION OF APPLICATIONS TO BE FUNDED: After the Council provides funding recommendations, the Board of Regents makes final determinations of applications to be funded based on the competitive review process and dollars available.

B. TIMETABLE: The following schedule for submission, assessment, and approval of funding will apply for FY 2022-23. **If deadline dates fall on a Saturday, Sunday, or holiday, the deadlines will be extended until 4:30 p.m. Central of the next working weekday.**

December 13, 2022	Request for applications issued
April 3, 2023 5:00 p.m. Central	Last day applicants may ask questions about the RFA
April 17, 2023 5:00 p.m. Central	Application submission deadline
April 18 – April 30, 2023	Applications reviewed by the CEMC Council
May 2023	Reports and recommendations of CEMC provided to the Board
June 2023	Final action by the Board
June 2023	Contracts negotiated and executed

IV. PROCEDURES AND DEADLINE FOR SUBMISSION OF APPLICATIONS

The submission deadline is absolute and no materials will be accepted after the date and time published in this RFA. Applications must be submitted via Dropbox at https://www.dropbox.com/request/AZllQqnRdOaxy8F00hmL. A submitted application may be withdrawn if the submitting institution determines revisions are needed, but the revised version must be received before the deadline.

V. APPLICATION REQUIREMENTS AND FORMAT

All narrative sections of the application should be presented in a single PDF document with pages numbered, 1-inch margins at the top, bottom, and each side. In addition, the font should be no smaller than 12 point. Forms must be completed and applications submitted via Dropbox at https://www.dropbox.com/request/AZllQqnRdOaxy8F00hmL.

The requirements and format must be followed closely. Applications that do not adhereto these guidelines may be disqualified for noncompliance. Each application must include the following information:

A. COVER PAGE: The cover page must contain the project title, lead institution, additional participating institutions (if applicable), the project lead and contact information, the intended Track (I or II), and whether the project is New or Sustained.

B. PROJECT SUMMARY: The project summary, limited to 2,500 characters (including spaces), is a concise description of the project containing a clear statement of goals, objectives, targeted metrics, methodology, and planned impact. It should address the aspects of the academic unit's vision statement and how the proposed activities correlate to provide solutions that result in cyber-relevant job candidates and/or employees. A reviewer should be able to understand what is being requested and why, what the project intends to accomplish, and the extent of the enhancement within the initial paragraph of the summary.

Sustained Projects should repurpose previous project elements as appropriate but must also detail plans for further program growth and expanded impact.

C. NARRATIVE: The narrative may not exceed ten (10) pages; it should be succinct and avoid repetition. Information applicable in multiple places may be referenced by title of section. Applications that do not conform to page limitations or the prescribed outline may be disqualified. The project narrative should address all requirements (and potential considerations) in Section II.B.

For multi-institutional applications, explain (as appropriate) in each of the following sections the multi-campus agreements relative to funding, resources, and arrangements by which the various institutions propose to share the benefits of the project and/or plans to make equipment/facilities available to other Louisiana campuses. Documentation must be provided describing the exact nature of any formal agreements related to the submitted project between/among the institutions.

Sustained Projects may and should repurpose previous application content but must also align requests for additional funding to detailed explanations of anticipated growth and strategy for expanded impact.

1. **THE CURRENT SITUATION**: Briefly describe the approach to the cybersecurity workforce challenge (including any potential local, regional, or statewide alignment), the academic unit applying, and how the unit's mission and scope position it to address the challenge.

2. **RATIONALE**: Summarize the need for the project and how it practically addresses challenges in cybersecurity workforce development. Describe opportunities to be addressed in the application for improving outcomes through the unit's capabilities, capacity, competitiveness, expertise, and partnership(s).

3. **PROJECT GOALS AND OBJECTIVES**: Define the project goals and provide measurable and reportable objectives for each. Take care to ensure the measurable objectives and metrics are realistic, tangible, as specific as possible, and directly related to the goals of workforce development.

4. **WORK PLAN**: Describe the specific activities that will be undertaken to achieve the goals and objectives described above. Indicate the person(s) who willconduct each activity. Provide a schedule of activities that lists benchmarks to be accomplished throughout the term of the project. Describe how each objective will be evaluated.

5. **IMPACT**: Describe the impact of the project on the state's cybersecurity workforce by citing specific data relative to the application goals. Data in the Current Situation section should be referenced to provide specific details on impact. Areas of focus should include:

   a. **Impact on Curriculum and Instruction:** Explain the impact which the proposed project will have on the variety and quality of curricular offerings and instructional methods within the affected unit(s).

   b. **Impact on Workforce Development**: Describe how the project will increase the cyber literacy and workforce competitiveness of graduates or incumbent and adult learners, and provide specific data that indicate the regional or statewide workforce needs that the project addresses. Applications are expected to provide data from state agencies that demonstrate how the project is addressing issues related to Louisiana's cybersecurity workforce.

   c. **Impact on Faculty Development:** Explain how the project will improve, expand, and complement faculty expertise in cyber education and workforce development.

   d. **Impact on Service of Students:** Explain how the proposed project will impact and improve the student learning experience. Describe how the application will increase the unit(s)' capacity for student and adult learning andtraining. Demonstrate how the project increases opportunities for students and learners post-graduation by aligning learning/training with opportunities. Provide evidence of the project's impact on the ability of the participating unit(s) to attract, retain and graduate students of high quality.

   e. **Economic Impact**: Describe the short- and long-term benefits of the project to Louisiana's economic development. Explain how the application will impact the unit's and/or institution's relationship with industrial sponsors.

6. MATCH: The application must include validation of at least 25% private or non-public funds for the requested CEMC funds. Matching funds may include but are 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. Documentation confirming the commitment of matching funds (such as letters of commitment from industry or government partners) must accompany the application.

7. PHYSICAL ENHANCEMENTS: The purpose of this section is to establish the precise relationship between the work plan and the item(s) of equipment or other physical enhancements requested. Each item should be referenced above as necessary as it relates to goals, work plan, and impact, and described in detailin this section.

a. **Equipment Request:** List each item requested, with cost information, and briefly indicate the how each major equipment item will be utilized within the work plan to improve cybersecurity workforce outcomes. Logical groupings of items should be made. Explain the reasoning behind (1) choosing each particular piece of equipment and (2) the alternatives that were considered and rejected due to price, quality, and/or appropriate fit for the academic unit going forward.
b. **Other Physical Enhancements:** Describe in detail non-equipment items to be purchased and the significance of the items to the project.
c. **Equipment and Facilities on Hand for Project:** Itemize and briefly explain major equipment/facilities on hand that will be used in conjunction with requested purchases to enhance the participating academic unit(s). This section should answer the question, "Has there been a thorough survey of the current equipment/facilities inventory and does the application plan to make full use of existing resources?"
d. **Equipment Housing, Maintenance, and Security**: Describe a reasonable plan to house and maintain the equipment and other physical property that ensures its maximum usable lifetime. Please note that Fund monies cannot be used to maintain equipment, whether existing or purchased through the award. Funds cannot be requested to purchase service contracts, warranties, or maintenance agreements that extend beyond the life of the funding. These items should be funded through institutional or other matching. If multidisciplinary, interdepartmental, or interinstitutional use of physical property is proposed, describe the plan foreffective utilization relative to each academic unit involved. Describe the plan for keeping all items secure and accounted for at all times.

8. EVALUATION: Describe plans to assess/evaluate the entire project and the degree to which it has achieved its goal(s), as well as its contributions to the unit, campus and state. Tangible and specific metrics along with a rationale for their selection and methodology for data collection/analysis are essential.

9. SUSTAINABILITY: Describe the academic unit's plan for ensuring that the project's impact and individual budget elements (including equipment, software, supplies, and funds dedicated to staff) are sustainable beyond the life of the funding.Issues such as equipment

repair, maintenance, salary support for new hires or released faculty, etc., should be addressed. To address workforce needs and ensure long-term success, sustainability is considered to be a fundamental element of applications.

10. FACULTY AND STAFF EXPERTISE: Identify the individuals who will conduct and administer the project, define their roles, and provide their qualifications for undertaking the specific responsibilities assigned to them.

D. <u>BUDGET AND BUDGET NARRATIVE/JUSTIFICATION:</u> A budget narrative MUST accompany the budget page that fully describes each item for which the expenditure of Fund dollars is requested and to which institutional/private match monies are committed. In addition, the significance of each item to the project should be indicated. All funds for which a commitment from an external source has been pledged and which are cited in the narrative section of the application must be listed on the budget page and explained in the budget narrative. Matching funds must be specified as "in cash" or "in kind." Use state contract prices for equipment purchases, if applicable.

VI. DISALLOWED BUDGETARY ITEMS

Cybersecurity Fund monies cannot be used for ongoing operational costs of existing or proposed programs, entities, or projects. Indirect costs may not be requested from the Cybersecurity Talent Initiative program but may be provided as an institutional match.

Cybersecurity Fund dollars may not be requested for maintenance or repair of equipment, whether existing or purchased through the Cybersecurity Fund. Long-term maintenance contracts for equipment cannot be requested from the Cybersecurity Fund. These expenses may be provided as a match.

The application must detail and fully justify the specific educational uses of any requested equipment related to project goals, objectives and activities.

VII. PROJECT ACTIVATION DATE AND ANTICIPATED DATE OF COMPLETION

The project activation date is **June 1, 2023** and the termination date is **June 30, 2024.**

Application Rating Forms and Scoring Rubrics: New and Sustained Projects

Projects will be assessed based on type, using separate rating forms for New and Sustained projects. To secure continued funding, Sustained projects must demonstrate quantifiable success from the previously funded project and articulate how that success will lead to ongoing growth and increases in success metrics.

	New Projects	**Sustained** Projects
Goals/Objectives	10	10
Work Plan	20	10
Impact	30	10
Evaluation	10	5
Sustainability	10	40
Applicants	10	5
Budget	10	20
	100	100

Application Rating Form: New Projects

Goals/Objectives (10 Points): To what degree are project goals clearly stated, reasonable, achievable, and related to the mission of the Louisiana Cybersecurity Talent Initiative? To what degree are the objectives measurable and related to the goal of producing candidates for jobs in cyber-related fields over the short term? Does the project reflect a commitment to directly supporting the participation and success of underrepresented groups (i.e., African American, Spanish/Hispanic/Latino, and other students of color, and women)? Does the project support access to a broad range of candidates, potentially including veterans or students/learners from rural communities and/or low-income conditions?

Work Plan (20 Points): To what degree does the application establish a compelling timeline for project activities, with a clear delineation of which team member is responsible for each task? To what degree does the work plan clearly, realistically, and practically identify the tasks necessary for achieving project goals and objectives?

Impact (30 points): To what degree does the project increase the likelihood of expanding the number of candidates from Louisiana institutions with industry-accepted foundational or emerging cybersecurity skills? To what degree does the project strengthen industry-institutional collaboration on cybersecurity talent development? To what degree does the project demonstrate scalability, sustainability, and adaptability to changing skill-need alignments? Would the project result in clear and visible success for all stakeholders?

Evaluation (10 Points): To what degree is a plan established for capturing numbers of students/graduates, candidates, apprenticeships, jobs, possible hires, or other employment information, and conducting appropriate analysis to understand the contributions of the proposed project to identified metrics?

Sustainability (10 Points): To what degree are the goals, impacts, and individual budgets sustainable beyond the life of the award? Are appropriate maintenance plans provided for equipment, software, and supplies, and sufficient funds dedicated to staff, faculty and graduate students? Are there concrete and realistic plans to sustain the project beyond funding from this initiative?

Applicants (10 Points): To what degree do the team members appear qualified of implementing the work plan? Is all necessary expertise in place to carry out planned activities at a high level of quality?

Budget (10 Points): To what degree is the budget efficiently crafted to maximize the project'simpact? Does the budget reflect the commitment, contribution, and participation of industry at a level appropriate to the projected work? Does the budget justification adequately explain the relationship of each individual request to the project's goals, work plan, and planned impact?

Application Rating Form: Sustained Projects

Goals/Objectives (10 Points): To what degree are ongoing project goals clearly stated, reasonable, achievable, and related to the mission of the Louisiana Cybersecurity Talent Initiative? To what degree are the objectives measurable and related to the goal of producing candidates for jobs in cyber-related fields in the short term? Does the project reflect a commitment to directly supporting the participation and success of underrepresented groups (i.e., African American, Spanish/Hispanic/Latino, and other students of color, and women)? Does the project support access for a broad range of candidates, potentially including veterans or students/learners from rural communities or low-income conditions?

Work Plan (10 Points): To what degree does the application establish a compelling timeline for project activities, with a clear delineation of which team member is responsible for each task? To what degree does the work plan clearly, realistically, and practically establish the tasks necessary for achieving project goals and objectives? What impediments or issues didthe initial project encounter, and how will this project address those challenges?

Impact (10 points): To what degree does the project increase or improve the likelihood of expanding the number of candidates from Louisiana institutions with industry-accepted foundational or emerging cybersecurity skills? To what degree does the project strengthen industry-institution collaboration related to cybersecurity talent development? To what degree does the project demonstrate scalability, sustainability, and adaptability to changing skill-need alignments? Would the project result in clear and visible success for all stakeholders?

Evaluation (5 Points): Were metrics used in previous projects appropriate and used for meaningful analysis of project outcomes? What additional metrics (like measures of growth, equity, outreach) have been introduced to demonstrate previous success and justify additional funding? Is the new evaluation plan aligned with the goals and projected impacts of the continuation project?

Sustainability (40 Points): To what degree is new investment needed to support the goals, impacts, and individual budget of the new project? How will matching dollars provide and maintain equipment, software, and supplies, as well as contribute to staff, faculty and graduate student support? Does the updated scope continue to build upon existing successes and position the effort for longer term success?

Applicants (5 Points): To what degree does the project team appear qualified to implement the work plan and expand the impact and reach as required for Sustained projects?

Budget (20 Points): To what degree is the budget efficiently crafted to maximize the project'simpact? Does the budget reflect the commitment, contribution, and participation of industry at a level appropriate to the projected work? Does the budget justification adequately explain the relationship of each individual request to the project's goals, work plan, and planned impact?