CYBERSECURITY EDUCATION MANAGEMENT COUNCIL

Guidelines for the Submission of

Louisiana Cybersecurity Talent Initiative Fund
Applications

Applications Due: April 19, 2021
5:00 p.m. Central

FISCAL YEAR 2021-22

Request for Applications

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 cybersecurity fields 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), comprising representatives of the Louisiana Board of Regents, Louisiana higher education institutions, Louisiana Department of Education, Louisiana Workforce Commission, Louisiana Economic Development, and 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 funding 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 RFA

Specific questions concerning this RFA and the requirements set forth herein should be directed to Dr. David Lafargue, Program Administrator (cybersecurity@laregents.edu). In compliance with R.S. 17:3138.9, questions will be accepted and answered until April 15, 2021 (or until 4:30 p.m. of the first working day following this date). No inquiries, whether oral or written, will be accepted after the deadline date to ensure all interested parties receive the same information.

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 degree programs 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, or participants who secure internships, apprenticeships, or jobs;
- Provide validation of at least 25% private or non-public funds as match, 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 all tracks for students (minors/majors), graduates, or learners for reporting;
- Align with 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*); and
- 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.

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).
- The degree, certificate, or certification programs supported by the project, and any awarded, if applicable.

C. PROJECT TYPES / TRACKS

1. Student Projects

Projects within this track 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 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) 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.

2. Incumbent Workforce and Adult Education Projects

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 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, Spanish/Hispanic/Latino, and other students of color, and women) 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 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 campuses, community and technical colleges, and regionally accredited independent institutions of higher education 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 for the project may be submitted for each year of the application. Sub-awards for partnering institutions must be described in the budget justification and referenced in the work plan.
4. If awarded, the grant will be contracted with and managed fully by the lead institution.

III. APPLICATION REVIEW PROCESS

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

A. FINAL SELECTION OF APPLICATIONS TO BE FUNDED: After recommendations are submitted from the Council, the Board of Regents makes final determinations of applications to be funded based on the competitive review process.

B. TIMETABLE: The following schedule for submission, assessment, and approval of grants will apply for FY 2021-22. **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.**

February 19, 2021	Request for applications issued
April 15, 2021	Last day applicants may ask questions about the RFA
April 19, 2021	Application submission deadline 5:00 pm CST
April 20 – April 26, 2021	Applications reviewed by CEMC
April 26, 2021	Reports and recommendations of CEMC provided to the Board

April 28, 2021	Final action by the Board
May and June 2021	Contracts negotiated and executed

IV. PROCEDURES AND DEADLINE FOR SUBMISSION OF APPLICATIONS

Submission deadlines are absolute; all campus work on the application, including final approval and submission to the Board of Regents by the designated campus office, must be completed on or before the deadline date and time. The online application submission system is programmed to close at the deadline(s) cited in this RFA. An application sent to the Board of Regents may be released upon request of the submitting institution if additional changes are needed, provided such request is made before the deadline for receipt. A released application must be resubmitted prior to the deadline to be eligible for funding consideration.

V. APPLICATION REQUIREMENTS AND FORMAT

All narrative sections of the application must 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 to the file upload link located on the website by the deadline provided.

The requirements and format must be followed closely. Applications that do not adhere to these guidelines will 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), and project lead and contact information.

B. PROJECT SUMMARY: The project summary, limited to 2,500 characters (including spaces), should be 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.

C. NARRATIVE: The narrative may not exceed ten (10) pages. The narrative 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 will 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.

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 will conduct 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 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.
   e. **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 and training. Demonstrate how the project increases opportunities for students and learners post-graduation by aligning learning/training with

workforce 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.

g. 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 or institution's relationship with industrial sponsors.

6. MATCH: The application must include validation of at least 25% private or non-public 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 detail in 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 relative to price, quality, and 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 it?"
- **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 grant. These items should be funded through institutional or other matching. If multidisciplinary, interdepartmental, or interinstitutional use of physical property is proposed, describe the plan for effective 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 as well as the rationale and methodology for these indicators 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 grant. Issues such as equipment repair, maintenance, salary support for new hires or released faculty, etc., should be addressed. To address workforce needs and ensure 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. BUDGET AND BUDGET NARRATIVE/JUSTIFICATION: A budget narrative should 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 the requested equipment as related to project goals, objectives and activities.

VII. PROJECT ACTIVATION DATE AND ANTICIPATED DATE OF COMPLETION

The project activation date is June 1, 2021 and the termination date is June 30, 2022.

Application Rating Form

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 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?

Comments:

- Strengths
- Weaknesses

Work Plan 20 Points

- To what degree does the application establish a compelling timeline for grant 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?

Comments:

- Strengths
- Weaknesses

Impact 30 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-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?

Comments:

- Strengths
- Weaknesses

Evaluation 10 Points

- To what degree is a plan established for capturing numbers of students/graduates, candidates, apprenticeships, jobs, possible hires, or other educational and employment information?

Comments:

- Strengths
- Weaknesses

Sustainability 10 Points

- To what degree are the goals, impacts, and individual budgets sustainable beyond the life of the award? To what degree are maintenance or sustainability plans provided for equipment, software, and supplies, as well as funds dedicated to staff, faculty and graduate students?

Comments:

- Strengths
- Weaknesses

Applicants 10 Points

- To what degree do the team members appear qualified of implementing the work plan?

Comments:

- Strengths
- Weaknesses

Budget 10 Points

- To what degree is the budget efficiently crafted to maximize the project's impact? Does the budget reflect the commitment, contribution, and participation of industry? To what degree does the budget justification clearly explain the relationship of each individual request to the application's impact, goals and work plan?

Comments:

- Strengths
- Weaknesses