

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

The Florida Center for Cybersecurity
at the University of South Florida (USF)

Call for Cyber and Information Technology Pathways Subgrant Applications:

Funding Opportunity Title:	Expanding Cybersecurity and IT Pathways
Expected Number of Awards:	TBD
Subgrant Application Announcement:	March 8, 2022
Subgrant Application Opening Date:	March 9, 2022
Subgrant Application Closing Date:	April 17, 2022
Estimated Total Program Funding:	\$17,0000,000
Subgrant Implementation Timeline:	June 2022 – August 2023

Eligible Subgrant Applicants: Any organization or jurisdiction that is part of Florida’s public education system, as defined by the applicable Florida Statutes enumerated in Section II. B below, to include Florida public school districts, post-secondary technical career centers, charter technical career centers, Florida College System (FCS) institutions, Florida State University System (SUS) institutions, and/or any combination of the above.

- I. Grant Purpose:** The purpose of the *Expanding Cybersecurity and Information Technology Pathways* program is to increase the number of trained and/or educated workers in Florida that are prepared to fill cybersecurity/information technology (IT) jobs in the state and the Nation.
- II. Grant Description:** The Cybersecurity/IT Pathways Grant will fund projects that prepare Florida’s citizens to become ‘job-ready’ candidates with the skills to meet the cybersecurity/IT employment needs of businesses, public agencies, and non-profit organizations across the state and the Nation. This is not only to take advantage of burgeoning labor market demand in these critical fields but also to meet a real national security imperative.

A. Goals of the Grant. Accordingly, the Florida Department of Education (FLDOE) has awarded the above-referenced grant to the Florida Center for Cybersecurity—also referred to as Cyber Florida—at the University of South Florida (USF), and pursuant to that grant, the Center will award sub-grants to eligible applicants with existing Pathways-relevant projects that can demonstrate the potential to be expanded and scaled for statewide adoption. As framed by FLDOE, successful applications may directly address the needs of Florida K-12 students, higher education students, adults, or any combination of those groups. Additional information on the FLDOE grant may be found at www.cyberflorida.org.

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

B. Subgrant Eligibility Requirements. Eligible applicants are limited to: Florida public school districts; Florida post-secondary technical career centers and charter technical career centers; Florida College System (FCS) institutions; and State University System (SUS) institutions. These entities are defined further under the following Florida statutes: §1001.30, §1001.44, §1002.34, §1000.21(3), and §1000.21(6). While the activities proposed within subgrant applications may include multiple partner organizations, each application must be submitted and led by at least one eligible entity as defined above. However, robust public/private partnerships are an important component of workforce education, and as such, project partners may include private businesses, other government entities and jurisdictions, and non-profit organizations. All appropriate conflict of interest rules shall apply without exception.

III. Proposed Subgrant Activities and Outcomes: Applicants will be required to specify activities and outcomes that they propose to undertake with subgrant funding.

A. Possible Program/Project Activities. Examples of possible program activities include but are not limited to: (1) integrated education and training of elementary, middle, high school, college, and/or working adult students, via applicable courses and/or curricula; (2) secondary continuing technical education (CTE) courses/programs; (3) non-credit training that includes preparation for industry certifications; (4) registered pre-apprenticeship and apprenticeship programs; (5) training programs for existing workers and/or ‘upskilling’ for those in other industries; (6) career/advanced technical certificates and applied technology degrees; and (7) teacher education and professional development.

B. Possible Program/Project Outcomes. In addition, applicants will be required to identify expected project/program outcomes that contribute to the overarching purpose of the Pathways grant. These may include but are not limited to such things as (1) *Student Outcomes*, such as increased enrollment in cybersecurity courses and programs, or increased completion of industry certification examinations; (2) *Programmatic or Institutional Outcomes*, such as improvements to existing curriculum frameworks, or the development of model articulation agreements; (3) *Workforce Outcomes*, such as the delivery of education and training programs that integrate employer involvement, or that support ‘hands on’ work-based learning opportunities; and (4) *Other Outcomes* that may be proposed by an applicant. Note that applicants will be asked to categorize their proposals according to this taxonomy as part of the application process, primarily as a way of ‘binning’ applications for review.

IV. Subgrant Administration: In total, approximately \$17 million will be awarded as subgrants to applicants to this subgrant program.

A. Distribution of Subgrant Funds. Of that total, approximately one-third of available funds will be awarded as subgrants to applicants from the Tampa Bay area, as defined in the initial FLDOE grant; and approximately one-third will be awarded as subgrants to applicants from the Greater Miami area, also defined in the initial FLDOE grant. In addition, Cyber Florida has determined that the remainder of available funds will be awarded as subgrants to ‘at large’ applicants from

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

other areas of the state. The final number and size of projects that receive funding will be determined based on an evaluation of applications received. In that regard, among other factors, subgrant awards will fund those programs that potentially contribute the most to the overall purpose of the FLDOE grant, and as specified below, these must be included in a subgrant application.

B. Grant Coordinators. During the project period, the primary point of contact for each subgrant recipient will be one of three Grant Coordinators, to be specified in the recipient's award letter. Reporting to Cyber Florida's Pathways Grant Management Office, these Grant Coordinators will provide guidance and support for subgrant recipients, but those recipients remain responsible for complying with all terms and conditions of the subgrant award, to include timely responses to inquiries regarding project status, budget, deliverables, and progress toward milestones. Grant recipients are also expected to participate in program evaluation inquiries and requests for data from the Pathways Grant program evaluation team.

C. Final Reports. In addition, by no later than August 15, 2023, subgrant recipients are required to submit a final report on their projects, including specific outcomes, other performance metrics, activities, lessons learned, and recommendations for future projects; specific requirements and format for this final report will be provided to recipients at a later date.

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

Pathways Subgrant Application Process:

- I. Application Submission and Due Date.** All subgrants will be awarded through a competitive selection process managed by the Florida Center for Cybersecurity's Pathways Grant Management Office, in collaboration with Grant Coordinators. Completed applications must be submitted through an online application portal accessed from www.cyberflorida.org and may be submitted on or after 9:00 AM, March 9, 2022. All applications must be received by close-of-business (COB) of April 17, 2022 (defined as 5:00 PM EDT) on that date. The application portal will ask applicants to answer a brief series of questions and then upload their proposal in portable document format (PDF). Proposals must adhere to the Pathways Subgrant Application Process requirements, as listed below.
- II. Application Review.** Completed applications that are received by the application deadline will be reviewed by the Pathways Subgrant Program Office, in collaboration with Grant Coordinators and with the input of subject matter experts. FLDOE and the Florida Cybersecurity Advisory Council will also be consulted. Applications that are incomplete or received after the deadline will not be evaluated. Final decisions will be made by Cyber Florida in consultation with FLDOE. Prospective subgrant recipients will be contacted by the Pathways Subgrant Program Office once all reviews are completed and all award decisions are finalized. Subgrant awards will be announced, and funds distributed as quickly as possible to allow selected recipients to begin their projects.
- III. Notice of Intent to Apply.** The Pathways Subgrant Program Office will be better able to manage the application and review process if it has an understanding of the number of applications it can expect. Therefore, prospective applicants are strongly encouraged to submit a *non-binding* Notice of Intent to Apply to pathways@cyberflorida.org by no later than COB March 23, 2022. Please note that such notices of intent are non-binding; thus, potential applicants who provide such a notice are not subsequently obligated to submit an application. As a minimum, the non-binding Notice of Intent may be as simple as an email briefly describing the project and stating an intent to apply for funding; additional details are welcome, but notices need not include any other application details.
- IV. Additional Grant Information.** Cyber Florida will conduct at least one Informational Webinar to answer questions about the Pathways grant program and subgrant awards from any eligible, prospective applicant; in addition, Cyber Florida will publish Frequently Asked Questions (FAQs) on its Web site. Prospective applicants are encouraged to read all grant application materials carefully, to attend scheduled pre-application Informational Webinars announced at www.cyberflorida.org, and to contact the Pathways Subgrant Program Office with any questions at pathways@cyberflorida.org. Note that Cyber Florida reserves the right to ask any applicant to clarify elements of its application or to provide additional supporting evidence at any time.

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

Subgrant Application Requirements:

- I. **Application Page Limit.** The application proposal will be limited to 15 single-spaced pages, in size 11 Calibri font, with additional internal limits described below; graphics are encouraged but will count against the page limit. A no more than (NMT) two-page resume for each individual identified as Key Project Personnel and the Project Budget Spreadsheet are not included in this limit but are subject to additional requirements, as specified below. Additional attachments may be included *within* the 15-page limit, but except for Key Personnel Resumes and the Program Budget Spreadsheet, attachments that exceed the page limit and other specifications *will not* be considered. The final application will be submitted in pdf form that includes all attachments

- II. **Summary of Application Contents.** Within the above 15-page limit, each application should include:
 - (A) a one-page summary of the proposed project/program summary;
 - (B) a table of contents;
 - (C) a detailed project/program narrative, to include the project's history, any additional partners or sponsors, etc.;
 - (D) a listing of no more than five Key Project Personnel, including their titles, proposed roles, and contact information, with no more than two-page resumes for each individual separately attached to the application; and
 - (E) a Budget Justification, in addition to a separate Project Budget Spreadsheet provided by Cyber Florida and separately attached to the application. Applicants may also provide additional documentation of current and pending additional external support, resources, and/or funding with applicable letters of commitment and/or other relevant evidence, but such additional documentation will count against page limits. Additional guidance is provided below.
 - A. **Project/Program Summary:** Applicants must provide a brief description of the proposed project/program. Limited to one page, this summary description should provide an overview of key details of the project information, including resource requirements and estimates, as specified in the remaining sections.

 - B. **Table of Contents:** Applicants must provide a table of contents that lists all sections of the application, including all attachments that are within the 15-page limit.

 - C. **Detailed Project/Program Narrative:** Applicants must provide a detailed description of the proposed project/program, including:
 1. **Problem Statement.** A problem statement that describes the overarching problem that the proposal attempts to address.

 2. **Proposed Project/Program Objectives.** One or more project/program objectives that describe what the project is specifically intended to accomplish; such objectives must be SMART; that is, specific, measurable, achievable, relevant, and time-based.

 3. **Proposed Project/Program Results and Other Performance Measures.** A detailed description of the results that the applicant expects to achieve, to include short-

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

term outcomes (that is, by the end of the project funding period) and other performance metrics, as well as intermediate/long-term impact and benefits over the next 2-5 years. This description should also include the project's proposed target population and its detailed demographics.

- 4. Proposed Project/Program Plan.** A description of the proposed project plan that details exactly what the applicant intends to do and how the applicant intends to do it, including activities to be undertaken, the relationship between those activities and project objectives; a detailed timeline that provides milestones and intermediate/final project deliverables; and relevant public sector, private sector, and/or non-profit partners, along with any evidence (to include letters of support) of their intended or committed contribution to the project. A Budget Justification that summarizes cost, facilities, and other expenses, must also be included in this section; note that this is *in addition* to the Project Budget Spreadsheet described in Section F below.
 - 5. Relevant Past Performance.** A description of what the applicant has done to date that may bear on an evaluation of the proposal, to include relevant background information and results; applicable evidence and points of contact; lessons learned from previous attempts, including challenges and successes; previous resource investments; and other relevant administrative details.
 - 6. Proposed Evaluation Plan.** A description of how the applicant intends to evaluate the efficacy of the project, both during and after the funding period. In other words, how will the applicant (and Cyber Florida) know if the project is a success? The description should include plans for final data collection and analysis.
 - 7. Contribution to Pathways Grant Goals.** Most importantly, the description must also detail how the project contributes to the overall goal of the Pathways grant, as well as the prospects for subsequent project expansion, adoption, and sustainability/scalability throughout the state
- D. Key Project/Program Personnel.** The proposal must identify at least three and no more than five Key Project Personnel who will be accountable for the proposed project or program, along with their titles, proposed roles, how they will contribute to the project, and appropriate contact information. At least one individual should be identified as the project's Principal Investigator (PI), who will serve as the primary point of contact for any questions Cyber Florida may have regarding the subgrant application. Applicants are also required to attach a (no more than) two-page resume for each Key Personnel; as noted, attached resumes will not count against the 15-page proposal limit.
- E. Final Evaluation of Applications.** Applications will be evaluated on each of the above elements but with particular emphasis on (1) the cost-effectiveness of the project plan; (2) the likelihood of anticipated results and their contribution to the overall goal of the grant;

THE FLORIDA CENTER FOR CYBERSECURITY

AT THE UNIVERSITY OF SOUTH FLORIDA

(3) the number, variety, contribution, and commitment of various project partners; and (4) its likely sustainability over time.

- F. Proposed Project Budget Spreadsheet.** All applicants must complete and attach a Project Budget Spreadsheet (available for download at www.cyberflorida.org/pathways), describing the subgrant funds the applicant is requesting, by category, to execute the project/program within the 2022-2023 academic year. The Budget Spreadsheet provides a more detailed breakdown of proposed spending in each category and is *in addition* to the Budget Justification to be included in the Proposed Project Plan, as described in Section C4 above. This Spreadsheet will not count against the 15-page limit.