

# **FC<sup>2</sup> Collaborative Seed Program**

## **Program Description:**

The Florida Center for Cybersecurity (FC<sup>2</sup>) supports and encourages collaboration across the State University System (SUS) to promote research innovation and productivity in cybersecurity. The competitive FC<sup>2</sup> Collaborative Seed Grant Program advances that objective by funding research teams with investigators from at least two different SUS institutions for projects that align with FC<sup>2</sup> strategic priorities and have strong potential to attract external funding.

## **Eligibility Information:**

Applicants must be eligible to be principal investigators (PI) for external grants at their home institutions. The proposed project must designate one PI and one Co-PI, who meet the eligibility criteria, each employed by a different SUS institution.

A faculty member may submit only one application as PI or Co-PI per funding cycle but is not limited as a collaborator or team member on other projects.

## **Award Information:**

### Estimated Funding and Number of Awards:

Approximately \$750,000 will be available from FC<sup>2</sup> annually for awards under this program. Budget for each award can be a maximum of \$50,000 for one year. It is estimated that there will be 10 to 15 awards per solicitation. Awards may be renewed competitively for one additional year.

Applications that include matching funds from an institutional and/or industrial sources will be given more weight during the review process. Matching can be in cash, academic release time for faculty members, or student stipends.

### Scope of the Award:

Applications must pertain to cybersecurity, information assurance, or digital forensics. Preference will be given to applications that address current high-priority topics, which for 2016 include:

- Cyber Mission Assurance (to protect or ensure the continued function and resilience of capabilities and assets through risk management)
- Cyber Resilience (the ability of a system or domain to withstand attacks or failures, and in such events, to reestablish itself quickly)
- Software Defined Networking
- Securing Cloud Infrastructures
- Security tools with a primary focus on machine learning
- Defensive Cyber
- Improving the Discovery and Retrieval of Relevant Knowledge/Intelligence Products
- Medical Device Security
- Insider Threat in the Cyber Domain
- Securing the Internet of Things (IoT)

Award funds may be allocated for a variety of expenses, including pilot projects, prototype development, demonstration of educational/public service programs, domestic travel, data collection and analysis, and graduate student salaries. Funds cannot be used for construction, renovation, administrative assistance, or international travel. Facilities and Administrative (F&A) costs are not allowed under this program. Summer salary for Co-PIs can be requested up to a total of \$10,000 per year (note: this is a total, not per Co-PI).

Project activities may include, but are not limited to

- Workshops on emerging multidisciplinary research areas (excluding food and beverage)
- Support of a high-level seminar series to promote networking for formation of an innovation program (excluding food and beverage)
- Development of concepts and white papers for large-scale centers, institutes or cluster hires
- Travel to establish partnerships or to interact with program officers
- Identification and recruitment of industrial, academic and/or government partnerships in support of initiatives
- Development of plans to promote industrial research collaborations
- Creation and support of resources such as research consortia, collaboration sites or social networking tools to facilitate large-scale inter-university research programs
- Collection of preliminary data needed for external proposal submission

Award recipients are required to submit a proposal for competitive external funding prior to the end of the Collaborative Seed Grant Program period.

## **Application Proposal Information:**

### Proposal Format:

The proposal should include a cover sheet, project summary, table of contents, project narrative, biographical sketches, budget and budget justification, current and pending support, facilities/equipment/other resources, and letters of commitment. The document should be in Microsoft Word (.PDF) format, and single-spaced, using Times New Roman, 12-point font and one-inch margins. The proposal should be submitted as one PDF document to the designated online portal. Additionally, each institution must submit separate complete budgets.

Application Content: The proposal should include the following elements:

- Cover Sheet
  - Title of proposed project
  - PI/Co-PI information (Name, Email, Primary Address)
  - Institution Information (Name, Address)
- Project Summary
  - Brief overview
  - Statement of the intellectual merit of the proposed project
  - Statement on the potential broader impacts of the proposed project
  - *1 page limit*
- Table of Contents
- Project Narrative
  - Objects of the proposed work and expected significance
  - Outline of the general work plan
  - A “Broader Impacts” section (aligned with the statement in the Project Summary) that illustrates ways to mesh project research and other activities with the interests of the Cybersecurity industry

- **If previously funded:** Provide a summary of the results, any corresponding publications, and new products developed as a result of the funding
- ALL references properly cited
- *10 page limit*
- Biographical Sketches
  - A list of all undergraduate, graduate, and post-doctoral education (Institution, Location, Major-Degree, Year)
  - A list of all academic/professional appointments in reverse chronological order
  - A list of up to five examples that demonstrate the broader impact of the individual's professional and scholarly activities that focus on integration, transfer of knowledge, and creation
  - Other Personnel: A list of postdoctoral associates, other professionals, and students (include the appropriate qualifications that merit their consideration in the evaluation of this project)
- Budget & Budget Justification
  - Budget: Correctly complete the [budget template](#) provided (Failure to do so may result in the disqualification of the project)
  - Separate budget for each institution involved
  - Budget Justification: Follow guidelines listed below
    - PI/Co-PI's: List effort and description of effort
    - Equipment: List all equipment to be utilized
    - Travel: Explain all funds requested for travel
    - Materials and Supplies: List all requested for project
    - Other costs: Tuition fees requested for graduate support, etc.
- Current and Pending Support
  - Information on all current and pending support for ongoing projects and proposals (this project included)
  - Include: The source, the project, and a brief overview of the project
- Facilities, Equipment, and Other Resources
  - Include a description of the internal and external resources that PI/Co-PI's will provide for the project
  - This information should be included in this section as opposed to the budget justification/project narrative
- Letters of Commitment
  - Must be written and signed by an authoritative figure
  - Amount must clearly match the amount indicated in the budget
  - Clear indication of the source of the match

## Review Process and Selection Criteria:

Applications will be assessed by review panels composed of subject matter experts from across the Florida SUS, which will be identified by members of the FC<sup>2</sup> SUS Advisory Committee. Experts from non-SUS institutions will be sought, if needed. Each proposal will receive at least three reviews addressing the following criteria and rated on a 100-point scale. The FC<sup>2</sup> director will make the final selection based on the rankings of the proposals and attention will be given to the diversity of ideas and the number of collaborative SUS and/or industry partners included. The following criteria will be used:

- Scholarly Merit and Feasibility (40 points)
  - Clear case to address (or has a plan to address) an important gap in existing knowledge or to significantly advance knowledge in the discipline
  - Project objectives are clearly specified, with appropriate outcomes metrics and are achievable and realistic for the project period
  - Clearly specified work plan
  - Aligns with FC<sup>2</sup> strategic priorities
- Qualifications of project personnel (20 points)
  - Co-PIs qualified to execute project plan, manage the team, and produce the deliverables
  - Team roles clearly defined
  - Includes multiple disciplines where appropriate
- Budget and facilities (20 points)
  - Appropriate amount. Properly allocated. Well justified. High return on investment.
  - Balance of involvement of participating SUS institutions.
  - Institutional or industrial matching funds.
- Broader Impact (10 pts)
  - Connections to collaborations with other SUS initiatives, industry in the state, and governmental assets in the state.
  - Technology transfer activities in terms of intellectual property generated, licenses and startup companies.
- Potential for generating external funding (10 points)
  - High potential for follow-up funding with a clearly defined plan to pursue a specific funding opportunity.

## Timeline:

RFP issued	November 7 <sup>th</sup> , 2016
Submission Deadline	January 6 <sup>th</sup> , 2017
Award Announcement	February 21 <sup>st</sup> , 2017

\*Subsequent years will follow a similar timeline

## **Reporting:**

Technical and financial reports are due 6 months after the end date of the project. The final report should include the following information (title of project, name of investigator(s), expected dates of performance, amount, and funding agency) about follow on proposal(s) submitted to other agencies for continued support of the project. Participation from a PI, Co-PI, or another approved individual is mandatory at the annual Florida Center for Cybersecurity research symposium.

## **Additional Comments:**

Any financial or programmatic changes will require prior approval of FC2 before such changes can be implemented.

Patentable ideas, trade secrets, privileged or confidential commercial or financial information, disclosure of which may harm the proposer, should be included in proposals only when such information is necessary to convey an understanding of the proposed project. Such information must be clearly marked in the proposal and be appropriately labeled with a legend such as: "The following is (proprietary or confidential) information that (name of proposing organization) requests not be released to persons outside USF, except for purposes of review and evaluation.

Please note that if your project is selected for funding, each recipient must provide a completed A-133 Financial Status Questionnaire <http://www.usf.edu/research-innovation/sr/documents/mini-audit-questionnaire.pdf> and a Subrecipient & Information Compliance Form <http://www.usf.edu/research-innovation/sr/documents/sub-info-compliance-cert-form.pdf>.