CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Fall 2019 Request for Proposals

The University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) is committed to pushing the boundaries of technology, social science, and humanities to positively influence how individuals, organizations, and governments deal with cybersecurity. The conceptual and practical aspects of the term 'cybersecurity' are evolving rapidly, as what we mean by 'cyber' and 'security' is changing in ways that would have been almost unimaginable a few years ago. CLTC believes that a transformative cybersecurity research program should not only address the most interesting and complex challenges of today's socio-technical security environment, but also grapple with the broader challenges of the next decade's environment. Through this, our fifth annual request for proposals (RFP), we will continue to fund research on a heterodox set of security issues and attempt to draw in new researchers, including those who have not previously worked in cybersecurity-related areas.

Proposals are due on **Thursday, October 24**, **2019 by 11:59pm PDT**. Submission instructions can be found below under "**Submission Process**."

GOALS

The primary goal of this RFP is to expand and refine understandings of—and means of intervening in—the cybersecurity problem space, broadly defined.

- This RFP is not restricted to any one discipline or tailored to any particular methodology.
- CLTC encourages the submission of proposals from multidisciplinary teams.
- CLTC will prioritize proposals that have the potential to make a meaningful, long-term impact on cybersecurity issues and outcomes.
- In addition to proposals seeking to undertake basic and applied research, we also welcome proposals for other effective uses of funds, including but not limited to academic course design, policy projects, and purposeful convenings.
- If you are unsure, or if you have questions regarding the substantive fit of your ideas with this RFP, please reach out to us at cltcgrants@berkeley.edu.

GRANTMAKING CATEGORIES

We anticipate making grants in two general categories:

- **Seed Grants**, generally $15,000 and below. These grants could fund an exploratory study, a small pilot, a PhD dissertation project, or other means of 'prospecting' a problem area.
- **Discrete Project Grants**, up to $100,000. These grants intend to fund projects that have defined boundaries with clear outcomes and potential impact. While these grants by default have a one-year timeline, CLTC will entertain proposals for longer discrete projects when scientifically justified.

RESEARCH AREAS

CLTC will consider proposals in all domains relevant to cybersecurity. The openness of that statement is intentional, as we seek to expand the range of disciplines and types of expertise and knowledge that can be brought to bear on this challenge. As an indication, CLTC's range of previously supported projects include (but are not limited to) work that addresses:

- Cyber talent pipeline, human capital, and education
- Security implications of artificial intelligence and machine learning
- Cybersecurity governance and regulatory regimes
- Protecting vulnerable individuals and organizations online
- Cybersecurity culture and dialogue
- Security implications of 5G networks and other emerging technologies
- Political, market, and legal 'shapers' of cybersecurity outcomes
- Behavioral and 'usable' cybersecurity
- Distributed-ledger technologies for cybersecurity purposes

We especially welcome proposals that address both technical and non-technical components, although it is not required. We encourage researchers with questions about the relevance of their ideas to discuss with us how to make the case.

GRANTEE ELIGIBILITY

All proposals must have a Project Lead* with an active UC Berkeley research affiliation, and the Project Lead must be enrolled in or have completed a graduate degree. It is unlikely that Project Leads will be funded for multiple projects. If you have an active UC Berkeley research affiliation, but do not have PI status at UC Berkeley (e.g. current graduate students), please indicate in your proposal the UC Berkeley faculty member(s) with PI status who will oversee the funding on the grant.

CLTC encourages collaboration with outside institutions—academic, commercial, and otherwise—as befits the research program. We also encourage (and will, on request, enthusiastically facilitate) contact with policy institutions, think tanks, agencies, firms, governments, and other means of practical dissemination of research results. We will look favorably on research proposals and budget requests that are designed to facilitate those connections.

While all proposals will be given equal consideration, if you are a current or former CLTC grantee with a deficit on your existing grant fund(s), further funding will not be administered until the deficit is cleared. All current and former grantees who have active balances on existing grant funds will be asked to provide a plan for spending down existing funding before new or renewal funding is administered.

(Note that CLTC utilizes the title "Project Lead" in place of "Principal Investigator (PI)" because UC Berkeley graduate students without "PI status" are eligible to submit proposals with the support of a UC Berkeley PI. For funding purposes, a UC Berkeley PI, as well as their financial contact/research administrator, is required for all proposals.)

SUBMISSION PROCESS

Submit proposals here: https://forms.gle/ciqKK4CnEWcDMV5C8

The form will request that you upload a PDF of your proposal; please use the following naming convention for your attachment: "CLTC RFP 2019 – [PI Last Name] – Project Title"**.**

Proposals will be reviewed by an internal, interdisciplinary committee and judged for scientific promise, potential impact, and contribution to CLTC's mission and goals. The assessment will include evaluation of a 'theory of impact' that ties the potential results of the research program not only to academic publications, but also to changes in the world of cybersecurity behaviors, technologies, policies, markets, conflicts, etc.

Proposals should adhere to the following format:

PROPOSAL BODY

The proposal body should include standard elements that describe and justify the research. This should include:

- **Scientific Promise**: What questions, in the context of existing knowledge and literature, will be addressed and how will they be addressed? What methodological and/or theoretical foundations ground this work? What new insights and knowledge are likely to be generated as a result of this work? How will the risks—scientific and otherwise, including any ethical concerns—be addressed?
- **Potential Impact:** How will the results of this work contribute to broader theory development? Who are the major research, policy, and/or decision-making constituencies that will find this work useful? How might results of this work influence future research programs and/or policy, practices, behaviors, regulations, etc.?
- **CLTC Relevance:** How will this work contribute to the broader research portfolio and mission of the Center for Long-Term Cybersecurity?
- **Program Development:** What are the roles of key research personnel? What is the project schedule for the year? If you intend to support an individual through salary or tuition support, please indicate this in the proposal and, if possible, name the person being supported.

For Seed Grants, the proposal body should not exceed three pages, single-spaced. For Discrete Project Grants, please limit the proposal body to seven pages maximum, single-spaced.

APPENDIX

Please include the following information in an appendix at the end of your proposal. (Appendices do not count against page limits.)

Biographies for the Project Lead(s) and other key research personnel named in the proposal. (Note: if the Project Lead does not have PI status with UC Berkeley, then a faculty member with PI status must oversee the grant funds. Please indicate the faculty PI here as "Project Supervisor." In this circumstance, a biography for the faculty PI is not required.);

A one-page itemized budget, including categories such as salary, equipment, and travel. Your budget should clearly indicate if you have any other sources of funding for the project, including the period of funding and dollar amount, as well as matching grants and pending grant proposals.

Financial Contact/Research Administrator's contact information (full name and email address). Depending on who has PI status, this would be the UC Berkeley financial contact for either the Project Lead or the Project Supervisor.

CONDITIONS OF AWARD

All awards will be made with the condition that grantees will provide:

- An updated abstract (in language appropriate for a public audience) to be posted on CLTC's website, as well as photographs and biographies of PIs, Co-PIs, and partners, submitted within two weeks of funding approval;
- A roughly one-page midterm report describing progress on the project, to be submitted halfway through the grant period;
- A roughly two-page report describing scientific progress and outcomes, as well as budget expenditures, to be submitted to CLTC within one month of the end of the grant period;
- A description of the project that is appropriate for a broader, non-academic audience, in a format (e.g. blog, video) that can be posted on the CLTC website;
- Acknowledgement of CLTC's support in any publications, presentations, articles, interviews, or other means of disseminating research results.

For Discrete Project Grants, the following additional conditions will apply:

- PIs may be invited to present an informal seminar on their group's work, aimed at the broader CLTC and/or business and policymaking communities, at some point during the year;
- PIs, as well as any individuals whose work is fully or more than 50% funded with CLTC funds, will be expected to participate in at least one CLTC event per semester.

Please note that, due to budgetary restrictions, not all proposals will be fully funded.

ADDITIONAL OPPORTUNITIES

In addition to the standard research grant submission process, CLTC will maintain a small fund for urgent, opportunistic use (e.g., to fund a small exploratory workshop on a newly emerging issue that was not anticipated during the regular grant cycle). To submit a request under this program, please contact the Center as early as possible to discuss your needs.

Although not part of this RFP, we encourage researchers to provide us with suggestions for how we might invest time and/or resources to better serve the broader UC Berkeley cybersecurity research community. If you have ideas about collective resources, facilities, and other 'infrastructural' elements that might be helpful for you and other researchers, please contact us to discuss.

RESEARCH EXCHANGE EVENT

Researchers interested in learning more about the kinds of projects we fund are invited to attend the annual CLTC Research Exchange, which will be held on **Thursday, October 3, 2019 from 9:30am-**

5:30pm, and will feature presentations by several of our 2018 and 2019 grantees. Please RSVP through our website, https://cltc.berkeley.edu/event/2019-cltc-research-exchange/, and/or email us at cltcevents@berkeley.edu with the subject line "CLTC Research Exchange" for additional information.

ABOUT THE CENTER FOR LONG-TERM CYBERSECURITY

The Center for Long-Term Cybersecurity was established in 2015 as a research and collaboration hub at the University of California, Berkeley. From our home in the School of Information, our mission is to help individuals and organizations address tomorrow's information security challenges to amplify the upside of the digital revolution. To join our listserv and receive more information about our events, please email cltc@berkeley.edu or visit our website at https://cltc.berkeley.edu/contact-us/.