CLTC
Center for Long-Term Cybersecurity

102 S Hall Rd
Berkeley, CA 94720
510-664-7506
cltc@berkeley.edu

## REQUEST FOR PROPOSALS: UC BERKELEY CENTER FOR LONG-TERM CYBERSECURITY

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. In this second Request for Proposals (RFP), we will continue to fund research on a heterodox set of security issues, but also seek (1) to encourage additional focus on a handful of core priority areas; and (2) to draw in new researchers, including those who have not previously worked in cybersecurity-related areas. Proposals are due on October 28, 2016

## 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 cross-disciplinary teams.
- CLTC will prioritize proposals that also have the potential to make a meaningful, longer term impact on cybersecurity issues and outcomes through technologies, actions, policies, behaviors, markets, etc.

## GRANTMAKING CATEGORIES

We anticipate making grants in two general categories:

1. Seed Grants, generally below $15,000. These grants could fund an exploratory study, a small pilot, a PhD dissertation project, or other means of 'prospecting' a problem area.

2. Discrete Project Grants, up to $100,000. These grants intend to fund projects that have defined boundaries with clear outcomes and impact potential. While the default will be that these grants have a one-year timeline, CLTC will entertain proposals for longer discrete projects when scientifically justified.

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.

## PROPOSAL PRIORITIES

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 kinds of expertise that can be brought to bear. We encourage researchers with questions about the relevance of their ideas to discuss with us how to make the case.

Specific funds will also be dedicated to proposals that fall into five priority areas, focused on encouraging the further development of cybersecurity objectives that serve the public interest:

(1) *Cyber risk*, including cyber insurance and the use of incentives to improve security;
(2) *Security implications of* a) the *Internet of Things* and b) *machine learning and artificial intelligence*;
(3) *Innovative approaches to the problems of identification and authentication on the internet* beyond conventional passwords;
(4) *Addressing the 'talent pipeline problem' for cybersecurity*, both by expanding the number of qualified cybersecurity professionals and increasing their diversity; and
(5) *New approaches to the regulatory landscape of cybersecurity*, including improved design of public, private, and mixed institutions.

Each of these areas encompasses both technical and non-technical components, and we especially welcome proposals that address both, although it is not required that any single proposal do so.

CLTC has also earmarked significant funds (especially seed grant funds) for PIs who have not previously worked in cybersecurity. Such applicants should indicate this on their submission cover sheet.

## GRANTEE ELIGIBILITY

PIs applying for CLTC grants must have an active UC Berkeley research affiliation, and must be enrolled in or have completed a graduate degree. Given the large number of worthy research proposals we received last year, it is unlikely that PIs will be funded for multiple projects this year.

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.

We are only able to pursue a limited number of subawards with outside institutions. If your grant application will require a subaward to enable the outside connections you need, please contact us as soon as possible so that we can work with you to avoid issues later on. Please also note that due to prime award restrictions, we are unable to pay off-campus indirect costs or overhead.

## SUBMISSION PROCESS

**Full Proposals are due by OCTOBER 28, 2016 to cltc@berkeley.edu. Please use the subject line: "CLTC RFP 2016 – [Last Name], [First Name]."**

Proposals will be reviewed by an internal interdisciplinary committee and judged for scientific promise, potential impact, contribution to CLTC mission goals, and long-term research program development. 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 follow the following format:

Cover Sheet (no more than one page). Please fill out the PDF form at https://cltc.berkeley.edu/files/2016/09/CLTC_RFP_Intake_Form.pdf and include it as the first page of your proposal.

Proposal Body (for Seed Grants, not to exceed two single-spaced pages; for Discrete Project Grants, not to exceed seven pages).

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

- Scientific Promise: What questions 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 Mission: How will this work contribute to the broader CLTC agenda?
- Program Development: What are the roles of key research personnel? What is the project schedule for the year?

Please append biographies for the PI and other key research personnel named in the proposal, as well as a one-page itemized budget, including categories such as salary, equipment, and travel. Biographies and budget do not count against the page limits.

- 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.
- Please indicate if you have any other sources of support for the project, including matching grants and pending grant proposals.

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

CLTC will host an informal information session to answer any questions about this Request for Proposals on Wednesday, September 28 from 4:30pm-5:00pm in South Hall, Room 202. Tea and

cookies will be served. Please RSVP here: https://cltc.berkeley.edu/rsvp-for-cltc-grant-information-session-wednesday-928-430pm/.

## CONDITIONS OF AWARD

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

- An updated abstract (in simple, jargon-free language) 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 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 to a broader non-academic audience at some point during the year, for example through a blog post or short video for the CLTC website; and
- Acknowledgement of CLTC's support in any publications, presentations, articles or interviews, and other means of disseminating research results.

For Discrete Project Grants, these additional conditions will apply:

- PIs may be asked 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 course of the year;
- PIs, as well as any new positions fully or more than 50% funded with CLTC funds, will be expected to participate in at least one CLTC event per semester.

## ADDITIONAL OPPORTUNITIES

In addition to the standard research grant submission process, the CLTC will maintain a small rainy-day 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 consider longer term needs that may serve the broader 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 at cltc@berkeley.edu to discuss.

## ABOUT THE CENTER FOR LONG-TERM CYBERSECURITY

The University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) is a multidisciplinary, campus-wide initiative supporting research, curriculum development, seminars, conferences, and outreach on the future of cybersecurity.

The Center for Long-Term Cybersecurity is made possible by the generous support of The William and Flora Hewlett Foundation. 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/.