CLTC
Center for Long-Term Cybersecurity

102 South Hall Rd
Berkeley, CA 94720
510-664-7506
cltcgrants@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 third annual 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 Thursday October 12, 2017 by 11:59pm PDT.

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.
- 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.

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.

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 four priority research areas.

Research Priorities:

1) **Cyber Talent Pipeline**—We are interested in projects that will help parse 1) challenges, both in terms of supply and demand, in getting sufficient and sufficiently trained persons working in cybersecurity; 2) challenges related to diversifying the cybersecurity workforce along a number of dimensions (and the possible benefits of doing so more boldly); and 3) opportunities, in terms of policy, incentives, and other solutions, to improve these outcomes.
2) **Security Implications of Artificial Intelligence and Machine Learning**—We encourage proposals that address long-term implications of AI/ML, including challenges for our political systems, economies, and societies. We are interested both in questions within the conventional remit of cybersecurity (e.g., on hacking and surveillance), and broader questions where changes in AI and ML may give rise to serious concerns for humans that rise to the level of security (e.g., in workforce disruption or interference with democratic discourse and electoral processes).
3) **New Cybersecurity Governance and Regulatory Regimes**—We are interested in projects that seek to parse the consequences of the existing cybersecurity regulatory and governance institutions, and any institutional gaps that may result from this current system. We are also interested in projects that explore ways in which a positive difference can be made, including but not limited to 1) domestic restructuring of US government agencies, 2) improved interactions between the US government and private sector actors, and 3) improved international collaboration on issues of cybersecurity.
4) **Protecting Vulnerable Individuals and Organizations**—Certain demographics of individuals—including but not limited to political dissidents, journalists, environmental defenders, refugees/immigrants, human rights advocates, and children/the elderly—face amplified vulnerabilities online. Some are targeted by dedicated adversaries using high-end tools and techniques. Few NGOs and media outlets—particularly outside the developed world—have the capability to protect themselves from these adversaries and level the playing field for online dissent and debate. We are interested in projects that help illuminate this issue.

Each of these interest 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. Applicants will be able to indicate this on the submission platform when uploading their proposals.

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. 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 sub-awards with outside institutions. If your grant application will require a sub-award 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 12, 2017, 11:59pm PDT. Please submit your proposal as a PDF named "CLTC RFP 2017 – [PI Last Name] – Project Title" on the following site. You will need to create an account: https://cltc-rfp17.hotcrp.com/.

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 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 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? 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 **2 pages**, single-spaced. For Discrete Project Grants, please limit the proposal body to **7 pages**, single-spaced.

Appendix
Please include the following information in an appendix at the end of your proposal:

- Biographies for the PI and other key research personnel named in the proposal;
- 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.

Appendices will not count against your page limits.

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 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 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.

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, 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 UC Berkeley. 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 cltcgrants@berkeley.edu to discuss.

RESEARCH EXCHANGE EVENT

If you're interested in learning more about the kinds of projects we fund, we are hosting a Research Exchange on Friday September 8, from 10am-4:30pm, featuring the work of our 2016 grantees. Faculty and researchers from across the Berkeley campus will be presenting. If you are interested in attending, please email cltcgrants@berkeley.edu with the subject line, "CLTC Research Exchange."

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/.