CLTC
Center for Long-Term Cybersecurity

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

REQUEST FOR PROPOSALS: 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' expands and expectations about what constitutes 'security' change in ways that would have been almost unimaginable a few years ago. CLTC believes that a transformative cybersecurity research program should not only grapple with the most interesting and complex challenges of today's socio-technical security environment but also the broader challenges of the next decade's environment. This environment encompasses a heterodox set of security issues that mark out what is truly important and worth protecting where human beings and digital systems interact.

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.

CLTC also seeks to stimulate the entry of new perspectives from cross-disciplinary collaborations and insights, in the interest of building capacity for on-going academic research input into what is becoming one of the most important problems of modern society. Both basic and applied research topics are welcome because both will bear on cybersecurity-relevant practices, technical and otherwise.

PROPOSAL PRIORITIES

CLTC prefers ambitious, 'stretch' proposals that aim at plausible and challenging characteristics of future cybersecurity landscapes that may evolve.

Relevance is much more important than disciplinary pedigree.

CLTC will prioritize the funding of research that has the potential through the development of new insights, basic scientific and otherwise, to transform technology trajectories, legislative and regulatory practices, economic and social incentives, individual user behaviors, and other aspects of practice.

As described in the original proposal to the Hewlett Foundation, CLTC is developing and refining a set of scenarios that build on the output from our inaugural workshop in late May 2015. These scenarios suggest a set of emerging problems that are of particular interest

which we name below. These topics aren't meant to be exclusive, but do indicate the types of heterodox issues on which we hope to facilitate greater attention from the research community:

- Development and deployment of unconventional technologies that modify (or revolutionize) the dynamics of attack and defense, or reflect and respond to continuing insecurity in digital networks

- Relationship between security, competitiveness, and innovation, in both licit and illicit environments

- Models and metaphors for creating and evaluating cybersecurity decision frameworks, within and across languages and cultures

- Data security and property rights, including 1) positive feedback effects that might emerge (i.e., the next attack or theft of data is made easier by virtue of the last one), and 2) new meanings of 'privacy' and personally identifiable information (PII)

- Human behavior and experience – cognitive and emotional – in cybersecurity, including the development of and responses to predictive algorithms on people, groups, organizations, and markets

- Social and political movements broadly related to cybersecurity issues, including new distributional inequalities that affect and are affected by security, and consequences of automation and digitization for labor markets, organizational strategies, and government policies

- Technical and political economy of cyber-crime and deviant/illicit markets

- Non-traditional targets of attack (and defense) that impact areas of human and organizational vulnerability, including data about memory, experience, and emotion.

- Human capital for cybersecurity - how will societies create and allocate the talent and knowledge that is needed?

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

Repeating for emphasis:

- 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 scientifically ambitious 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 SCOPE AND ELIGIBILITY

This is the first round in what will be an annual RFP process. Applicants should be aware that the CLTC anticipates scaling its grantmaking over time.

We anticipate making grants in three general categories:

1. Seed Grants, generally below $10 K. These grants could fund an exploratory study, a small pilot, or other means of 'prospecting' a problem area (including areas that might later be eligible for a multi-year grant under category 3 below).

2. Discrete Project Grants, up to $100 K. These grants intend to fund projects that have defined boundaries with clear outcomes and impact potential.

3. Multi-Year Grants, up to $200 K. These grants intend to fund collaborative research that is more ambitious and potentially uncertain. Applications for a Multi-Year Grant should specify first year milestones, at which point CLTC will review progress with the PI. The second year of funding is contingent on that review.

Principal Investigators ("PIs") applying for CLTC grants must have an active Berkeley research affiliation, and must be enrolled in or have completed a graduate degree. (CLTC will consider funding undergraduate research at a later time.)

CLTC encourages collaboration with outside institutions, academic, commercial, and otherwise, as befits the research program. We also encourage (and we 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.

SUBMISSION PROCESS

The submission process has two stages, both of which are mandatory: a short letter of intent, and a full proposal.

Letters of Intent are due SEPTEMBER 28. Please submit your letter of intent through this website: http://cltc.berkeley.edu/cltc/cltc-grant-letter-of-intent/. In addition to filling out a brief form describing key aspects of the project, the body of the Letter of Intent should be a very brief concept note (less than 1 page, in PDF format) describing the basic thrust of the

research effort, principal goals, and how it fits with CLTC objectives. CLTC will be happy to assist in match-making among projects and people with common interests if the need arises — thus, it would be appropriate to submit a letter of intent that is not yet fully staffed but has within it a request for assistance in identifying needed intellectual resources.

Full Proposals are due by OCTOBER 26. The link for the full proposal submission site will be distributed to all Principal Investigators who file a Letter of Intent. Proposals should follow the following format:

Cover Sheet (no more than one page). Please include:
- Title of Proposal and which category of grant is being requested.
- Principal Investigator and contact information
- Key additional personnel and contact information
- Project Proposal Abstract, with a short non-technical description that describes the problem to be studied and why it is important; and a technical description that summarizes the goals and scope of the research, the methods that will be used, and the potential significance of findings.
- Statement of 'Deliverables': what form will the results of this research take?

Proposal Body (for Seed Grants, not to exceed 2 pages; for Discrete Project Grants, not to exceed 5 pages; for Multi-Year Grants, not to exceed 7 pages).

The proposal body should include standard elements that describe and justify the research such as:

- What questions will be addressed and how will they be addressed?
- What methodological and/or theoretical foundations ground this work? How will the results of this work contribute to broader theory development?
- What new insights and knowledge is likely to be generated as a result of this work? What are possible stretch outcomes?
- Who are the major constituencies, scientific and practical, that will find this work useful? How might results of this work influence future research programs and/or policy, practices, behaviors, regulations, and the like?
- How will this work contribute to the broader CLTC agenda?
- How will the risks —scientific and otherwise, including any ethical concerns — be addressed?
- How will you measure progress against your goals?

The final page of the proposal should address practical points such as

- Roles of key research personnel
- Basic schedule and identification of any relevant milestones

- Budget: how will the funds be used? Please break down the costs by category (people, travel, facilities, etc.)
- Any other sources of support for the project, including matching grants and pending grant proposals

Please append bios for the PI and other key research personnel named in the proposal.

The CLTC will host an informal, non-obligatory Information Session on the grant application process in South Hall, Room 107, on September 7 from 4:00-5:00pm. CLTC will also host a handful of office hours for those seeking one-on-one advice; please check the CLTC website for more details.

In addition to the standard research grant submission process, the CLTC will maintain a small rainy-day fund for urgent, opportunistic use (i.e. 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.

On the other side of the spectrum, while not a part of this Request for Proposals, we strongly encourage conversations about perceived longer term needs for collective resources, facilities, and other research 'infrastructural' elements that CLTC could help to develop within the overall Berkeley cybersecurity research community. Please contact the Center to discuss your aspirational ideas on this score.

REVIEW PROCESS AND CONDITIONS OF AWARD

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 in-practice cybersecurity behaviors, technologies, policies, markets, conflicts, etc.

All awards will be made with these conditions:

- A short (~2 page) report describing scientific progress and outcomes to be submitted to CLTC within one month of the end of the grant period.
- An abstract (in simple, jargon-free language) to be posted on CLTC's website, submitted within 2 weeks of funding approval
- Acknowledgement of CLTC support in publications and other means of disseminating research results

For Discrete Project Grants and Multi-Year Grants, these additional conditions will apply

- Recipients will be asked to describe their work to a broader, non-academic audience, for example through a blog post or short video for the CLTC website
- PIs will 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 acknowledged to be part of the CLTC community on the CLTC website, and will be expected to participate in at least 1 CLTC event a semester

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 http://cltc.berkeley.edu/.