CLTC
Center for Long-Term Cybersecurity
UC Berkeley

# The Center for Long-Term Cybersecurity
# CLTC Fall 2021 Request for Proposals

The University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) is committed to helping individuals and organizations address tomorrow's information security challenges to amplify the upside of the digital revolution. CLTC believes that a transformative research agenda which addresses the most interesting and complex challenges of the socio-technical security environment that will evolve over this coming decade is needed to advance this mission. In our sixth annual request for proposals (RFP), we will fund research on a wide range of digital security issues, and we encourage researchers from a variety of disciplines to apply. Proposals are due on **Sunday, November 7**, **2021 by 11:59pm** PDT. Submission instructions can be found below under "**Submission Process.**"

## GOALS

The primary goal of this RFP is to support graduate student researchers at UC Berkeley who are looking 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.
- 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

**Proposals may seek up to $25,000 in funding.** Awards for projects that pursue an exploratory study, a capstone project, a small pilot or other means of 'prospecting' a problem area are more likely to be funded under $10,000. Awards for more mature projects with defined boundaries, clear outcomes, and anticipated impact are more likely to be funded in the $15,000-$25,000 range. Proposals for renewal funding for projects previously supported by CLTC will be considered in this category.

## RESEARCH AREAS

CLTC will consider proposals in all domains relevant to cybersecurity. The openness of that statement is intentional, as we continue to expand the range of disciplines and types of expertise and knowledge that can be brought to bear. 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**
- **Security implications of emerging technologies (e.g 5G Networks, Quantum Computing)**
- **Political, market, and legal 'shapers' of cybersecurity outcomes**
- **Behavioral and 'usable' cybersecurity**
- **Cybersecurity representations, culture, and public dialogue (including art of any medium)**
- **Cybersecurity in the health sector**

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

This RFP is limited to proposals from graduate student researchers, both individuals and teams. All proposals must have a Project Lead[1] who will be enrolled in a graduate degree at UC Berkeley during the grant term January-December 2021. The Project Lead will be the primary contact for all communications with regard to your proposal. It is unlikely that any one Project Lead will be funded for multiple projects. All proposals, including proposals for renewal funding for projects previously supported by CLTC, will be given equal consideration. Funding for renewal proposals will not be disbursed until previous funds have been spent down and any funding deficits have been cleared. We strongly encourage all student researchers to identify a faculty supervisor for your proposed research.

## SUBMISSION PROCESS

Please submit your proposal through this form. The form will request that you upload a PDF of your proposal; please use the following naming convention for your attachment: "CLTC RFP 2021 – [Project Lead 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,

[1] CLTC utilizes the title "Project Lead" in place of "Principal Investigator (PI)" because UC Berkeley graduate students do not formally have "PI status" on campus.

policies, markets, conflicts, etc. We look favorably on proposals that plan for practical dissemination of research results.

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.

The proposal body should not exceed four pages, single-spaced.

## APPENDIX

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

- Biographies for the Project Lead and other key research personnel named in the proposal. (Note: if applicable, please include the name, departmental affiliation, and email address of your faculty supervisor.);
- 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). This would be the UC Berkeley financial contact for the project’s faculty supervisor. If a faculty supervisor has not been identified for your project, please indicate that here.

## 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 research personnel, 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;
- Upon request, participation in CLTC's annual Research Exchange, an event featuring brief presentations from CLTC grantees on their research in progress;
- Upon request, 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.

## RESEARCH EXCHANGE EVENT

Researchers interested in learning more about the kinds of projects we fund are invited to attend the CLTC's virtual Research Exchange, which will be held on **October 7, 2021 from 10:00am-12:00pm,** and will feature presentations by several of our 2020 and 2021 grantees. If you are interested in receiving more information on this event, you can 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 mailing list and receive more information about our events, please email cltc@berkeley.edu or visit our website at https://cltc.berkeley.edu/contact-us/.