NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 23-091

Dear Colleague Letter: Supporting Cybersecurity & Privacy Education and Workforce Development

April 24, 2023

Dear Colleagues:

Cybersecurity and privacy research evolves constantly and rapidly to address current and emerging threats, and it is critical that educational and training curriculum evolve in lockstep with these advances. There is a critical need for novel educational and pedagogical approaches to build a highly skilled cybersecurity and privacy workforce to protect and defend U.S. cyberspace, ensure national security, and mitigate harms to individuals and communities from the use of digital technologies. The National Science Foundation's (NSF) Secure and Trustworthy Cyberspace (SaTC) program views security and privacy as a multidisciplinary subject that can lead to fundamentally new ways to design, build, and operate cyber systems; protect existing infrastructure; and motivate and educate individuals about cybersecurity. The education (EDU) designation in SaTC is focused on the development of evidence-based and evidence-generating approaches that will improve cybersecurity education and workforce development at the K-12, undergraduate, graduate, and professional education levels. This Dear Colleague Letter (DCL) aims to complement efforts under the EDU designation, as well as efforts to strengthen the national cybersecurity workforce pipeline via the NSF CyberCorps®: Scholarship for Service program and the Cyber Defense Education and Training program at the Cybersecurity and Infrastructure Security Agency.

This DCL invites novel and transformative approaches for formal or informal educational innovations in cybersecurity and privacy, and identifies opportunities for two types of additional funding: education supplements to existing SaTC research awards, and EArly-concept Grants for Exploratory Research (EAGER) proposals.

- Education supplements: Principal Investigators (PIs) on all existing SaTC Small, Medium, Large, and Frontier awards (Core and Transition to Practice) and Faculty Early Career Development Program (CAREER) and Computer and Information Science and Engineering (CISE) Research Initiation Initiative (CRII) awards may submit a supplemental funding request for an education supplement to enable the co-evolution of

cybersecurity curricula with the state-of-the-art in the cybersecurity body of knowledge. These requests should leverage the original SaTC project to rapidly translate research advances to novel educational materials that can lead to new ways of teaching and learning cybersecurity concepts and principles.
- EAGER proposals: The EAGER type of proposal supports exploratory work, in its early stages, on untested but potentially transformative research ideas or approaches. This work may be considered especially "high risk – high payoff" in the sense that it, for example, involves radically different approaches, applies new expertise, or engages novel disciplinary or interdisciplinary approaches to cybersecurity education and workforce development.

Proposals and supplemental funding requests should clearly describe the approach, expected outcomes, and budget for the proposed effort. The proposed effort, as outlined in the following paragraphs and bullet list, should be focused on advancing cybersecurity and privacy education and workforce development.

Proposals and supplemental funding requests that demonstrate innovation, feasibility, and potential for development of education and workforce skills on all research topics within the scope of the SaTC program are welcome, and submissions that describe an interdisciplinary approach are especially encouraged. Of particular interest are proposals and supplemental funding requests that target emerging areas such as artificial intelligence and machine learning (including generative AI), cyber-digital assets (such as digital ledgers, blockchains, and cryptocurrencies), software assurance and resilience, virtual and augmented reality, wireless networking, and quantum computing. The submissions should emphasize secure- and privacy-by-design approaches, and multidisciplinary socio-technical aspects of cybersecurity and privacy including understanding of data protection and privacy laws and their ramifications as well as the threats, risks and harms of emerging technologies.

Proposals and supplemental funding requests are encouraged to consider ethics and accountability through the integration of social and behavioral content into technical programs. Programs that aim to diversify the workforce including through participation of Minority Serving Institutions are particularly encouraged. Submissions may outline efforts that can be undertaken across one or more age groups, communities, or education levels to achieve these goals. Possible activities include but not limited to:

- Developing new curriculum, training or teaching materials, laboratory enhancements, or hands-on educational tools in cybersecurity and privacy that will address significant gaps in the knowledge and skills of the Nation’s cybersecurity and privacy workforce;
- Developing programs to initiate or evolve cybersecurity that expand education delivery methods for K-12 students, teachers, counselors and post-secondary institutions and encourage students to pursue cybersecurity careers;
- Designing novel approaches to help undergraduate and graduate students understand

and participate in design, development, management, commercialization, and operation of cybersecurity and privacy solutions, and lab-to-market processes; and
- Establishing a methodology for evaluating the effectiveness of cyber-training activities, events and exercises intended to lead to expert-level performance in trainees, and using the results of evaluation to enable development and iterative improvement of training programs that address the rapidly changing threat ecosystem.

SUBMISSION PROCESS

Supplemental funding requests: Prior to submission of a supplemental funding request, PIs must submit a one-page summary of the proposed topic and approach for review by NSF. The one-page summary (PDF preferred) should be sent to SaTC@nsf.gov, with a CC to the award's cognizant program director by May 23, 2023. Please use the subject line "Education DCL: Supplement:" followed by the title of the project and include the 7-digit award number for which the supplement is requested. PIs for projects selected for additional consideration will be notified no later than June 7, 2023, that they are invited to submit a supplemental funding request. The request must be prepared in accordance with the guidance for supplemental support specified in the NSF Proposal and Award Policies and Procedures Guide (PAPPG) Chapter VI.E.5 and must be submitted through Research.gov no later than July 7, 2023. Supplements submitted without an invitation from the SaTC program officer will be Returned Without Review; the notification should be uploaded in research.gov as a Supplementary Document part of the proposal submission. The amount for the supplement must be no more than 20% of the original award amount, less any supplements already awarded (with the exception of REU & RET supplements). Supplements to collaborative projects made as separate awards are welcome; it is at the discretion of the PIs whether some or all of the institutions in the collaborative team submit supplement requests. Also, in the case of supplements to collaborative projects made as separate awards, each award must have its own supplement request (i.e., there are no collaborative supplements across multiple awards) and must individually adhere to the 20% limit.

EAGER proposals: Prior to submission of an EAGER proposal, PIs must submit a two-page concept outline of the proposed topic and approach for review by NSF. The two-page concept outline (PDF preferred) should be sent to SaTC@nsf.gov by May 23, 2023. Please use the subject line "Education DCL: EAGER:" followed by the title of your project. PIs for selected topics will be notified no later than June 7, 2023, that they are invited to submit an EAGER proposal; the notification must be uploaded in research.gov as a Supplementary Document part of the proposal submission. The proposal must be prepared in accordance with the guidance contained in PAPPG Chapter II.F.3 and must be submitted through Research.gov no later than July 7, 2023. Proposers should select the current PAPPG as the funding opportunity and direct proposals to the Secure and Trustworthy Cyberspace (SaTC) program in the CISE Directorate.

For both supplements and EAGERs, the one-page summary (supplements) or two-page concept outline (EAGERs) should include the names of the team members and institutions and the title of the project, so it can be reviewed even if separated from the email where it is submitted.

Sincerely,

Margaret Martonosi, Assistant Director
Directorate for Computer and Information Science and Engineering (CISE)

James L. Moore III, Assistant Director
Directorate for STEM Education (EDU)

Susan S. Margulies, Assistant Director
Directorate for Engineering (ENG)

Sean L. Jones, Assistant Director
Directorate for Mathematical and Physical Sciences (MPS)

Sylvia M. Butterfield, Acting Assistant Director
Directorate for Social, Behavioral and Economic Sciences (SBE)