NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 20-072

Dear Colleague Letter: Letter: Cybersecurity Education in the Age of Artificial Intelligence

April 6, 2020

Dear Colleagues:

The National Science Foundation (NSF) is announcing its intention to fund a small number of Early Concept Grants for Exploratory Research (EAGER) to encourage advances in cybersecurity education, an area supported by the Foundation's Secure and Trustworthy Cyberspace Education Designation (SaTC-EDU), CyberCorps®: Scholarships for Service, and Advanced Technological Education (ATE) programs

EAGER is a mechanism to support 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 perspectives.

In particular, with this Dear Colleague Letter (DCL), we wish to alert you to our interest in using the EAGER mechanism to encourage new collaborations between the Artificial Intelligence (AI), cybersecurity, and education research communities.

The 2019 Federal Cybersecurity Research and Development Strategic Plan [1] highlighted the mutual needs and benefits of AI and cybersecurity. AI techniques are expected to enhance cybersecurity by assisting human system managers with automated monitoring, analysis, and responses to adversarial attacks. Conversely, it is essential to guard AI technologies from unintended uses and hostile exploitation by leveraging cybersecurity practices. Research results at the intersection of AI and cybersecurity can lead to widespread changes in our understanding of the foundations of cybersecurity, and in turn, give rise to fundamentally new ways to motivate and educate students about cybersecurity in the age of AI. Likewise, the summary report for a June 2019 technical workshop on "Artificial Intelligence and Cybersecurity: Opportunities and Challenges" noted how the interplay between AI, machine learning, and cybersecurity will continue to introduce new opportunities and challenges in the

security of AI as well as AI for cybersecurity. Basic research in AI together with research on cybersecurity education might expand existing AI opportunities and resources in cybersecurity education and workforce development. Education efforts are needed to foster workforce knowledge and skills about applying AI expertise to cybersecurity as well as building robust and trustworthy AI. This DCL seeks to promote exploration of possible partnerships between AI researchers, cybersecurity researchers, and education researchers in order to inspire novel education and outreach efforts. Such collaborative efforts could also foster a robust workforce with integrated AI and cybersecurity competencies, and develop an informed public that understands the privacy, confidentiality, ethics, safety, and security implications of AI.

Opportunities for participation by undergraduate and graduate students and postdoctoral fellows, K-12 students, industry representatives, and others are encouraged. NSF welcomes proposals that include efforts to broaden participation of underrepresented groups (women, minorities, and persons with disabilities) in the development of the research and education agendas.

INSTRUCTIONS:

Responses to this DCL will be handled as a two-step process:

Step 1: Teams are required to send a research concept outline, including project title, team members, institutions involved, and a summary of the project concept (up to two pages) by email to satc-edu@nsf.gov. Two rounds of submissions are available with the deadline for the first round at midnight EDT on **May 15, 2020**, and for the second round at midnight EDT on **August 31, 2020**. To ensure proper processing, please begin the proposal title as well as the subject line of your initial email with: "**EAGER: SaTC AI-Cybersecurity**". NSF Program directors will review these research concept outlines and will invite the authors of those of most interest to submit full EAGER proposals.

Step 2: Those who have been invited will submit their EAGER proposal for review. Submissions received without an invitation from an NSF program director will be returned without review.

To prepare a proposal responsive to the program outlined in this DCL, the following guidelines should be addressed:

1. Proposals submitted pursuant to this DCL should include teams of PIs who have demonstrated expertise in AI, cybersecurity, and education research.
    - Proposals may include two (or more) PIs from a single institution or PIs from several institutions (a collaborative proposal).
    - A PI may participate in only one submission pursuant to this DCL.

2. Proposals should describe how the contribution of each discipline (AI, cybersecurity, and education research) will contribute to intellectual merit and broader impacts for the cybersecurity education research community. Ideally, the research will be interdependent and integrated, will contribute novel understanding, will impact the security, privacy, and trustworthiness of AI, and provide innovation in cybersecurity education. The research will make contributions valued by the AI, cybersecurity, and education research communities. The desired level of integration and impact may require extra efforts in leadership, regular communication, and cross-training during the project. Proposals must describe how such collaboration will work in the planning, research, and dissemination stages. Proposals must have clear and specific plans for assessment and evaluation.

3. EAGER is a funding mechanism for supporting exploratory work, in its early stages, on untested but potentially transformative research ideas or approaches. Thus, proposals responsive to this DCL must include a section stating their appropriateness for an EAGER award (for instance, proposals submitted in response to this DCL may be "high-risk, high-reward" by way of involving radically different approaches, applying new expertise, or engaging novel disciplinary or interdisciplinary perspectives). EAGER proposals may request up to $300,000 over two years.

Submission of EAGER proposals will be via Fastlane or Grants.gov. EAGER submissions should follow the guidelines for EAGER proposals contained in Chapter II.E.2 the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG). The complete text of the PAPPG is available electronically on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.

Please contact the following SaTC program directors with any questions regarding this DCL - Li Yang, James Joshi, and Nigamanth Sridhar - at satc-edu@nsf.gov.

Sincerely,

Karen Marrongelle Assistant
Director, EHR

Margaret Martonosi Assistant
Director, CISE

---

[1]https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf