National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

NSF 14-075

Dear Colleague Letter: Cybersecurity Education EAGERs - Pushing the Dimensions of the Domain

May 29, 2014

Dear Colleagues:

The National Science Foundation (NSF) is announcing its intention to fund a small number of Early Concept Grants for Exploratory Research (EAGERs) to encourage advances in **cybersecurity education**, an area supported by the Foundation's Secure and Trustworthy Cyberspace (SaTC) (see solicitation NSF 13-578: http://www.nsf.gov/pubs/2013/nsf13578/nsf13578.htm) and CyberCorpsÂ®: Scholarship for Service (see solicitation NSF 14-510: http://www.nsf.gov/pubs/2014/nsf14510/nsf14510.htm) programs.

EAGER is a mechanism for supporting 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 that we are interested in using the EAGER mechanism to encourage new collaborations between the cybersecurity research and computing education research communities. The proposed research should fit the Cybersecurity Education (EDU) perspective within the SaTC solicitation.

The results of SaTC-funded research can lead to widespread changes in our understanding of the foundations of cybersecurity that can, in turn, give rise to fundamentally new ways to motivate and educate students about cybersecurity. Basic research in cybersecurity together with research on learning can address the challenge of expanding existing educational opportunities and resources in cybersecurity. Below are some examples of research pathways that could facilitate advances in how cybersecurity education is defined, delivered, and assessed. This list is by no means intended to be complete, nor is it meant to suggest what topics are of interest to NSF; instead, it is meant to give some notion of the broad spectrum of possibilities for such research under this DCL.

- Identification of the core knowledge and skills that cybersecurity professionals should understand and possess.
- Identification of the core knowledge and skills that all computer science students should understand and possess in the context of secure software development and other cybersecurity areas.
- Identification of the core cybersecurity knowledge and skills specific engineering disciplines (e.g., civil engineering, bioengineering) should understand and possess, particularly in the context of their engineering discipline.
- Identification of the implications for educational practice, innovation, and assessment of the interdisciplinary nature of cybersecurity education.

- Development of mechanisms that facilitate agile adjustment of cybersecurity education, integrating current cybersecurity practices and content.
- Evaluation of the efficacy of various instructional delivery methods and assessment strategies such as lab-based, hands-on learning, case studies, and collaborative as well as competitive project-based learning.
- Facilitation of the growth and development of the cybersecurity education community by gathering educational materials into centralized resource repositories and networks.
- Identification of characteristics of cybersecurity learners, and relationships between present instructional practices and barriers to inclusion, recruitment, and retention of women and underrepresented populations.
- Development of alternative credentialing and multiple pathways into cybersecurity.
- Development of curriculum delivery models that address unique and specific cybersecurity education challenges such as making room for dedicated courses, weaving instruction throughout courses in existing programs, expanding undergraduate coursework and programs of study, and aligning with core concepts.

The process for submission is as follows:

- Investigators should e-mail a two-page summary of their idea(s) (plus references and CVs on additional pages, if desired) to Victor Piotrowski, Valerie Barr, Jeremy Epstein, and Harriet Taylor at satc-edu@nsf.gov. The deadline for consideration is August 1, 2014. There is no specified format for these summaries, but a brief statement of how the proposed work furthers cybersecurity education should be included. The two-page summary should not include any budget information.
- NSF Program Directors will review the two-page summaries, and will invite those of most interest to submit EAGER proposals. Notifications for first-round submissions are expected by September 1, 2014.
- The anticipated deadline for submission of invited EAGER proposals is September 30, 2014.Â Submission of EAGER proposals will be via Fastlane or Grants.gov.
- EAGER submissions should follow the NSF's *Grant Proposal Guide* (GPG) II.D.2 (see http://www.nsf.gov/publications/pub_summ.jsp?ods_key=gpg).

Investigators are encouraged to review the final report of a recent cybersecurity education workshop at https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf.

An investigator may be included as a PI or a co-PI in only one submission in response to this DCL; if more than one is submitted, only the first one submitted will be considered.

For further information, please contact the cognizant program directors - Victor Piotrowski, Valerie Barr, Jeremy Epstein, and Harriet Taylor - at satc-edu@nsf.gov.

Sincerely,

Farnam Jahanian
Assistant Director, CISE

Joan Ferrini-Mundy
Assistant Director, EHR