NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

NSF 15-005

Dear Colleague Letter: SaTC EAGERs Enabling New Collaborations

October 23, 2014

The National Science Foundation is announcing its intentions to build upon the success of previous Early Concept Grants for Exploratory Research (EAGERs) in the area supported by the Secure and Trustworthy Cyberspace (SaTC) program (see solicitation 14-599: http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf14599) and to accept additional EAGER proposals that encourage novel interdisciplinary research resulting from new collaborations between one or more Computer and Information Science and Engineering (CISE) researchers and one or more Social, Behavioral and Economic Science (SBE) researchers. (Research teams with a history of collaborating together should instead submit directly to the SaTC solicitation.) The proposed research should fit both the Trustworthy Computing (TWC) and the Social, Behavioral and Economic (SBE) Sciences perspectives within the SaTC solicitation.

Below are some examples of the types of topics that computer and social and behavioral scientists could conceivably study together under such an EAGER project. This list is by no means intended to be complete, nor is it meant to suggest what topics are of interest to the NSF. Instead, it is meant to give some notion of the broad spectrum of possibilities for such research. The respective role of social and computer scientists under different topics may vary from fully interdisciplinary involvement of both, which would be ideal, to varying degrees of mutual consultation and resource provision.

- Incentive, communication, and profitability mechanisms of attackers.
- Modeling and experimentation to identify the strengths and weaknesses of incentive mechanisms for enhancing security, particularly in realistic cyber-contexts.
- Methods, including automated methods, for detecting deception or adverse intentions *relevant to attacks on cyberinfrastructure*.
- Social network analysis and other methods of detecting malware propagation, for instance via social media.
- Socio-technical solutions to reduce end-user risk exposure, such as crowdsourcing.
- Research to ascertain the tradeoffs between security and privacy and how better mixtures of these could be found or negotiated.
- Methods, including automated methods, to train, incentivize, or nudge end-users to improve their cybersecurity position.
- The impact of norms and other factors on promoting good citizenship with respect to cyberspace.
- End-user motivating factors that allow successful security invasion tactics and countermeasures.
- Cyber-security insurance: obstacles and solutions.
- The privacy needs of end-users and organizations and how these constrain or do not constrain cybersecurity efforts.
- Motivators and indicators of insider threat and countermeasures to such threat among end-users, user communities, national and international communities, and so forth.
- Factors behind susceptibility of subpopulations to cybercrime e.g., youth, the elderly and

countermeasures.
- The impact of trust and institutional design on cybersecurity decisions.
- Incentives and motivators for cybersecurity in firms and other organizations.
- International norms, rules of engagement, and escalation dynamics of cyber-attacks and cyber-warfare.
- Systemic and structural factors that promote or undermine a secure cyberspace.

The above topics could involve an array of social science fields, including, but not limited to: economics, sociology, psychology, political science, science of organization (organizational research/management science), communication research, education research, linguistics, and anthropology. The subfields that may be relevant are many, and can include such areas as behavioral economics, behavioral decision theory, behavioral game theory, game theory, political psychology, social network analysis and theory, social psychology, cognitive psychology, online communication research, and criminology.

Two rounds of submissions are anticipated, with approximately 4 to 5 EAGERs to be awarded during each round, subject to the availability of funds.

The process for submission is as follows:

- Investigators should e-mail a two-page summary of their research idea(s) (plus references and CVs on additional pages, if desired) to jepstein@nsf.gov. The deadline for consideration in the first round is December 1, 2014; the deadline for consideration in the second round is March 2, 2015. There is no specified format for these summaries, but a brief statement of any prior collaboration between the proposing PIs should be included.
- 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 January 16, 2015, and for second-round submissions by April 1, 2015.
- The anticipated deadlines for submission of invited EAGER proposals are February 17, 2015, and May 1, 2015 for the first and second rounds, respectively. 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). Additionally, they must indicate that the collaboration is new and should clarify how the proposed collaboration will take place. (As noted in the GPG, EAGER is a funding 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," for example, in the sense that it involves radically different approaches, applies new expertise, or engages novel disciplinary or interdisciplinary perspectives.)

Investigators are encouraged to review the abstracts of projects funded under the previous Dear Colleague Letters (http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf13037 and http://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf14016) to understand representative topics and approaches that may be of interest to NSF[1].

An investigator may be included in only one submission in response to this Dear Colleague Letter (DCL); if more than one is submitted, only the first one submitted will be considered. Submission in response to the previous Dear Colleague Letters does not preclude submission in response to this DCL.

For further information, please contact the cognizant SaTC program directors at satc@nsf.gov.

Sincerely,

Suzanne Iacono
Assistant Director (Acting), CISE

Fay Lomax Cook
Assistant Director, SBE

---

[1]See award nos. 1343141, 1343528, 1343430, 1343433, 1343453, 1343766, 1347075, 1347113, 1347151, and 1347186 (FY13 awards), along with 1444633, 1444827, 1444823, 1444840, 1444861, 1444863, 1444871, 1444500, 1445079, 1450193, 1450500, 1450600, 1450619, 1450624, and 1450625 (FY14 awards) in the NSF award database (http://www.nsf.gov/awardsearch).