National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

NSF 13-037

Dear Colleague Letter - SaTC EAGERs Enabling New Collaborations Between Computer and Social Scientists

Date: 12/31/12

NSF expects to fund a small number of Early Concept Grants for Exploratory Research (EAGERs) in the area supported by the Secure and Trustworthy Cyberspace (SaTC) program (see solicitation NSF 12-596: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709). 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" in the sense that it, for example, involves radically different approaches, applies new expertise, or engages novel disciplinary or interdisciplinary perspectives.

With this DCL we wish to alert you that we are particularly interested in using the EAGER mechanism to 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 and the Social, Behavioral and Economic 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 directly relevant to cyber-attacks.
- 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 evasion 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.

Interested investigators must first discuss ideas with the cognizant SaTC program directors and, upon program director approval, may then submit an EAGER proposal in accordance with the NSF's Grant Proposal Guide II.D.2 (http://www.nsf.gov/pubs/policydocs/pappguide/nsf13001/gpg_2.jsp#IID2). Because of limited funding, PIs are encouraged to act as soon as possible. Proposals will be accepted through August 31, 2013. In addition, the proposal must indicate that the collaboration is new and should clarify how the proposed collaboration will take place.

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

Sincerely,

Keith Marzullo
Division Director, CISE/CNS

Jeryl Mumpower
Division Director, SBE/SES