National Science Foundation
4201 Wilson Boulevard
Arlington, Virginia 22230

NSF 13-131

Dear Colleague Letter: Toward a Research Coordination Network (RCN) Addressing Experimental and Evaluation Methods and Techniques for Cybersecurity

Date: September 19, 2013

With this Dear Colleague Letter, the NSF Secure and Trustworthy Cyberspace (SaTC) program wishes to notify the community of its intent to support and foster a multi-year community dialog about leveraging experimental and evaluation techniques from multiple disciplines to further the science of cybersecurity.

Specifically, NSF expects to support at least one Research Coordination Network (RCN) under the SaTC umbrella (see NSF 13-578: http://www.nsf.gov/pubs/2013/nsf13578/nsf13578.htm). RCN (see NSF 13-520: http://www.nsf.gov/pubs/2013/nsf13520/nsf13520.htm) is a funding mechanism for advancing a field by supporting groups of investigators to communicate their activities – in this case, across disciplinary boundaries. A RCN does **not** support primary research; rather, a RCN supports the means by which investigators can share information, develop community standards, and advance science and education through communication and sharing of ideas.

From its inception, the SaTC program, and the cybersecurity community more broadly, has recognized that this problem space requires a coordinated multi-disciplinary approach, involving not only traditional computer science but also advances in many other diverse disciplines including the social and behavioral sciences, including psychology, sociology, and economics. Over time, each discipline has developed its own body of techniques and standards, suited toward its core area of expertise. The potential benefits to a researcher of crossing disciplinary boundaries are clear: a computer scientist, for example, can make use of the techniques established by social scientists on how to properly conduct human studies. In practice, however, both social and technical obstacles arise. For example, a researcher might fail to realize that a common experimental technique assumes statistical independence or the absence of strategic behavior; when applied to a cybersecurity application, such assumptions may be invalid. Another obstacle is that peer reviewers can often have difficulty accurately assessing unfamiliar methodologies.

As a result, NSF would like to foster a general understanding in the cybersecurity research community regarding:

- Research methodologies and analysis techniques from the social, behavioral, and economic sciences (SBE) that can be applied toward cybersecurity but are not currently widely used (or used at all) by computer and information scientists;
- Methodologies and techniques that are currently in use by computer and information scientists but could be better applied and improved;
- Methodologies and techniques that are best suited for particular classes of cybersecurity problems;
- Limitations and hidden assumptions in analysis techniques;
- Effective means for cybersecurity researchers to learn about, and effectively use, appropriate

methodologies and techniques, particularly those developed outside of their own disciplines; and
- Threats to internal and external validity of experiments (or other research studies) caused by technological and social changes.

It is therefore anticipated the RCN will:

- Involve a steering committee that represents a diverse set (in terms of use of methodology) of cybersecurity researchers;
- Present a well-defined plan for (a) identifying sub-communities with different methodological or analytic needs and interests, and (b) effectively interacting with them;
- Not be a pre-ordained declaration about how cybersecurity research should be conducted, but instead be open to input from the community more broadly;
- Describe concrete plans for dissemination and outreach of results to multiple and diverse sub-communities; and
- Offer concrete evaluation plans to ensure effectiveness.

This Dear Colleague Letter will be in effect until December 15, 2013. PIs are encouraged to refer to the RCN solicitation (see NSF 13-520: http://www.nsf.gov/pubs/2013/nsf13520/nsf13520.htm) for detailed instructions and review criteria. It is anticipated that the RCN will be funded at up to $500,000 for up to three years.

For further information, please contact the cognizant Program Directors at satc@nsf.gov.

Sincerely,

Keith Marzullo
Division Director, CISE/CNS

Jeryl Mumpower
Division Director, SBE/SES