NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

NSF 17-061

Dear Colleague Letter: Encouraging Submission of Industry/University Cooperative Research Centers (IUCRC) Proposals in the Area of Cybersecurity

March 9, 2017

Dear Colleagues:

For over 40 years, the National Science Foundation's (NSF) Industry/University Cooperative Research Centers (IUCRC) program has fostered long-term partnerships among academe, industry, and government in various technology sectors through multi-university industry-focused research centers. These partnerships, developed through the cooperative execution of precompetitive research, strengthen the U.S. innovation ecosystem and the Nation's overall economic competitiveness. Precompetitive research conducted by IUCRCs addresses application-inspired fundamental topics that industry recognizes as longer-term challenges; industry members benefit from collaboration with academic partners in the definition and execution of the corresponding research. NSF provides catalyzing investment to the centers, which are primarily supported by industrial members and other stakeholders. The research carried out at each center is of interest to both the center faculty and the center's industry members. IUCRCs contribute to the Nation's research infrastructure base and enhance the intellectual capacity of the science and engineering workforce through the integration of research and education. As appropriate, IUCRCs establish international collaborations to advance these goals within the global context.

Cyberspace encompasses computing systems, software systems, information technology, networks, communications systems, and users. It is interwoven in every aspect of society and impacts every major system in our Nation (e.g., telecommunications, financial, energy, transportation, and healthcare). While enabling a vast array of applications, cyberspace and its underlying infrastructure are major targets of threats. Attackers can exploit system vulnerabilities to disrupt or destroy key services; to disable critical infrastructures; to steal critical data, intellectual property, or money; to engage in some type of fraud; and to violate the privacy of individuals, corporations, or government entities. Given the national security risks and substantial economic consequences of cyber-attacks, building a resilient and secure cyberspace is a national problem with global implications. Cybersecurity is extremely challenging due to a number of factors: the scale of cyberspace; the complex interactions within and among systems; the ability of attackers to initiate threats from anywhere in the world; the rapidly increasing number, type, and sophistication of attacks; the widespread use of personal smart devices with Internet connectivity; and the rapidly expanding deployment of cyber-physical systems that integrate various technologies (e.g.,

inexpensive sensors, actuators) with physical systems.

Foundational precompetitive research involving industry, academe, and government stakeholders is critical to the development of innovative and transformative cybersecurity solutions that are scalable, proactive, capable of learning, and adaptive with continuous monitoring and real-time assessment, while adhering to relevant policy and/or transparency regulations. Comprehensive cybersecurity will require scientifically rigorous yet practical solutions along several dimensions: application and software security, network/Internet security, information security, privacy protection, system security, recovery and mitigation, cryptography, usability, and many more. The IUCRC model, in which industry members collectively fund center projects that address shared research challenges, can be enabling to such a critical field by leveraging investment and reducing the risk for each participating member organization.

This Dear Colleague Letter (DCL) encourages collaborations between industry and academe in the area of cybersecurity. The aim is to establish multi-university IUCRCs that, in collaboration with their industry partners, are capable of collectively addressing large-scale and cross-disciplinary challenges in the broad area of cybersecurity. NSF therefore welcomes and encourages proposals in response to the IUCRC program solicitation, NSF 17-516, in the areas outlined in this DCL. This DCL is also complementary to NSF's Secure and Trustworthy Cyberspace (SaTC) program (https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709), and topics highlighted in the SaTC program solicitation (NSF 16-580) are potential areas of precompetitive research that a multi-university IUCRC in cybersecurity might address.

Any precompetitive research that enhances the translation of basic research in the area of cybersecurity would be considered. The structure of IUCRCs promotes extensive industry involvement in research planning and review, which leads to *direct* technology transfer, bridging the gap that traditionally has kept industry from capitalizing fully and quickly on the results of research at academic institutions. This close relationship with industry in IUCRCs through the cooperative research model also ensures the broader impacts of the projects. Thus, any proposed themes should be considered with respect to the nature and structure of IUCRCs.

The NSF IUCRC program seeks to support novel IUCRCs covering unique research themes that do not overlap with other IUCRCs. To avoid the submission of IUCRC proposals overlapping significantly in research focus or industry sectors, any interested Principal Investigator(s) should email a one-page summary of the proposal concept to the cognizant NSF Program Directors listed below.

- Dmitri Perkins, IUCRC Program Director, Division of Computer and Network Systems (CNS), Directorate for Computer and Information Science and Engineering (CISE). Telephone: (703) 292-7096; E-mail: dperkins@nsf.gov.
- Thyaga Nandagopal, Program Director, Division of Computer and Network Systems (CNS), Directorate for Computer and Information Science and Engineering (CISE). Telephone: (703) 292-8950; E-mail: tnandago@nsf.gov.
- Nina Amla, Program Director, Division of Computer and Communications Foundations (CCF), Directorate for Computer and Information Science and Engineering (CISE). Telephone: (703) 292-7991; E-mail: namla@nsf.gov.

Please contact one of the NSF Program Directors listed above if you have questions about this IUCRC

DCL.

Sincerely,

James Kurose
Assistant Director, Directorate for Computer and Information Science and Engineering

Barry Johnson
Assistant Director (Acting), Directorate for Engineering