



NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

NSF 17-072

Dear Colleague Letter: Encouraging Submission of Industry/University Cooperative Research Centers (IUCRC) Proposals in Areas Related to the Internet of Things

March 29, 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.

The Internet of Things (IoT) is an emerging paradigm in the development and deployment of the Internet and has the potential to impact every aspect of daily life. IoT is generally understood to refer to the internetworking of physical devices that contain electronics, sensors, actuators and software, and that are able to collect and exchange data about, and in some cases interact with, the physical environment. These cyber-physical systems (CPS) have the potential to increase efficiency, accuracy, safety, and convenience through increased interconnection and intelligence of the integrated physical and computing environments. At the same time, the trend toward connecting "everything" is rapidly expanding the perimeter or surface of concern that must be secured, and the potential for exposure of personally-identifiable information. Given the projected impact of IoT in nearly every industry sector including healthcare, agriculture/farming, manufacturing, energy, transportation, communication, security, finance, clothing, and sports, foundational precompetitive research is important to enable designs and applications that meet critical performance, security, and privacy guarantees. The IUCRC model, in which industry members collectively fund projects that address shared research challenges, can be enabling to such a nascent 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 research related to IoT specifically and, more broadly, cyber-physical systems. 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 context of IoT. NSF therefore welcomes and encourages proposals in response to the IUCRC program solicitation, [NSF 17-516](#), in the areas outlined in this DCL. Potential areas of precompetitive research that are of interest include, but are

not limited to:

- Mobile technologies and applications;
- Healthcare and biomedical technologies;
- Smart grids and energy management;
- IoT Platforms, sensors, controls, and actuators;
- Agriculture and farming-based applications;
- Smart City/Community applications;
- Transportation and traffic management systems;
- Industrial and Manufacturing applications;
- Metrics, measurements, and benchmarking;
- Standards, practices, and policies (e.g., legal, regulatory); and
- Trust, security, and privacy in IoT.

The above list is provided for illustrative purposes only, and is not meant to be exhaustive. **Any precompetitive research areas that would be applicable within the context of IoT and/or CPS would be considered.**

IoT will certainly involve complex interactions and dependencies at the component, system, and end-to-end levels. This strongly suggests a "security-first approach" where effective technical solutions for security, trust, and privacy are not afterthoughts, but instead are foundational aspects of any IoT device design or end-to-end system. This is especially important in the consumer space, where the incentive to produce low-cost IoT-based consumer appliances could lead to less secure devices with major security and privacy faults. The successful realization of an IoT-enabled world will thus depend not only on solving technical and engineering challenges, but will also require significant collaboration among academe, industry, and government to develop thoughtful and well-crafted standards, practices, and policies (including legal and regulatory) that take into account the complexities and societal implications of the IoT. To this end, **any proposed IUCRC in any area related to IoT must include a clear and compelling plan to address relevant trust, security, and privacy issues within the overall mission of the proposed Center.** Examples of such issues would include, but are not limited to, access control, identity management, policy/standards/best practices, security compliance frameworks, and security benchmarking/testing.

The structure of IUCRCs promotes the 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 broader impacts of the projects. Thus, the areas mentioned above or any other appropriate topic 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 thrust areas 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.
- David Corman, Program Director, Division of Computer and Network Systems (CNS), Directorate for Computer and Information Science and Engineering (CISE). Telephone: (703) 292-8754, email: dcorman@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