NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 20-042

Dear Colleague Letter: Secure Analog-RF Electronics and Electromagnetics (SARE)

February 6, 2020

Dear Colleagues:

While the tremendous growth of interconnected devices has resulted in significant benefits to society, security of these devices has emerged as a major concern. Each communication device or sensor connecting or interacting with other devices, sensors, or the environment has potential security vulnerability. This is particularly important when many wirelessly connected personal electronic devices transmit sensitive personal financial, health, and other private information over the air. Furthermore, while electronic devices with electromagnetic sensing capabilities such as automobile radar and motion-sensing devices are used for safety enhancement, their vulnerability to hacking or exploitation raises concerns on both security and public safety. Current security approaches based solely on digital techniques have limitations when applied to electronic devices with RF and analog functions. To enhance and ensure security of these electronic devices, new approaches employing RF and analog techniques are needed, which may involve novel concepts in materials, devices, circuits, systems, or combinations of them.

With this Dear Colleague Letter (DCL), the Directorate for Engineering and the Directorate for Mathematical and Physical Sciences of the National Science Foundation announce their interest in receiving EArly-Concept Grants for Exploratory Research (EAGER) proposals to support research in fundamental theory, design, algorithm, and experimental verification of RF, analog, and mixed-signal techniques that will significantly enhance and ensure the security of electronic devices. To encourage convergence in research, PIs are expected to submit proposals demonstrating complementary expertise to tackle the challenging security

problems involving multiple disciplines.

Examples of research topics include novel RF, analog, and mixed-signal approaches to:

1. address the security vulnerability caused by electromagnetic emissions;
2. address the security vulnerability originated from the power management circuits;
3. ensure secure communications and sensing within the RF spectrum from kHz to THz;
4. ensure trusted microelectronics going through multiple phases of design, fabrication, packaging, and validation;
5. explore advanced materials and devices that can enhance and ensure security.

Proposals must be prepared and submitted in accordance with the guidance for EAGER proposals contained in Chapter II.E.2 of the NSF Proposal & Award Policies & Procedures Guide (PAPPG). This includes discussing the proposal with at least one of the program directors listed below well before submission, and establishing that the project satisfies the high-risk/high-return expectations for EAGERs. In addition, as stated above, proposals are expected to demonstrate sufficient complementary expertise to tackle the challenging security problems. Proposals may then be submitted to the program of one of the program directors contacted, with the prefix "EAGER: SARE: [title]". Proposals will be evaluated as received. For consideration for funding in Fiscal Year 2020, proposals must be submitted by April 6, 2020.

> Jenshan Lin, ENG/ECCS, jenlin@nsf.gov
> Ruyan Guo, ENG/ECCS, rguo@nsf.gov
> Mohammod Ali, ENG/ECCS, moali@nsf.gov
> Albert Wang, ENG/ECCS, awang@nsf.gov
> Robert Opila, MPS/DMR, robopila@nsf.gov

Sincerely,

Dawn Tilbury
Assistant Director,
Directorate for Engineering

Anne Kinney
Assistant Director,
Directorate for Mathematical & Physical Sciences