NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 23-063

Dear Colleague Letter: Request for Information on Future Directions for the NSF Secure & Trustworthy Cyberspace Program

March 1, 2023

Dear Colleagues:

OVERVIEW

For over a decade, the National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) program has been NSF's flagship cybersecurity and privacy research program, supporting approximately $1 billion in research across nearly 3,000 projects. Over that time, SaTC has expanded and evolved to include topics on interdisciplinary research between computer and information scientists, and social scientists; block-chain/distributed ledgers and cryptocurrencies; hardware security; information integrity; mathematics and statistics; societal aspects of privacy; cyber-physical systems; quantum computing; and education and educational research at the intersection of artificial intelligence, cybersecurity and privacy. SaTC-funded center-scale research activities have focused on cloud computing security, medical devices security, security and privacy for marginalized populations, security for artificial intelligence systems, secure sharing of private data, web privacy, open-source supply chain software security, and Internet of Things security.

As SaTC marks its 10th anniversary, NSF seeks, via this Dear Colleague Letter (DCL), input from industry, institutions of higher education (IHEs), non-profits, state and local governments, and other interested parties on possible topics and future directions for cybersecurity and privacy research.

This DCL does *not* invite research proposals. However, the submission of collective input spanning different perspectives may result in the identification of potential topics for future research funding opportunities. Through this DCL, NSF is providing the community a direct opportunity to offer input on potential novel and far-reaching topic ideas, grand research challenges, and unexplored opportunities for SaTC and/or future programs in FY 2024 and beyond.

No changes to the SaTC solicitation are expected as a result of this DCL before October 1, 2023.

BACKGROUND

The objectives of the SaTC program are to address fundamental scientific research questions across the disciplines of cybersecurity and privacy, including technical, sociotechnical, and educational topics. SaTC also seeks to support Transition to Practice, moving scientific research results from the laboratory into operational settings.

The breadth of the SaTC program is reflected in the topic areas identified in the latest solicitation (NSF 22-517), which lists 20 different research topics and many sub-areas within each. At the same time, it is important to address newer vulnerabilities and the expanding threat landscape and attack surface resulting from the increased reliance of our society on an ubiquitous, internet enabled hyper-connected cyberspace.

OBJECTIVE

The goal of this DCL is to identify a broad range of important research topic areas that the community thinks are currently under-served by or should be part of a cybersecurity and privacy program, including topics that may have currently been considered outside the scope of SaTC. In addition, the DCL seeks to identify areas currently in scope of the program that have matured to a sufficient extent that they should be sun-setted as they no longer need NSF support, and receive funding from industry or application-focused or mission-oriented government agencies. Within those topic areas that the community believes are appropriate for the program going forward, this DCL also seeks input on prioritization. NSF specifically seeks to identify additional areas where disciplinary, interdisciplinary, and multidisciplinary research is needed to address technical and societal challenges.

WHAT NSF IS LOOKING FOR?

Responses must provide the following information:

1. Name [Point of Contact] (up to 100 characters)
2. E-mail (up to 50 characters)
3. Institutional Affiliation (up to 50 characters)
4. Research Topic Area Title (up to 100 characters)
5. What is the research topic area need that is being targeted? (up to 2000 characters)
6. Is this a proposal for a new topic area, or sunsetting an existing topic area? (up to 100 characters)
7. What disciplines will be involved in the research topic area? (up to 200 characters)
8. Who are the major stakeholders (e.g., academia, private industry, government, non-profit) that need to be engaged to address the relevant societal need? (up to 1000

characters)
9. How does this relate to existing topic areas within the scope of the SaTC program? (up to 1000 characters)
10. Why should this research topic area be part of the SaTC program? (up to 500 characters)
11. Do you have any other comments on future directions for the SaTC program? (up to 500 words)

After receiving the DCL input, NSF may hold interactive sessions such as online town halls to seek further refinement of areas identified as being of particular importance.

This DCL seeks input from the whole academic community as well as from non-academic experts such as industry or government thought leaders and experts from the non-profit sector. Submitters may include current SaTC principal investigators (PIs); submission from non-PIs is especially welcomed. NSF encourages suggestions from both seasoned and new researchers coming into the field. NSF strongly encourages groundbreaking/game changing ideas and insights into future cyber security research. Input focusing on individual projects is discouraged.

Submissions from Minority Serving Institutions (MSIs) are particularly encouraged.

TIMELINE

Responses to this DCL must be submitted by **March 24, 2023**.

HOW TO RESPOND TO THIS DCL?

Respond to the survey at https://www.surveymonkey.com/r/nsfsecure_trustworthycyberspace addressing the above ten questions no later than March 24, 2023. Submissions may be from individuals or groups. More than two submissions from any individual are discouraged.

WHAT WILL NSF DO WITH THIS INFORMATION?

NSF will use the information to shape future program designs in the field of cybersecurity and privacy. Please do not include confidential or proprietary information in your submission.

Sincerely,

Margaret Martonosi, Assistant Director
Directorate for Computer and Information Science & Engineering (CISE)

James L. Moore III, Assistant Director
Directorate for STEM Education (EDU)

Susan S. Margulies, Assistant Director
Directorate for Engineering (ENG)

Sean L. Jones, Assistant Director
Directorate for Mathematical & Physical Sciences (MPS)

Sylvia Butterfield, Acting Assistant Director
Directorate for Social, Behavioral, & Economic Sciences (SBE)