

## NSF 22-050

## Dear Colleague Letter: Inviting Proposals Related to Information Integrity to the Secure and Trustworthy Cyberspace Program

February 24, 2022

## Dear Colleagues:

One of the biggest challenges we face in society today is ensuring that the information that we depend on in almost every facet of our lives is accurate and trustworthy. Although information manipulated for political, ideological, or commercial gain is not new, the dissemination of inaccurate information at unprecedented speed and scale in the modern digital landscape is a new phenomenon with potential for vast harm. There are many terms in use to characterize manipulated information, including misinformation, disinformation, and malinformation. By any of these names, wide-spread distortions of the truth serve to undermine public trust in critical democratic institutions and the validity of scientific evidence, and authentic communication. They have potentially destabilizing consequences for national security, democratic processes, economic stability and growth, public health, the natural and built environment, local and national crisis response efforts, human rights and protections, and civil society.

The National Science Foundation's (NSF) Secure and Trustworthy Cyberspace (SaTC) program aims to promote fundamental research on security, privacy, and trustworthy cyberspace as a multidisciplinary subject that leads to new knowledge and approaches to design, build, and operate cyber systems, protect persons, organizations, and existing infrastructure, and motivate and educate individuals about cybersecurity and privacy. The purpose of this Dear Colleague Letter (DCL) is to encourage the submission of novel and high impact proposals that advance knowledge on the integrity of information to the SaTC Program solicitation.

Proposals should tackle more than isolated slices of the entire information ecosystem, which includes the various actors and their different capabilities, actions, incentives, and intentions, and the different platforms and strategies for creating, collecting, disseminating, consuming, and sharing manipulated information. This DCL invites proposals that:

- apply the highest standards of research methodology and use of evidence to characterize the psychological, sociological, economic, and cultural contexts of information manipulation and its consequences;
- design strategies to effectively mitigate violations of information integrity, along with metrics and plans for evaluating the success of those strategies, and systems that are more resistant to those violations;
- measure and understand the consequences and effects of information manipulation on individuals, communities, and institutions, and develop public awareness pathways to build societal resistance to information manipulation; and
- design and develop curricular materials at all levels of education (K-12, post-secondary, adult and other vulnerable populations), both in formal and informal settings, and accompanying pedagogical methods to enable a more informed future citizenry.

Proposals that advance information integrity both within or across disciplines are welcome.

This DCL does not constitute a new competition nor a new program. Rather, interested proposers should prepare and submit proposals in accordance with the instructions in the program solicitation (SaTC Program solicitation) and the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG). We invite submissions to the CORE, EDU and TTP designations of the SaTC solicitation as appropriate to the work proposed. See the SaTC solicitation for more details on these types of proposals, as well as on the kinds of topics the SaTC program is interested in around information integrity. Additionally, to call attention to responsiveness to this DCL, project summaries should include "IntegrityDCL" in the keyword list. Proposals submitted to this DCL will count towards the proposal limits imposed in the SaTC solicitation.

Questions should be directed to: satc@nsf.gov.

Sincerely,

Sylvia Butterfield Acting Assistant Director, EHR

Kellina M. Craig-Henderson Acting Assistant Director, SBE

Margaret Martonosi Assistant Director, CISE

REFERENCES

https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf