Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 22-517

REPLACES DOCUMENT(S):
NSF 21-500

National Science Foundation

Directorate for Computer and Information Science and Engineering
Division of Computer and Network Systems
Division of Computing and Communication Foundations
Division of Information and Intelligent Systems
Office of Advanced Cyberinfrastructure

Directorate for Social, Behavioral and Economic Sciences
Division of Social and Economic Sciences
Division of Behavioral and Cognitive Sciences

Directorate for Mathematical and Physical Sciences
Division of Mathematical Sciences

Directorate for Engineering
Division of Electrical, Communications and Cyber Systems

Directorate for STEM Education
Division of Graduate Education

Full Proposl Deadline(s) (due by 5 p.m. submitter's local time):

Proposals Accepted Anytime

IMPORTANT INFORMATION AND REVISION NOTES

- The limit for SaTC Small submissions is increased from $500,000 to $600,000.
- SaTC will not accept Large proposals in FY22 and FY23.
- Broadening Participation in Computing (BPC) plans are required for Medium proposals at time of submission (was previously only at time of award), if the lead or non-lead organizations are in CISE research areas.
- Descriptions of topic areas have been updated and several have been renamed.

Important Information

Innovating and migrating proposal preparation and submission capabilities from FastLane to Research.gov is part of the ongoing NSF information technology modernization efforts, as described in Important Notice No. 147. In support of these efforts, research proposals submitted in response to this program solicitation must be prepared and submitted via Research.gov or via Grants.gov, and may not be prepared or submitted via FastLane.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 22-1), which is effective for proposals submitted, or due, on or after October 4, 2021.

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Secure and Trustworthy Cyberspace (SaTC)

Synopsis of Program:

In today's increasingly networked, distributed, and asynchronous world, cybersecurity involves hardware, software, networks, data, people, and integration with the physical world. Society's overwhelming reliance on this complex cyberspace, however, has exposed its fragility and vulnerabilities that defy existing cyber-defense measures; corporations, agencies, national infrastructure, and individuals continue to suffer cyber-attacks. Achieving a truly secure cyberspace requires addressing both challenging scientific and engineering problems involving many components of a system, and vulnerabilities that stem from human behaviors and choices. Examining the fundamentals of security and privacy as a multidisciplinary subject can lead to fundamentally new ways to design, build, and operate cyber systems; protect existing infrastructure; and motivate and educate individuals about cybersecurity.

The goals of the SaTC program are aligned with the National Science and Technology Council's (NSTC) Federal Cybersecurity Research and Development Strategic Plan (RDSP) and National Privacy Research Strategy (NPRS) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. The RDSP identified six areas critical to successful cybersecurity research and development: (1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure. The NPRS, which complements the RDSP, identifies a