

Funding Opportunity: NSF Releases Security, Privacy, and Trust in Cyberspace 2.0 Solicitation

Lewis-Burke Associates LLC – December 12, 2024

The National Science Foundation (NSF) has released the updated Security, Privacy, and Trust in Cyberspace (SaTC 2.0) solicitation. SaTC 2.0 aims to increase trust in global cyber ecosystems, which includes the security, privacy, and resilience of cyberspace. SaTC 2.0 includes the NSF Directorates for Computer and Information Science and Engineering (CISE), Mathematical and Physical Sciences (MPS), Social, Behavioral and Economic Sciences (SBE), and STEM Education (EDU). The Engineering Directorate, which participated in the last solicitation, has not joined in this round. Note that the original SaTC program stood for “Secure and Trustworthy Cyberspace (SaTC), the updated solicitation includes Privacy.

Proposals may be submitted in the following categories:

- The Research (**RES**) designation is the core of the SaTC 2.0 research program and will support projects up to \$1.2 million for up to four years. Proposals over \$600,000 must include Broadening Participation in Computing and collaboration plans. RES proposals may include an optional Transition to Education (TTE) plan up to \$50,000 (within the RES total) to develop education activities aligned with the proposed research.
- The Education (**EDU**) designation is for proposals focused on SaTC education and workforce training. EDU proposals are up to \$500,000 for up to three years. EDU proposals that include cybersecurity experts and education researcher(s) on the PI team may request an additional \$100,000 beyond the \$500,000 limit.
- The Seedling (**SEED**) category is for special topics defined by accompanying Dear Colleague Letters. SEED projects will be limited to \$300,000 for up to two years.

The SaTC program has been updated to reflect the major changes in cybersecurity over the past decade. This includes factors related to new technologies, new applications, scale, and increased expectations. Some key highlights from the updated program include the integration of social, economic, and cyber ecosystems; the optional Transition to Education (TTE) plan to co-evolve research and education; and the Seedling program that will enable SaTC to be more flexible and nimble. SaTC 2.0 has greater focus on “(1) integration of social, economic, and cyber ecosystems; (2) forward-looking, next-generation, clean-slate ideas that are resilient to potential or unforeseen threats; and (3) approaches to anticipate and mitigate potential threats in new and emerging applications and technologies.”

The updated program includes a “focus on a complex and interdependent cyber ecosystem that involves hardware, software, networks, data, people, organizations, countries, and the physical world.” Broad topic areas of interest for SaTC 2.0 include computing and communication systems; foundations; human aspects; information ecosystems; and cybersecurity and artificial intelligence. However, research that covers multiple topics and/or new areas are encouraged.

Additional details are included in the full solicitation. Note that other NSF programs that support Security and Privacy include Privacy-Preserving Data Sharing in Practice ([PDS](#)), CyberCorps



Scholarship for Service ([SFS](#)), and the [SPHERE](#) testbeds funded by the NSF Mid-Scale Research Infrastructure program.

Due Dates: Full proposals are due by **September 29, 2025**, and the last Monday in September, annually thereafter; and also, **January 26, 2026**, and the last Monday in January, annually thereafter.

Total Funding and Award Size: NSF anticipates total funding of up to \$60 million per year for the SaTC program to support approximately 75 awards.

Eligibility: Two- and four-year accredited U.S.-based institutions of higher education, non-profit non-academic organizations, associated with educational or research activities are eligible to apply. There is a limit on the number of proposals per PI or co-PI in that during a 12-month period, an individual may not participate as PI, co-PI, or Senior/Key Personnel in more than four proposals. There is a limit of:

- two proposals designated as RES;
- one proposal designated as EDU; and
- one proposal designated as SEED.

Sources and Additional Information:

- The SaTC program page is available at <https://new.nsf.gov/funding/opportunities/satc-20-security-privacy-trust-cyberspace>.
- The SaTC solicitation is available at <https://new.nsf.gov/funding/opportunities/satc-20-security-privacy-trust-cyberspace/nsf25-515/solicitation>.