NSF 25-515: Security, Privacy, and Trust in Cyberspace (SaTC 2.0)

Program Solicitation

Document Information

Document History
- **Posted:** December 5, 2024
- **Replaces:** NSF 24-504

View the program page

U.S. 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 STEM Education
    Division of Graduate Education

Full Proposal Target Date(s):

September 29, 2025

    Last Monday in September, Annually Thereafter

January 26, 2026

    Last Monday in January, Annually Thereafter

        Proposers are highly encouraged to submit by a target date. Proposals will be accepted anytime, but they may miss a particular panel or committee meeting.

📄 Table Of Contents

Important Information And Revision Notes

- New focus on a complex and interdependent cyber ecosystem that involves hardware, software, networks, data, people, organizations, countries, and the physical world.
- Increased emphasis 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.
- Changed the CORE designation for research proposals to RES. Proposals submitted to the research (RES) project designation cannot exceed $1.2M; proposal budgets must be commensurate with the complexity, scope, and scientific and societal impact of the proposed research.
- Introduced five broad topics of interest: computing and communication systems; foundations; human aspects; information ecosystems; and cybersecurity and artificial intelligence.
- Added an optional Transition to Education (TTE) supplemental plan for all proposals designated as RES.
- Clarified definitions of Education (EDU) and education research focused EDU proposals.
- Added new Seedling (SEED) designation.

- Removed the Transition to Practice (TTP) designation.
- Added two target submission dates.
- Added new requirements for inclusion of keywords in RES proposal submissions.
- Added new eligibility constraints for the number of proposals per PI or co-PI.

Any proposal submitted in response to this solicitation should be submitted in accordance with the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) that is in effect at the time the proposal is submitted. The NSF PAPPG is regularly revised and it is the responsibility of the proposer to ensure that the proposal meets the requirements specified in this solicitation and the applicable version of the PAPPG.

Summary Of Program Requirements

General Information

Program Title:

Security, Privacy, and Trust in Cyberspace (SaTC 2.0)

Synopsis of Program:

Our world is at a pivotal moment where the boundaries dividing the physical and social worlds from the cyber world have become blurred. Cyberspace has evolved from an interconnected digital environment into a complex and interdependent cyber ecosystem that involves hardware, software, networks, data, people, organizations, countries, and the physical world. Critical functions of everyday life are deeply intertwined with computing, including health, government, commerce, the public sphere, education, critical infrastructure, interpersonal communication, and transportation. The complexity and inter-dependencies in cyberspace can be misused and exploited by malicious actors. These in turn can trigger adverse outcomes such as disruption of critical infrastructure and systems; theft of intellectual property and sensitive data; amplification of inequalities; disclosure of private information of individuals, organizations, and governments; and threats to lives, livelihoods, and reputations. Furthermore, constant attacks on the data and assets of corporations, governments, and individuals undermine people's trust in decision-making and processes that depend critically on these cyber systems.

The Security, Privacy, and Trust in Cyberspace (SaTC 2.0) program aims to build trust in global cyber ecosystems. Trust is the core tenet of this program and, for the purposes of this solicitation, is broadly defined to include our confidence in the security, privacy, and resilience of cyberspace, particularly in the face of malicious intent. Achieving this level of confidence in cyberspace requires not only understanding the vulnerabilities in a system that could be exploited and how they can be addressed, but also understanding the social and technical dimensions of trust in cyber systems, along with the educational efforts needed to increase public awareness of risks in cyberspace, and building a well-trained corps of privacy and security professionals.

SaTC 2.0 spans the interests of NSF's Directorates for Computer and Information Science and Engineering (CISE), Mathematical and Physical Sciences (MPS), Social, Behavioral and Economic Sciences (SBE), and STEM Education (EDU). Proposals must be submitted pursuant to one of the following designations, each of which may have additional requirements:

- RES: The Research (RES) designation is the focus of the multidisciplinary SaTC 2.0 research program. RES projects are limited to $1,200,000 in total budget, with durations of up to four years. Proposals with a total budget of more than $600,000 have additional requirements including Broadening Participation in Computing and collaboration plans. RES proposals may include an optional Transition to Education (TTE) plan with a budget up to $50,000 (within the RES total budget request) to co-evolve novel educational initiatives in the context of the proposed research.

- EDU: The Education (EDU) designation is used to identify proposals focusing on education and workforce training in building trust in security, privacy, and resilience of cyberspace. EDU proposals are limited to $500,000 in total budget, with durations of up to three years. EDU proposals that primarily focus on education research with demonstrated collaboration, as reflected in the PI team between cybersecurity subject matter experts and education researcher(s), may request an additional $100,000 beyond the $500,000 limit.
- SEED: The Seedling (SEED) category is intended for special topics defined by accompanying Dear Colleague Letters. SEED projects are limited to $300,000 in total budget, with durations of up to two years.

Broadening Participation In STEM

NSF recognizes the unique lived experiences of individuals from communities that are underrepresented and/or under-served in science, technology, engineering, and mathematics (STEM) and the barriers to inclusion and access to STEM education and careers. NSF highly encourages the leadership, partnership, and contributions in all NSF opportunities of individuals who are members of such communities supported by NSF. This includes leading and designing STEM research and education proposals for funding; serving as peer reviewers, advisory committee members, and/or committee of visitor members; and serving as NSF leadership, program, and/or administrative staff. NSF also highly encourages demographically diverse institutions of higher education (IHEs) to lead, partner, and contribute to NSF opportunities on behalf of their research and education communities. NSF expects that all individuals, including those who are members of groups that are underrepresented and/or under-served in STEM, are treated equitably and inclusively in the Foundation's proposal and award process.

NSF encourages IHEs that enroll, educate, graduate, and employ individuals who are members of groups underrepresented and/or under-served in STEM education programs and careers to lead, partner, and contribute to NSF opportunities, including leading and designing STEM research and education proposals for funding. Such IHEs include, but may not be limited to, community colleges and two-year institutions, mission-based institutions such as Historically Black Colleges and Universities (HBCUs), Tribal Colleges and Universities (TCUs), women's colleges, and institutions that primarily serve persons with disabilities, as well as institutions defined by enrollment such as Predominantly Undergraduate Institutions (PUIs), Minority-Serving Institutions (MSIs), and Hispanic Serving Institutions (HSIs).

"Broadening participation in STEM" is the comprehensive phrase used by NSF to refer to the Foundation's goal of increasing the representation and diversity of individuals, organizations, and geographic regions that contribute to STEM teaching, research, and innovation. To broaden participation in STEM, it is necessary to address issues of equity, inclusion, and access in STEM education, training, and careers. Whereas all NSF programs might support broadening participation components, some programs primarily focus on supporting broadening participation research and projects. Examples can be found on the NSF Broadening Participation in STEM website.

Cognizant Program Officer(s):

Please note that the following information is current at the time of publishing. See program website for any updates to the points of contact.

- Daniela A. Oliveira, Lead Program Director, CISE/CNS, telephone: (703) 292-4352, email: satc@nsf.gov
- Daniel R. Cosley, Program Director, CISE/IIS, telephone: (703) 292-8832, email: satc@nsf.gov
- Jeremy J. Epstein, Program Director, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov Sol
- Greenspan, Program Director, CISE/CCF, telephone: (703) 292-8910, email: satc@nsf.gov
- Karen Karavanic, Program Director, CISE/CNS, telephone: (703) 292-2594, email: satc@nsf.gov
- Sara Kiesler, Program Director, SBE/SES, telephone: (703) 292-8643, email: satc@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, telephone: (703) 292-4878, email: satc@nsf.gov
- Phillip A. Regalia, Program Director, CISE/CCF, telephone: (703) 292-2981, email: satc@nsf.gov

- Ambareen Siraj, Program Director, EDU/DGE, telephone: (703) 292-8182, email: satc-edu@nsf.gov
- Anna Squicciarini, Program Director, CISE/CNS, telephone: (703) 292-5177, email: satc@nsf.gov
- Selcuk Uluagac, Program Director, CISE/CNS, telephone: (703) 292-4540, email: satc@nsf.gov
- Xiaogang (Cliff) Wang, Program Director, CISE/CNS, telephone: (703) 292-2812, email: satc@nsf.gov
- Emily E. Witt, Program Director, MPS/DMS, telephone: (703) 292-5111, email: ewitt@nsf.gov
- ChunSheng (Sam) Xin, Program Director, EDU/DGE, telephone: (703) 292-7353, email: satc-edu@nsf.gov
- Li Yang, Program Director, EDU/DGE, telephone: (703) 292-2677, email: satc-edu@nsf.gov
- Qiaoyan Yu, Program Director, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov
- Nan Zhang, Expert, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov

Applicable Catalog of Federal Domestic Assistance (CFDA) Number(s):

- 47.049 --- Mathematical and Physical Sciences
- 47.070 --- Computer and Information Science and Engineering
- 47.075 --- Social Behavioral and Economic Sciences
- 47.076 --- STEM Education

Award Information

Anticipated Type of Award: Standard Grant or Continuing Grant

Estimated Number of Awards: 75

Anticipated Funding Amount: $60,000,000 per year, dependent on the availability of funds.

Eligibility Information

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Institutions of Higher Education (IHEs): Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the US, acting on behalf of their faculty members. Special Instructions for International Branch Campuses of U.S. IHEs: If the proposal includes funding to be provided to an international branch campus of a US institution of higher education (including through use of sub-awards and consultant arrangements), the proposer must explain the benefit(s) to the project of performance at the international branch campus, and justify why the project activities cannot be performed at the US campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research laboratories, professional societies and similar organizations located in the U.S. that are directly associated with educational or research activities.

Who May Serve as PI:

As of the date the proposal is submitted, any PI, co-PI, or other Senior/Key project personnel must hold either:

- a tenured or tenure-track position, *or*
- a primary, full-time, paid appointment in a research or teaching position

at a US-based campus of an organization eligible to submit to this solicitation (see above), with exceptions granted for family or medical leave, as determined by the submitting organization. Individuals with

primary appointments at for-profit non-academic organizations or at overseas branch campuses of U.S. institutions of higher education are not eligible.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or co-PI: 4

During any contiguous 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.

This limit is applied beginning with this SaTC 2.0 solicitation and future versions of the SaTC 2.0 solicitation, unless noted otherwise.

These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. Any proposal that exceeds this limit at the time of submission for any PI, co-PI, or other Senior/Key Personnel will be returned without review. **No exceptions will be made**. Proposals that are withdrawn prior to commencement of merit review, or those that are returned without review by NSF, will not count against this proposal limit. Proposers are strongly encouraged to verify the dates of prior SaTC 2.0 submissions for all personnel on their teams to avoid their proposals being deemed non-compliant.

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

- **Letters of Intent:** Not required
- **Preliminary Proposal Submission:** Not required
- **Full Proposals:**
  - Full Proposals submitted via Research.gov: *NSF Proposal and Award Policies and Procedures Guide* (PAPPG) guidelines apply. The complete text of the PAPPG is available electronically on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.
  - Full Proposals submitted via Grants.gov: *NSF Grants.gov Application Guide: A Guide for the Preparation and Submission of NSF Applications via Grants.gov* guidelines apply (Note: The *NSF Grants.gov Application Guide* is available on the Grants.gov website and on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=grantsgovguide).

B. Budgetary Information

- **Cost Sharing Requirements:**

  Inclusion of voluntary committed cost sharing is prohibited.

- **Indirect Cost (F&A) Limitations:**

  Not Applicable

- **Other Budgetary Limitations:**

  Other budgetary limitations apply. Please see the full text of this solicitation for further information.

C. Due Dates

- **Full Proposal Target Date(s)**:

    September 29, 2025

    > Last Monday in September, Annually Thereafter

    January 26, 2026

    > Last Monday in January, Annually Thereafter

    >> Proposers are highly encouraged to submit by a target date. Proposals will be accepted anytime, but they may miss a particular panel or committee meeting.

Proposal Review Information Criteria

Merit Review Criteria:

National Science Board approved criteria. Additional merit review criteria apply. Please see the full text of this solicitation for further information.

Award Administration Information

Award Conditions:

Additional award conditions apply. Please see the full text of this solicitation for further information.

Reporting Requirements:

Additional reporting requirements apply. Please see the full text of this solicitation for further information.

I. Introduction

Society relies on a complex cyber ecosystem for vital communications, economic prosperity, individual well-being, resilient societal infrastructures, physical safety, and the advancement of knowledge. With this reliance comes an increase in the severity and nature of threats targeting the ecosystem with deleterious consequences, as noted in the 2023 Federal Cybersecurity Research and Development Strategic Plan[1]: "the structure of the digital ecosystem and its components remains prone to disruption or unintentional human-errors, vulnerable to exploitation, and is often co-opted by malicious actors." Society's confidence in this complex cyberspace depends on cybersecurity, broadly defined — thus constituting a national priority that integrates the technical, legal, and normative proscription, prevention, and mitigation of cyber-attacks, intrusions on privacy, and other cyber-facilitated harms, particularly those that fall on vulnerable groups.

Compounding the potential for attacks and harm are rapidly evolving computing-based technologies, our interactions with them, and the ways they are deployed in society. Emerging capabilities such as artificial intelligence, computing in the post Moore's law era, quantum computing, and immersive technologies such as brain-computer interfaces and virtual reality raise new risks, vulnerabilities, attack scenarios, and harms. Advances in computing and its deployment throughout the cyber ecosystem also offer opportunities for a more secure, private, and resilient cyberspace.

To develop trustworthy cyberspace now and in the future, research will need to address not just the properties of computer systems and data, but the many elements of our complex cyber ecosystem, and with richer and inter-related notions of trust and deeper integration of new technologies, applications, social contexts, and understanding of human behavior. This solicitation re-envisions the high-level goals of NSF's flagship Secure and Trustworthy Cyberspace (SaTC) program in the context of the current and future cyber ecosystem.

The overarching vision of the Security, Privacy, and Trust in Cyberspace (SaTC 2.0) program is informed by recent governmental and academic reports and strategic plans that describe critical needs and approaches toward a more

secure, resilient, and trustworthy cyberspace. This solicitation is strongly aligned with the 2023 Federal Cybersecurity Research and Development Strategic Plan, that states the need for "fundamental changes to the underlying dynamics of the digital ecosystem, shifting the advantage to its defenders and perpetually frustrating the forces that would threaten it," with the goal of achieving a "defensible, resilient digital ecosystem where it is costlier to attack systems than defend them, where sensitive information is secure and protected, and where neither incidents nor errors cascade into catastrophic, systemic consequences." The solicitation is also aligned with the National Privacy Research Strategy[2] and National Strategy to Advance Privacy-Preserving Data Sharing and Analytics[3] in that the proliferation of data collection methods along with the next generation of connectivity and ubiquitous sensors lead to massive data gathering and "such opportunities cannot be fully realized unless there are appropriate safeguards to protect privacy"; and the National Artificial Intelligence Research and Development Strategic Plan[4] in that it views AI as a powerful technology that can improve societal wellbeing, but that needs to be applied in a trustworthy and safe manner. The community-driven Secure and Trustworthy Computing 2.0 Vision Statement[5], providing a comprehensive road-map for cybersecurity and privacy research for the next decade, also informed the program's updated vision.

---

[1] https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf.

[2] https://www.nitrd.gov/pubs/NationalPrivacyResearchStrategy.pdf.

[3] https://www.nitrd.gov/pubs/National-Strategy-to-Advance-Privacy-Preserving-Data-Sharing-and-Analytics.pdf.

[4] https://www.nitrd.gov/pubs/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

[5] https://arxiv.org/abs/2308.00623 ⬀ .

II. Program Description

The SaTC 2.0 program aims to build trust in all aspects of global cyber ecosystems. Trust can assume different meanings according to the context but, for the purposes of this solicitation, is broadly defined to include concepts covering security, privacy, and resilience of cyberspace, particularly in the face of malicious intent and specific threats. Achieving this level of confidence in cyberspace requires not only understanding the vulnerabilities in a system that could be exploited and how they can be addressed, but also understanding the social and technical dimensions of trust in cyber systems, as well as educational efforts needed to increase public awareness of risks in cyberspace and to build a well-trained corps of privacy and security professionals. Examining the fundamentals of trust from these different perspectives and with strong research methodologies can lead to fundamentally new and holistic ways to design, build, and operate future trustworthy cyber systems, protect people and existing cyberinfrastructure, and motivate and educate the professional cybersecurity workforce and the general public.

SaTC 2.0 welcomes proposals that address trust in cyberspace, broadly defined, that draw on expertise in one or more of these areas: computer and information science and engineering; education; mathematics; statistics; and social, behavioral, and economic sciences. Proposals that advance fundamental research in cybersecurity, privacy, trust, and resilience research within a single discipline are welcome, as are inter- and multi-disciplinary efforts that span multiple areas. Proposals whose security science exposes underlying principles having predictive value that extend across different security domains and are resilient against strong, adaptive attackers are preferred over those that are limited to a single platform, technology, or system, or that offer ad-hoc solutions that are not generalizable. The program especially encourages proposals with forward-looking, next-generation, clean-slate ideas that provide defenders with a distinct advantage and offer resilience against potential or unforeseen threats. Of particular interest are approaches to anticipate and mitigate risks and potential threats in new and emerging applications and technologies.

SaTC 2.0 is designed to be distinct from other NSF programs through its focus on cyberspace; its attention to trust, security, and privacy; and its integration of social, economic, and technical considerations. Proposals whose core contributions do not directly align with these goals of SaTC 2.0 may be better suited to other types of solicitations and programs. For instance, proposals where security, privacy, malice, and threat are a small part of the proposal and whose main contributions would be recognized as core to existing CISE programs should consider those programs instead. Proposals whose main contributions are on underlying techniques that address reliability or resilience in cyberspace more generally in the context of other design considerations and lack malicious or deceptive threats are encouraged to consider other CISE programs including CISE [Core](#), [Formal Methods in the Field](#) (FMitF) and [Cyber Physical Systems](#) (CPS). Proposals mainly focused on theoretical advances in decision making, public policy, the provision of public services, and international affairs, without explicit analysis of cyberspace, may be more suited for one of several programs in the Social, Behavioral, and Economic Sciences Directorate (SBE), such as Accountable Institutions and Behavior (AIB). Proposals that focus on well understood security and/or privacy issues in specific domains may be better suited for programs focused on novel advances in those domains: for example, CPS or [Smart Health and Biomedical Research in the Era of Artificial Intelligence and Advanced Data Science](#) (SCH). Proposals whose main contributions are on enabling important new capabilities in robotics but lack novelty in security and/or privacy may wish to consider the [Foundational Research in Robotics](#) (FRR) program. Proposals solely focused on enhancing the trust in research cyberinfrastructure may be better suited for [Cybersecurity Innovation for Cyberinfrastructure](#) (CICI) program. Proposals focused on transition of research into practice may be more appropriate for one of several programs in the Technology, Innovation, and Partnership Directorate (TIP), such as [Privacy-Preserving Data Sharing in Practice](#) (PDaSP).

The SATC 2.0 program spans the interests of NSF's Directorates for Computer and Information Science and Engineering (CISE), Mathematical and Physical Sciences (MPS), Social, Behavioral and Economic Sciences (SBE), and STEM Education (EDU). Proposals must be submitted pursuant to one of the following designations, each of which may have additional requirements:

- RES: This designation is the focus of the SaTC 2.0 **research** program.
- EDU: This designation is used to identify proposals focusing on **education and training** in cybersecurity and/or privacy.
- SEED: This designation is intended for **special topics** defined by accompanying Dear Colleague Letters.

RESEARCH (RES) PROJECT DESIGNATION

RES Projects are limited to total budgets up to $1,200,000 for durations of up to four years. This designation is intended for all research projects that range from single-investigator studies and/or studies of exploratory concepts to multi-investigator integrated efforts with larger-scale activities. **The budget request must be commensurate with the complexity, scope, and scientific and societal impact of the proposed project.** SaTC 2.0 will maintain a balanced portfolio of awards at all budget levels so proposers should tailor their budget to the needs of the proposed activities rather than tailoring their proposed activities to a specific budget number. Projects with budgets above $600,000 have additional requirements as detailed in section V.A. RES proposals may include an optional **Transition to Education (TTE)** plan with a budget allocation of up to $50,000 within the RES total budget request to co-evolve novel educational initiatives in the context of the proposed research.

All RES proposals should (a) clearly articulate the notion of trust that the research will focus on; (b) include a clear and concise description of the specific risk(s), malicious intent or applicable threat scenario or model that the proposed research addresses; (c) discuss the generalizable contributions that will be developed beyond the state of the art (theories, research methods, empirical understanding, capabilities, tools and datasets, or other contributions appropriate to the project and the intellectual communities the project speaks to); and (d) discuss evaluation, reproducibility, trade-offs, and countermeasures involved in the project as appropriate. Proposals that focus primarily on the design, development, or use of offensive techniques are out of scope, especially to the extent such work may prove harmful to the operation of existing cyber infrastructure and/or be at odds with ethical, legal, and diplomatic concerns or other applicable rules and regulations.

Projects are expected to include, but not be limited to, expertise in one or more the following research disciplines that correspond to the core building blocks of cyberspace: algorithms; artificial intelligence; compilers; communication networks; cryptography; data science; economics; ethics; formal methods; hardware security architecture and design; human centered computing; law and policy; machine learning; mathematics; programming languages; quantum and other emerging computing models and architectures; social and behavioral sciences; software; statistics; and systems.

Broad topics of interest include computing and communication systems; foundations; human aspects; information ecosystems; and cybersecurity and artificial intelligence. A brief description of each is offered below; proposers should not feel obliged, however, to restrict themselves to these categories or see them as mutually exclusive; indeed, research directions that span key topics and/or probe those yet to be uncovered are especially encouraged.

- Computing and Communication Systems: Approaches for making existing cyber systems more resilient to current and emerging threats, and designing the next generation of systems, software, networks, and hardware that are secure, private and trustworthy by design. Examples include vulnerabilities and malware, digital forensics, access control, authentication, autonomous, distributed, and embedded systems, wired/wireless networks, secure software development, trusted execution environments, microarchitecture and integrated circuits.

- Foundations: Formal, mathematical, and other rigorous approaches for defining, modeling, designing, and ensuring trust in cyberspace. Examples include cryptography, formal methods, game theory, information theory, privacy theory, quantum computing, mechanism design, programming languages, probability, and statistics.

- Human Aspects: Social, behavioral, economic, cognitive, and other rigorous empirical approaches for understanding and addressing ethical, political, legal, cultural, and societal dimensions of cyber ecosystems and threats to society's trust in these systems and risks to human and organizational security, safety, and well-being. Examples include human-centered design, usable security and privacy, community security and norms, risks to persons, organizations, society, and marginalized populations.

- Information Ecosystems: Approaches to safeguard information ecosystems ranging from the trustworthy generation, dissemination, analysis, storage, and provenance of multi-modal data, to protecting the entities who consume this information. Examples include privacy-enhancing technologies, information leakage, provenance and authenticity, steganalysis, and trustworthy generation of synthetic data.

- Cybersecurity and Artificial Intelligence: Approaches to address the bidirectional role of AI both in eroding trust in cyberspace and in enhancing security, privacy and trust in cyberspace. Examples include adversarial machine learning and other attacks on AI systems themselves, attackers' use/weaponization of AI against people, information, and systems, responsible use of AI in predicting, detecting, and responding to attacks, and privacy-preserving machine learning.

Proposers are also strongly encouraged to consider crosscutting issues, including but not limited to clean slate approaches that ensure security and privacy by design rather than remedying existing imperfect approaches, systems, networks, theories, and/or frameworks; end-to-end security methodology that works across layers of the cyberspace; trade-offs among different notions of trust; cyber resilience to and recovery from security attacks; ethical implications and unintended consequences of the research; and reproducibility, metrics, datasets, open source code, and research infrastructure to be used or generated in the proposed project.

Optional Transition To Education (TTE) Plans in RES Proposals

Proposers who choose to submit a TTE plan as part of their SaTC 2.0 RES research proposal must describe how successful research outcomes will be transitioned into an educational setting for formal or informal learning. The optional TTE plan must support the design, development, and deployment of innovative cybersecurity or privacy educational materials grounded in research. The TTE plan, not exceeding 2 pages and submitted as a supplementary document, should outline major activities and milestones, and it must detail how the deliverables will be made accessible to the broader academic community. It should also include evaluation with quantifiable metrics for learning assessment, aligned with the accompanying RES evaluation plan.

The TTE plan will be evaluated with particular attention to: (a) the description of the educational need to be addressed; (b) the novelty of the educational content; (c) how the research or technology will be transitioned into education and its

impact on the cybersecurity workforce; (d) the identification of an intended population that will serve as early adopters of the proposed educational content; (e) the deployment plan for implementing/piloting the educational materials; (f) the explanation of the post-grant, long-term sustainability of the educational content; (g) the extent to which learning experiences will feed back into research (if applicable); and (h) the justification of the TTE budget for the effort, which may include up to $50,000 within the RES total budget request.

Questions regarding the TTE designation should be addressed directly to satc-EDU Program Officers via satc-EDU@nsf.gov

Broadening Participation in Computing (BPC) Plans in RES Proposals

All projects with a total budget greater than $600,000 that include an organization (department, school, or institute) that primarily carries out research and education in computer science, computer engineering, information science, and/or other closely related fields, must include a BPC plan (see details in Section V.A. Proposal Preparation).

For projects where none of the PIs or co-PIs are from computing organizations as described above, a BPC plan is not required. To emphasize this point, PIs are encouraged to include a statement titled "Broadening Participation in Computing Plan" and the text "no PI on this project is in a computing organization, so no BPC plan is required".

CISE has long been committed to Broadening Participation in Computing (BPC). This commitment means addressing the underrepresentation of many groups in CISE relative to their participation in postsecondary education (https://ncses.nsf.gov/pubs/nsb20223/data). Broadening participation will require a range of measures, including institutional programs and activities as well as culture changes across colleges, departments, classes, and research groups.

CISE continues the BPC effort started in 2018 that encourages the research community to engage in meaningful BPC activities. Specifically: Each project with a total budget greater than $600,000 must include a BPC plan. CISE encourages the use of the resources available at the NSF-funded BPCnet Resource Portal (https://bpcnet.org/ ⧉). BPCnet provides BPC plan templates, suggested activities, opportunities for consultant services, and publicly available data to support PIs and departments in creating their BPC Plans. *CISE encourages PIs to leverage Departmental BPC Plans verified by BPCnet which coordinate efforts within their institution.* BPC plans must include roles for all PIs and co-PIs and be included as a Supplementary Document, following the guidelines as described in the Proposal Preparation Instructions.

A meaningful BPC plan can answer positively to the following five elements:

1. Goal and Context: Does the plan describe a goal and the data from your institution(s) or local community that justifies that goal?
2. Intended population(s): Does the plan identify the characteristics of participants, including school level?
3. Strategy: Does the plan describe activities that address the stated goal(s) and intended population(s)?
4. Measurement: Is there a plan to measure the outcome(s) of the activities?
5. PI Engagement: Is there a clear role for each PI and co-PI? Does the plan describe how the PI is prepared (or will prepare or collaborate) to do the proposed work?

All PIs and co-PIs are expected to participate in BPC activities in a manner aligned with their personal contexts, interests, and skills. More information regarding the BPC effort can be found at https://www.nsf.gov/cise/bpc.

EDUCATION (EDU) PROJECT DESIGNATION

The Education (EDU) designation labels proposals that focus on cybersecurity education and workforce development in ensuring cybersecurity including security, privacy, trust, and resilience of cyberspace. The EDU project class supports the development of a robust and diverse cybersecurity workforce, as well as a cyber-aware citizenry.

EDU proposals are limited to $500,000 in total budget, with durations of up to three years. Education research focused EDU proposals that demonstrate collaboration between cybersecurity subject matter experts and education researcher(s), as reflected in the PI team, **may request an additional $100,000 beyond the $500,000 limit.** The additional funding request must be justified primarily to support the education research activities of the proposed

project. To qualify for the increased budget cap, proposals must address contributions in both cybersecurity and education, leading to novel understanding and impact on cybersecurity learning, pedagogy, and equity and inclusion in educational settings.

SaTC 2.0 EDU seeks innovative inquiries into and the development of evidence-based and evidence-generating approaches that will enhance cybersecurity education and workforce development at the K-12, undergraduate, graduate, and professional education levels; and/or develop cybersecurity awareness that promotes safe online behavior across all age groups. EDU proposals must directly contribute to the development of foundational cyber skills or transformation of cybersecurity education in terms of scope, mechanism, methods, tools, and engagement of diverse learners through traditional or non-traditional approaches. Competitive EDU proposals should leverage findings from basic and/or applied research in cybersecurity and student learning to propose state-of-the-art interventions in education and workforce development, emphasizing both intellectual merit and broader impacts. They should address the challenges of expanding existing educational opportunities and resources in cybersecurity and/or privacy.

EDU projects are expected to contribute to the cybersecurity and/or privacy education knowledge base by enhancing cybersecurity learning and learning environments in formal and/or informal settings, incorporating traditional and/or non-traditional methods of student learning within and across disciplines. This may include, but is not limited to, the following efforts:

- Conduct research that enhances the teaching and learning of cybersecurity, privacy and trust at K-12 and post-secondary levels;
- Based on the findings of basic and applied research in cybersecurity, define a cybersecurity body of knowledge and establish curricular activities for new course modules and educational pathways leading to wide dissemination and adoption;
- Research approaches to increasing undergraduate and graduate enrollment in cybersecurity and produce more cybersecurity professionals and practitioners;
- Investigate approaches to develop a cybersecurity workforce, including research and development workforce, in critical areas, such as secure software design and development, trustworthy AI development and usage, human-centered approaches to building secure systems, quantum computing, memory safety techniques, formal methods, advanced manufacturing, aerospace, microelectronics, and advanced wireless technologies;
- Design and implement new skill-based approaches, such as hands-on learning experiences, competitions, certifications, micro-credentials, and alignment with national and industry standards;
- Create innovative and scalable strategies to increase the number of cybersecurity faculty in institutions of higher education and K-12 schools;
- Develop approaches to support institutional collaborations between community colleges and four-year colleges and universities
- Cultivate digital literacy to ensure correct and safe online behavior for everyone;
- Integrate cybersecurity, privacy, and trust concepts into educational opportunities for learners of all ages;
- Design and develop instructional strategies to align cybersecurity education and workforce development with the NICE Cybersecurity Workforce Framework and make them more diverse, inclusive and culturally responsive;
- Investigate effective and ethical use of AI and automation in cybersecurity and privacy education; and
- Evaluate the effectiveness of learning, outreach, and retention methods and activities.

All EDU proposals must have detailed plans for assessment and evaluation that are clearly aligned with the project's stated goals based on appropriate metrics. The evaluation should incorporate both formative evaluation to guide project improvements and summative evaluation to assess and document project outcomes, accomplishments, and lessons learned. Funds to support an evaluator independent of the project must be requested. The evaluator, while external to the project, may be employed by a project's home institution, provided they work in a separate organizational unit with a distinct reporting line from the project's home unit. The evaluator can be listed as project personnel, but cannot serve as a PI, co-PI, or other Senior/Key Personnel on the project. Evaluators are expected to adhere to the American Evaluation

Association's Guiding Principles for Evaluators and project evaluations are expected to be consistent with standards established by the [Joint Committee on Standards for Educational Evaluation](#) ⬈.

All EDU proposals must include a dissemination strategy that is tied to broader impact goals and a clear plan to report on the project and its successes and lessons learned to appropriate audiences. Please note the new EDU Data Management Plan guidelines at [STEM Education Data Management and Sharing Plan Guidance for Proposals and Awards - Directorate for STEM Education (EDU) | NSF - National Science Foundation](#).

In addition to promoting innovative work at the frontier of cybersecurity education, the program encourages education research focused EDU proposals, especially those from diverse institutions and student populations, to produce novel knowledge about the efficacy and transferability of findings. Education research focused EDU proposals aim to advance knowledge and understanding with potential relevance to the cybersecurity community, emphasizing the development or refinement of foundational or applied education research related to cybersecurity and/or privacy education. While applied research aims for specific relevance (e.g., to a particular curriculum or technology) with direct and immediate implications for practice, fundamental education research is crucial for advancing broad, long-term understanding of key relevance and principles, providing a foundation for future innovations in cybersecurity education research. For guidelines and resources for STEM education research, see the following:

- [Common Guidelines for Education Research and Development](#)
- [Companion Guidelines on Replication and Reproducibility in Education Research](#)
- [Discipline-based education research: Understanding and improving learning in undergraduate science and engineering](#) ⬈

SEEDLING (SEED) PROJECT DESIGNATION

The SEED designation is intended for special topic areas to be defined by accompanying Dear Colleague Letters (DCLs) while this solicitation is in effect. **The total budget for SEED projects is limited to $300,000, with durations of up to two years.** The associated DCLs will solicit proposal submissions in specified topic areas within a specified time frame. Investigators seeking to submit SEED proposals in response to a DCL may be required to (a) submit concept outlines (as described in the PAPPG Chapter I.D.1) to be evaluated by the SaTC 2.0 Program and invited for proposal submission; or (b) have a specific team composition intended to foster multi- and/or interdisciplinary research. The accompanying DCLs will only solicit proposals within specified submission windows and all active DCLs will be listed on the SaTC 2.0 Program web [page](#). SEED proposals are expected to follow all applicable proposal preparation guidelines for RES submissions (as described in Section V.A).

SaTC 2.0 PI Meetings

The SaTC 2.0 program plans to host PI meetings every other year with participation from all active SaTC 2.0 projects. This meeting will be a community-wide event with representatives from federal agencies, academia, industry, and international institutions. Principal investigators from all solicitation designations are encouraged to participate in these meetings. The first PI meeting is expected to be held in Fall 2026, and approximately every two years thereafter.

For all SaTC 2.0 awards of duration less than or equal to 3 years, at least one project representative (PI/co-PI/senior researcher or NSF-approved replacement) from each organization should attend the first PI meeting held after the award date. For awards of duration greater than 3 years, at least one project representative (PI/co-PI/senior researcher or NSF-approved replacement) from each organization should attend one PI meeting every two years for the duration of the project. PIs are explicitly required to budget for travel to the PI meetings.

Access to Experimental Research Infrastructure

PIs may consider utilizing NSF-supported research infrastructure (such as the [Platforms for Advanced Wireless Research](#) ⬈[6], [FABRIC](#) ⬈[7], [Chameleon](#) ⬈[8], [CloudLab](#) ⬈[9], and [National Artificial Intelligence Research Resource (NAIRR) Pilot](#) ⬈[10]) when formulating their research plans and submitting proposals. Descriptions of the capabilities of each system and their availability can be found at websites.

[6] https://advancedwireless.org/ .

[7] https://portal.fabric-testbed.net/ .

[8] https://www.chameleoncloud.org/ .

[9] https://cloudlab.us/ .

[10] https://nairrpilot.org/ .

III. Award Information

Anticipated Type of Award: Continuing Grant or Standard Grant

Estimated Number of Awards: 75

NSF anticipates approximately 15 EDU awards, 60 RES awards.

Anticipated Funding Amount: $60,000,000 per year, dependent on the availability of funds.

IV. Eligibility Information

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Institutions of Higher Education (IHEs): Two- and four-year IHEs (including community colleges) accredited in, and having a campus located in the U.S., acting on behalf of their faculty members. Special Instructions for International Branch Campuses of US IHEs: If the proposal includes funding to be provided to an international branch campus of a US institution of higher education (including through use of sub-awards and consultant arrangements), the proposer must explain the benefit(s) to the project of performance at the international branch campus, and justify why the project activities cannot be performed at the US campus.
- Non-profit, non-academic organizations: Independent museums, observatories, research laboratories, professional societies and similar organizations located in the U.S. that are directly associated with educational or research activities.

Who May Serve as PI:

As of the date the proposal is submitted, any PI, co-PI, or other Senior/Key project personnel must hold either:

- a tenured or tenure-track position, *or*
- a primary, full-time, paid appointment in a research or teaching position

at a US-based campus of an organization eligible to submit to this solicitation (see above), with exceptions granted for family or medical leave, as determined by the submitting organization. Individuals with *primary* appointments at for-profit non-academic organizations or at overseas branch campuses of U.S. institutions of higher education are not eligible.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or co-PI: 4

> During any contiguous 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.
>
> This limit is applied beginning with this SaTC 2.0 solicitation and future versions of the SaTC 2.0 solicitation, unless noted otherwise.
>
> **These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently**. Any proposal that exceeds this limit at the time of submission for any PI, co-PI, or other Senior/Key Personnel will be returned without review. **No exceptions will be made**. Proposals that are withdrawn prior to commencement of merit review, or those that are returned without review by NSF, will not count against this proposal limit. Proposers are strongly encouraged to verify the dates of prior SaTC 2.0 submissions for all personnel on their teams to avoid their proposals being deemed non-compliant.

Additional Eligibility Info:

> Sub-awards are not permitted to overseas campuses/offices of US-based proposing organizations.

V. Proposal Preparation And Submission Instructions

A. Proposal Preparation Instructions

Full Proposal Preparation Instructions: Proposers may opt to submit proposals in response to this Program Solicitation via Research.gov or Grants.gov.

- Full Proposals submitted via Research.gov: Proposals submitted in response to this program solicitation should be prepared and submitted in accordance with the general guidelines contained in the *NSF Proposal and Award Policies and Procedures Guide* (PAPPG). The complete text of the PAPPG is available electronically on the NSF website at: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg. Paper copies of the PAPPG may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-8134 or by e-mail from nsfpubs@nsf.gov. The Prepare New Proposal setup will prompt you for the program solicitation number.

- Full proposals submitted via Grants.gov: Proposals submitted in response to this program solicitation via Grants.gov should be prepared and submitted in accordance with the *NSF Grants.gov Application Guide: A Guide for the Preparation and Submission of NSF Applications via Grants.gov*. The complete text of the *NSF Grants.gov Application Guide* is available on the Grants.gov website and on the NSF website at: (https://www.nsf.gov/publications/pub_summ.jsp?ods_key=grantsgovguide). To obtain copies of the Application Guide and Application Forms Package, click on the Apply tab on the Grants.gov site, then click on the Apply Step 1: Download a Grant Application Package and Application Instructions link and enter the funding opportunity number, (the program solicitation number without the NSF prefix) and press the Download Package button. Paper copies of the Grants.gov Application Guide also may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-8134 or by e-mail from nsfpubs@nsf.gov.

In determining which method to utilize in the electronic preparation and submission of the proposal, please note the following:

Collaborative Proposals. All collaborative proposals submitted as separate submissions from multiple organizations must be submitted via Research.gov. PAPPG Chapter II.E.3 provides additional information on collaborative proposals.

See PAPPG Chapter II.D.2 for guidance on the required sections of a full research proposal submitted to NSF. Please note that the proposal preparation instructions provided in this program solicitation may deviate from the PAPPG instructions.

The Seedling (SEED) category is intended for special topics that will be announced through the use of Dear Colleague Letters (DCLs). The accompanying DCLs will only solicit proposals within specified submission windows and all active DCLs will be listed on the SaTC 2.0 Program web page. SEED proposals are expected to follow all applicable proposal preparation guidelines for RES submissions and the SEED-specific guidance below. See Section II, Program Description, for additional information.

Proposal Title:

Proposal titles must begin with the acronym SaTC 2.0, followed by a colon, and the acronym that indicates the designation. Select the designation acronym from the following list:

- SaTC 2.0 core research designation: **RES**;
- SaTC 2.0 seedling designation: **SEED**; or
- Cybersecurity Education designation: **EDU**.

Research proposals can be RES or SEED. The acronym, RES, should be followed by a colon, and then the title of the proposed project. For example, if you are submitting a Seeding proposal, the title of your proposal would be **SaTC 2.0: SEED: Title, and** if you are submitting a RES proposal with a TTE option, the title of your proposal would be **SaTC 2.0: RES: TTE: Title.** If you submit a proposal as part of a set of collaborative proposals, the words "Collaborative Research" followed by a colon should appear at the beginning of the title, before the "SaTC 2.0" acronym. For example, if you are submitting a collaborative set of proposals to the SaTC 2.0 EDU designation, the title of each proposal would be **Collaborative Research: SaTC 2.0: EDU: Title.** Please note that if submitting via Research.gov, the system will automatically insert the prepended title "Collaborative Research" when the collaborative set of proposals is created.

Start Date:

To avoid overdue reports blocking award actions during the end of a fiscal year, organizations are discouraged from seeking project start dates between July 2 and September 30 of a given year. Recipient organizations may incur allowable pre-award costs within the 90-day period immediately preceding the start date of the grant subject to the conditions specified in the PAPPG; this will allow support for students or other relevant activities to begin over this period.

Project Summary:

Keywords

All RES and SEED proposals **must include a prioritized list of 1-6 keywords** that describe the general area(s) of the investigation, to assist in identifying reviewers with appropriate knowledge and expertise to review the proposal. The list of keywords should be the last paragraph of the Overview section of the Project Summary.

The first keyword **must** (and other keywords may) be drawn from the following list of topic areas that correspond to key areas of study: authentication and access control; biometrics and human sensing; cryptography; cyber-physical systems; data science, ML, and AI; digital forensics; education; formal methods; hardware security; human-centric computing; information protection; programming language; mathematics and statistics; privacy; secure software development; social, behavioral, and economic sciences; systems; usable security and privacy; and wired and wireless networking.

Project Description:

The project description for proposals submitted to the RES and EDU designations is limited to 15 pages, and 10 pages for the SEED designation. See also Section II, Program Description, in this solicitation for additional guidance.

Supplementary Documents:

In the Supplementary Documents Section, upload the following:

1. (required) A list of Project Personnel and Partner Institutions (required. Note: in collaborative proposals, the lead institution should provide this information for all participants):

Provide current, accurate information for all personnel and institutions involved in the project. NSF staff will use this information in the merit review process to manage reviewer selection. The list must include all PIs, co-PIs, Senior/Key Personnel, funded/unfunded Consultants or Collaborators, Sub-awardees, Postdocs, and project-level advisory committee members. This list should be numbered and include (in this order) Full name, Organization(s), and Role in the project, with each item separated by a semi-colon. Each person listed should start a new numbered line. For example:

1. Mei Lin; XYZ University; PI

2. Jak Jabes; University of PQR; Senior/Key Personnel

3. Jane Brown; XYZ University; Postdoctoral Researcher

4. Rakel Ademas; ABC Inc.; Funded Consultant

5. Maria Wan; Welldone Institution; Unfunded Collaborator

6. Rimon Greene; ZZZ University; Subawardee

2. Collaboration Plan (required for all projects with more than one PI and a budget of more than $600,000):

Because the success of collaborative research efforts is known to depend on thoughtful coordination mechanisms that regularly bring together the various participants of the project, all proposals with more than one investigator and a total of more than $600,000 must include a Collaboration Plan of up to 2 pages. The length of and degree of detail provided in the Collaboration Plan should be commensurate with the complexity of the proposed project. Where appropriate, the Collaboration Plan might include: 1) the specific roles of the project participants in all organizations involved; 2) information on how the project will be managed across all the investigators, organizations, and/or disciplines; 3) identification of the specific coordination mechanisms that will enable cross-investigator, cross-organization, and/or cross-discipline scientific integration (e.g., yearly conferences, graduate student exchange, project meetings at conferences, use of regular video conferences, software repositories, etc.), and 4) specific references to the budget line items that support collaboration and coordination mechanisms. If a proposal with a budget exceeding $600,000 and more than one investigator does not include a Collaboration Plan of up to 2 pages, that proposal will be returned without review.

Collaboration plans are optional for proposals with a budget of $600,000 or less and EDU proposals with multiple investigators and/or organizations.

3. *Letters of collaboration:*

Letter of collaboration from academic or industry partners are welcome to document specific contributions they will make to the project. Letters should explicitly describe the resources (e.g., hardware, software, test facilities, data, research expertise) to be provided by the collaborating entity. Any collaboration letter may be no longer than a single page, with fonts and margins with the requirements in PAPPG Chapter II.C.2.

4. Data Management and Sharing Plan (required):

Proposals must include a Supplementary Document of no more than two pages labeled "Data Management and Sharing Plan." The data management and sharing plan must be substantive and specific to the project and should address all project-relevant aspects of data privacy and security. In addition to addressing how the project will conform to NSF's policy on the dissemination and sharing of research results, the Data Management and Sharing Plan should address the following topics if they are relevant to the project:

- **Handling of sensitive data**: This includes sensitivity of the data to be collected, ethics of data collection and identification of harms that could arise from its collection or inadvertent dissemination, techniques that will be used to protect the privacy of individuals and organizations associated with the data, and plans to request Institutional Review Board (IRB) approval for data collection, aggregation, and analysis.

- **Data sharing:** This covers methods for providing other researchers with controlled access to datasets and the time period during which data will be available. If the project will develop software or hardware, the Data Management and Sharing Plan should discuss not only what access other researchers will have to source code or

hardware design artifacts (e.g., specific open source licenses) and the physical location of the data repository (e.g., commercial cloud, private server, campus server), but also the method by which other researchers may access these products of the project (e.g., GitHub repository).

- **Authorization for data access and protection of data:** This addresses policies for authorizing access to the data and techniques (including security protections) that will be used to prevent the unauthorized dissemination of the data.

- **Source and provenance of the data:** This specifies the type of data (synthetic vs. real data), the source of the generated data (whether it was generated by any LLM/synthetic or collected/produced via real means/methods), and methods to tag data and its origin for provenance, accountability and reproducibility.

For additional information on the Dissemination and Sharing of Research Results, see:
https://www.nsf.gov/bfa/dias/policy/dmp.jsp.

5. Broadening Participation in Computing (BPC) Plans for projects with budgets greater than $600,000:

Each project with a budget greater than $600,000 and with a lead or non-lead organization (department, school, or institute) that primarily carries out research and education in computer science, computer engineering, information science, and/or other closely related field must include a BPC plan as a supplementary document at the time of submission. Each plan should begin with the heading "Broadening Participation in Computing (BPC) Plan –" followed by either "**Standalone" or "Connected"**.

- A **Standalone BPC Plan** does not include Departmental BPC Plans. Instead, the BPC activities of all PIs are listed in a single document that is up to 3 pages for the whole project and specifically addresses all five elements of a BPC plan: (1) the goal and context of the proposed activity, (2) intended population(s), (3) strategy, (4) measurement, and (5) PI engagement. *This option must be used if one or more of the collaborating institutions do not have a Departmental BPC Plan verified by BPCnet*.

- A **Connected BPC Plan** may be used when each PI and co-PI will engage in an activity listed in a Verified Departmental BPC Plan from their institution. Note that the (1) goal and context, (2) intended population, (3) strategy, and (4) measurement are already addressed in Verified Departmental BPC Plans. Therefore, a **Connected BPC Plan** is a document that only has to address the following, organized as:
    - up to 2 pages that describe (5) what strategies in the departmental plan the PI and co-PIs will focus on, their specific roles, and their preparation for their work;
    - followed by the verified Departmental BPC Plans from each institution.

The BPC plans should be submitted as one document (including departmental plans for Connected BPC plans) under the "Supplementary Documents" section by the lead institution. The BPC plan should not be utilized as a space to elaborate on other broader impact activities unrelated to addressing members of groups underrepresented in computing.

Any organizational resources that support BPC activities should also be described in the Facilities, Equipment and Other Resources section of the proposal (for additional information about Facilities, Equipment and Other Resources, see PAPPG Chapter II.D.2) if not already described in a linked departmental plan.

For projects where *none* of the PIs or co-PIs are from computing organizations as described above, a BPC plan is not required. To emphasize this point, PIs are encouraged to include a statement titled "Broadening Participation in Computing Plan" and the text "no PI on this project is in a computing organization, so no BPC plan is required".

6. Optional TTE Plan for RES proposals:

The TTE plan should be labeled as "Transition to Education Plan" and should not exceeding 2 pages. The TTE plan should contain the following components: (a) the description of the educational need to be addressed; (b) the novelty of the educational content; (c) how the research or technology will be transitioned into education and its impact on the cybersecurity workforce; (d) the identification of an intended population that will serve as early adopters of the proposed educational content; (e) the deployment plan for implementing/piloting the educational materials; (f) the explanation of

the post-grant, long-term sustainability of the educational content; (g) the extent to which learning experiences will feed back into research (if applicable); and (h) the justification of the TTE budget for the effort, which may include up to $50,000 within the RES total budget request.

No other Supplementary Documents, except as permitted by the NSF Proposal & Award Policies & Procedures Guide (such as RUI Certifications and RUI Impact Statements), are allowed.

Single Copy Documents:

Collaborators and Other Affiliations Information: Proposers should follow the guidance specified in PAPPG Chapter II.D.2.

Note the distinction to item (1) under Supplementary Documents above: the listing of all project participants is collected by the project lead and entered as a Supplementary Document, which is then automatically included with all proposals in a project. The Collaborators and Other Affiliations are entered for each participant within each proposal and, as Single Copy Documents, are available only to NSF staff.

Submission Checklist:

In an effort to assist proposal preparation, the following checklist is provided as a summary reminder of the solicitation-specific items that should be checked before submitting a proposal to this solicitation. For the items marked with Returned without Review (RWR), the proposal may be returned without review if the required item is non-compliant as of the date of proposal submission.

- The last paragraph of the Overview section of the Project Summary **must** consist of a prioritized list of 1-6 keywords, separated by semi-colons.
- (RWR) The maximum budget shown on the Cover Sheet and on the budget sheets **must** not exceed $300,000 for SEED proposals, $1,200,000 for RES proposals (including the budget for the optional TTE plan), and $500,000 ($600,000 if special conditions listed above are met) for EDU proposals.
- (RWR) If more than one PI is involved, a collaboration plan (up to 2 pages) **must** be provided for all projects with a budget greater than $600,000 as a Supplementary Document, even if all investigators are affiliated with the same organization.
- (RWR) **All projects with a total budget greater than $600,000 that include an organization (department, school, or institute) that primarily carries out research and education in computer science, computer engineering, information science, and/or other closely related fields, must include a BPC plan** submitted as a Supplementary Document. In the case of separately submitted collaborative proposals, the BPC plan should be submitted by the lead organization.
- A Project Personnel and Partner Institutions list included as a Supplementary Document.
- All EDU proposals must have detailed plans for assessment and evaluation that are clearly aligned with the project's stated goals based on appropriate metrics.

Proposals that do not comply with the requirements marked as RWR will be returned without review.

B. Budgetary Information

Cost Sharing:

Inclusion of voluntary committed cost sharing is prohibited.

Other Budgetary Limitations:

Project budgets must include funding for one or more project representatives (PI/co-PI/senior researcher or NSF-approved replacement) to attend the first SaTC PI meeting held after the beginning of the award. The first PI meeting for

awards made under this solicitation is expected to be held in Fall 2024, and approximately every two years thereafter. These requirements for PI meeting attendance apply to collaborative proposals as a whole, not to each part of a project.

C. Due Dates

- **Full Proposal Target Date(s)**:

  September 29, 2025

    Last Monday in September, Annually Thereafter

  January 26, 2026

    Last Monday in January, Annually Thereafter

      Proposers are highly encouraged to submit by a target date. Proposals will be accepted anytime, but they may miss a particular panel or committee meeting.

D. Research.gov/Grants.gov Requirements

For Proposals Submitted Via Research.gov:

To prepare and submit a proposal via Research.gov, see detailed technical instructions available at: https://www.research.gov/research-portal/appmanager/base/desktop?
_nfpb=true&_pageLabel=research_node_display&_nodePath=/researchGov/Service/Desktop/ProposalPreparationa
For Research.gov user support, call the Research.gov Help Desk at 1-800-381-1532 or e-mail rgov@nsf.gov. The Research.gov Help Desk answers general technical questions related to the use of the Research.gov system. Specific questions related to this program solicitation should be referred to the NSF program staff contact(s) listed in Section VIII of this funding opportunity.

For Proposals Submitted Via Grants.gov:

Before using Grants.gov for the first time, each organization must register to create an institutional profile. Once registered, the applicant's organization can then apply for any federal grant on the Grants.gov website. Comprehensive information about using Grants.gov is available on the Grants.gov Applicant Resources web-page: https://www.grants.gov/applicants. In addition, the NSF Grants.gov Application Guide (see link in Section V.A) provides instructions regarding the technical preparation of proposals via Grants.gov. For Grants.gov user support, contact the Grants.gov Contact Center at 1-800-518-4726 or by email: support@grants.gov. The Grants.gov Contact Center answers general technical questions related to the use of Grants.gov. Specific questions related to this program solicitation should be referred to the NSF program staff contact(s) listed in Section VIII of this solicitation.

Submitting the Proposal: Once all documents have been completed, the Authorized Organizational Representative (AOR) must submit the application to Grants.gov and verify the desired funding opportunity and agency to which the application is submitted. The AOR must then sign and submit the application to Grants.gov. The completed application will be transferred to Research.gov for further processing.

The NSF Grants.gov Proposal Processing in Research.gov informational page provides submission guidance to applicants and links to helpful resources including the NSF Grants.gov Application Guide, Grants.gov Proposal Processing in Research.gov how-to guide, and Grants.gov Submitted Proposals Frequently Asked Questions. Grants.gov proposals must pass all NSF pre-check and post-check validations in order to be accepted by Research.gov at NSF.

When submitting via Grants.gov, NSF strongly recommends applicants initiate proposal submission at least five business days in advance of a deadline to allow adequate time to address NSF compliance errors and resubmissions by 5:00 p.m. submitting organization's local time on the deadline. Please note that

some errors cannot be corrected in Grants.gov. Once a proposal passes pre-checks but fails any post-check, an applicant can only correct and submit the in-progress proposal in Research.gov.

Proposers that submitted via Research.gov may use Research.gov to verify the status of their submission to NSF. For proposers that submitted via Grants.gov, until an application has been received and validated by NSF, the Authorized Organizational Representative may check the status of an application on Grants.gov. After proposers have received an e-mail notification from NSF, Research.gov should be used to check the status of an application.

VI. NSF Proposal Processing And Review Procedures

Proposals received by NSF are assigned to the appropriate NSF program for acknowledgment and, if they meet NSF requirements, for review. All proposals are carefully reviewed by a scientist, engineer, or educator serving as an NSF Program Officer, and usually by three to ten other persons outside NSF either as *ad hoc* reviewers, panelists, or both, who are experts in the particular fields represented by the proposal. These reviewers are selected by Program Officers charged with oversight of the review process. Proposers are invited to suggest names of persons they believe are especially well qualified to review the proposal and/or persons they would prefer not review the proposal. These suggestions may serve as one source in the reviewer selection process at the Program Officer's discretion. Submission of such names, however, is optional. Care is taken to ensure that reviewers have no conflicts of interest with the proposal. In addition, Program Officers may obtain comments from site visits before recommending final action on proposals. Senior NSF staff further review recommendations for awards. A flowchart that depicts the entire NSF proposal and award process (and associated timeline) is included in PAPPG Exhibit III-1.

A comprehensive description of the Foundation's merit review process is available on the NSF website at: https://www.nsf.gov/bfa/dias/policy/merit_review/.

Proposers should also be aware of core strategies that are essential to the fulfillment of NSF's mission, as articulated in *Leading the World in Discovery and Innovation, STEM Talent Development and the Delivery of Benefits from Research - NSF Strategic Plan for Fiscal Years (FY) 2022 - 2026*. These strategies are integrated in the program planning and implementation process, of which proposal review is one part. NSF's mission is particularly well-implemented through the integration of research and education and broadening participation in NSF programs, projects, and activities.

One of the strategic objectives in support of NSF's mission is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions must recruit, train, and prepare a diverse STEM workforce to advance the frontiers of science and participate in the U.S. technology-based economy. NSF's contribution to the national innovation ecosystem is to provide cutting-edge research under the guidance of the Nation's most creative scientists and engineers. NSF also supports development of a strong science, technology, engineering, and mathematics (STEM) workforce by investing in building the knowledge that informs improvements in STEM teaching and learning.

NSF's mission calls for the broadening of opportunities and expanding participation of groups, institutions, and geographic regions that are underrepresented in STEM disciplines, which is essential to the health and vitality of science and engineering. NSF is committed to this principle of diversity and deems it central to the programs, projects, and activities it considers and supports.

A. Merit Review Principles and Criteria

The National Science Foundation strives to invest in a robust and diverse portfolio of projects that creates new knowledge and enables breakthroughs in understanding across all areas of science and engineering research and education. To identify which projects to support, NSF relies on a merit review process that incorporates consideration of both the technical aspects of a proposed project and its potential to contribute more broadly to advancing NSF's mission "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense; and for other purposes." NSF makes every effort to conduct a fair, competitive, transparent merit review process for the selection of projects.

1. Merit Review Principles

These principles are to be given due diligence by PIs and organizations when preparing proposals and managing projects, by reviewers when reading and evaluating proposals, and by NSF program staff when determining whether or not to recommend proposals for funding and while overseeing awards. Given that NSF is the primary federal agency charged with nurturing and supporting excellence in basic research and education, the following three principles apply:

- All NSF projects should be of the highest quality and have the potential to advance, if not transform, the frontiers of knowledge.
- NSF projects, in the aggregate, should contribute more broadly to achieving societal goals. These "Broader Impacts" may be accomplished through the research itself, through activities that are directly related to specific research projects, or through activities that are supported by, but are complementary to, the project. The project activities may be based on previously established and/or innovative methods and approaches, but in either case must be well justified.
- Meaningful assessment and evaluation of NSF funded projects should be based on appropriate metrics, keeping in mind the likely correlation between the effect of broader impacts and the resources provided to implement projects. If the size of the activity is limited, evaluation of that activity in isolation is not likely to be meaningful. Thus, assessing the effectiveness of these activities may best be done at a higher, more aggregated, level than the individual project.

With respect to the third principle, even if assessment of Broader Impacts outcomes for particular projects is done at an aggregated level, PIs are expected to be accountable for carrying out the activities described in the funded project. Thus, individual projects should include clearly stated goals, specific descriptions of the activities that the PI intends to do, and a plan in place to document the outputs of those activities.

These three merit review principles provide the basis for the merit review criteria, as well as a context within which the users of the criteria can better understand their intent.

2. Merit Review Criteria

All NSF proposals are evaluated through use of the two National Science Board approved merit review criteria. In some instances, however, NSF will employ additional criteria as required to highlight the specific objectives of certain programs and activities.

The two merit review criteria are listed below. **Both** criteria are to be given **full consideration** during the review and decision-making processes; each criterion is necessary but neither, by itself, is sufficient. Therefore, proposers must fully address both criteria. (PAPPG Chapter II.D.2.d(i). contains additional information for use by proposers in development of the Project Description section of the proposal). Reviewers are strongly encouraged to review the criteria, including PAPPG Chapter II.D.2.d(i), prior to the review of a proposal.

When evaluating NSF proposals, reviewers will be asked to consider what the proposers want to do, why they want to do it, how they plan to do it, how they will know if they succeed, and what benefits could accrue if the project is successful. These issues apply both to the technical aspects of the proposal and the way in which the project may make broader contributions. To that end, reviewers will be asked to evaluate all proposals against two criteria:

- **Intellectual Merit:** The Intellectual Merit criterion encompasses the potential to advance knowledge; and
- **Broader Impacts:** The Broader Impacts criterion encompasses the potential to benefit society and contribute to the achievement of specific, desired societal outcomes.

The following elements should be considered in the review for both criteria:

1. What is the potential for the proposed activity to
   a. Advance knowledge and understanding within its own field or across different fields (Intellectual Merit); and
   b. Benefit society or advance desired societal outcomes (Broader Impacts)?

2. To what extent do the proposed activities suggest and explore creative, original, or potentially transformative concepts?

3. Is the plan for carrying out the proposed activities well-reasoned, well-organized, and based on a sound rationale? Does the plan incorporate a mechanism to assess success?

4. How well qualified is the individual, team, or organization to conduct the proposed activities?

5. Are there adequate resources available to the PI (either at the home organization or through collaborations) to carry out the proposed activities?

Broader impacts may be accomplished through the research itself, through the activities that are directly related to specific research projects, or through activities that are supported by, but are complementary to, the project. NSF values the advancement of scientific knowledge and activities that contribute to achievement of societally relevant outcomes. Such outcomes include, but are not limited to: full participation of women, persons with disabilities, and other underrepresented groups in science, technology, engineering, and mathematics (STEM); improved STEM education and educator development at any level; increased public scientific literacy and public engagement with science and technology; improved well-being of individuals in society; development of a diverse, globally competitive STEM workforce; increased partnerships between academia, industry, and others; improved national security; increased economic competitiveness of the United States; and enhanced infrastructure for research and education.

Proposers are reminded that reviewers will also be asked to review the Data Management and Sharing Plan and the Mentoring Plan, as appropriate.

Additional Solicitation Specific Review Criteria

For all RES projects, reviewers will be asked to evaluate **the extent to which the project scope justifies the level of investment requested.**

For multi-investigator RES projects with a budget greater than $600,000, reviewers will be asked to comment on:

- the degree to which the Collaboration Plan adequately demonstrates that the participating investigators will work synergistically to accomplish the project objectives; and

- whether key personnel, and especially lead PIs, have allocated adequate time for both their individual technical contributions and the leadership of collaborative activities necessary to realize the synergistic effects of larger-scale research.

For RES projects with a TTE Plan, reviewers will be asked to comment on whether the TTE plan meaningfully addresses:

- the need and novelty of the educational content;

- how the research or technology will be transitioned into education and impact the cybersecurity workforce;

- the identification of an intended population that will serve as an early adopter of the proposed educational content;

- the deployment plan for implementing the pilot into an educational setting;

- the post-grant, long-term sustainability of the deployed educational content; and

- the extent to which learning experiences will feed back into research (if applicable).

For projects **that are required to include a BPC plan**, reviewer will be asked to comment on whether the Broadening Participation in Computing (BPC) plan meaningfully addresses the five elements of a BPC Plan:

- the goal and context of the proposed activity;

- intended population(s);

- strategy;

- measurement; and

- PI engagement.

B. Review and Selection Process

Proposals submitted in response to this program solicitation will be reviewed by Ad hoc Review and/or Panel Review, or Internal NSF Review.

The program will use ad-hoc, panel or internal review.

Reviewers will be asked to evaluate proposals using two National Science Board approved merit review criteria and, if applicable, additional program specific criteria. A summary rating and accompanying narrative will be completed and submitted by each reviewer. The Program Officer assigned to manage the proposal's review will consider the advice of reviewers and will formulate a recommendation.

After scientific, technical and programmatic review and consideration of appropriate factors, the NSF Program Officer recommends to the cognizant Division Director whether the proposal should be declined or recommended for award. NSF strives to be able to tell proposers whether their proposals have been declined or recommended for funding within six months. Large or particularly complex proposals or proposals from new recipients may require additional review and processing time. The time interval begins on the deadline or target date, or receipt date, whichever is later. The interval ends when the Division Director acts upon the Program Officer's recommendation.

After programmatic approval has been obtained, the proposals recommended for funding will be forwarded to the Division of Grants and Agreements or the Division of Acquisition and Cooperative Support for review of business, financial, and policy implications. After an administrative review has occurred, Grants and Agreements Officers perform the processing and issuance of a grant or other agreement. Proposers are cautioned that only a Grants and Agreements Officer may make commitments, obligations or awards on behalf of NSF or authorize the expenditure of funds. No commitment on the part of NSF should be inferred from technical or budgetary discussions with a NSF Program Officer. A Principal Investigator or organization that makes financial or personnel commitments in the absence of a grant or cooperative agreement signed by the NSF Grants and Agreements Officer does so at their own risk.

Once an award or declination decision has been made, Principal Investigators are provided feedback about their proposals. In all cases, reviews are treated as confidential documents. Verbatim copies of reviews, excluding the names of the reviewers or any reviewer-identifying information, are sent to the Principal Investigator/Project Director by the Program Officer. In addition, the proposer will receive an explanation of the decision to award or decline funding.

VII. Award Administration Information

A. Notification of the Award

Notification of the award is made to *the submitting organization* by an NSF Grants and Agreements Officer. Organizations whose proposals are declined will be advised as promptly as possible by the cognizant NSF Program administering the program. Verbatim copies of reviews, not including the identity of the reviewer, will be provided automatically to the Principal Investigator. (See Section VI.B. for additional information on the review process.)

B. Award Conditions

An NSF award consists of: (1) the award notice, which includes any special provisions applicable to the award and any numbered amendments thereto; (2) the budget, which indicates the amounts, by categories of expense, on which NSF has based its support (or otherwise communicates any specific approvals or disapprovals of proposed expenditures); (3) the proposal referenced in the award notice; (4) the applicable award conditions, such as Grant General Conditions (GC-1)*; and (5) any announcement or other NSF issuance that may be incorporated by reference in the award notice. Cooperative agreements also are administered in accordance with NSF Cooperative Agreement Financial and Administrative Terms and Conditions (CA-FATC) and the applicable Programmatic Terms and Conditions. NSF awards are electronically signed by an NSF Grants and Agreements Officer and transmitted electronically to the organization via e-mail.

*These documents may be accessed electronically on NSF's Website at
https://www.nsf.gov/awards/managing/award_conditions.jsp?org=NSF. Paper copies may be obtained from the NSF
Publications Clearinghouse, telephone (703) 292-8134 or by e-mail from nsfpubs@nsf.gov.

More comprehensive information on NSF Award Conditions and other important information on the administration of
NSF awards is contained in the NSF *Proposal & Award Policies & Procedures Guide* (PAPPG) Chapter VII, available
electronically on the NSF Website at https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.

Administrative and National Policy Requirements

Build America, Buy America

As expressed in Executive Order 14005, Ensuring the Future is Made in All of America by All of America's Workers (86 FR
7475), it is the policy of the executive branch to use terms and conditions of Federal financial assistance awards to
maximize, consistent with law, the use of goods, products, and materials produced in, and services offered in, the United
States.

Consistent with the requirements of the Build America, Buy America Act (Pub. L. 117-58, Division G, Title IX, Subtitle A,
November 15, 2021), no funding made available through this funding opportunity may be obligated for infrastructure
projects under an award unless all iron, steel, manufactured products, and construction materials used in the project are
produced in the United States. For additional information, visit NSF's Build America, Buy America web-page

Special Award Conditions:

For all awards, special award conditions will require that at least one representative (PI/co-PI/senior researchers or NSF-
approved replacement) from each SaTC project attend the first SaTC PI meeting held after the beginning of the award.
The first PI meeting for awards made under this solicitation is expected in Fall 2026.

C. Reporting Requirements

For all multi-year grants (including both standard and continuing grants), the Principal Investigator must submit an annual
project report to the cognizant Program Officer no later than 90 days prior to the end of the current budget period. (Some
programs or awards require submission of more frequent project reports). No later than 120 days following expiration of
a grant, the PI also is required to submit a final annual project report, and a project outcomes report for the general
public.

Failure to provide the required annual or final annual project reports, or the project outcomes report, will delay NSF
review and processing of any future funding increments as well as any pending proposals for all identified PIs and co-PIs
on a given award. PIs should examine the formats of the required reports in advance to assure availability of required
data.

PIs are required to use NSF's electronic project-reporting system, available through Research.gov, for preparation and
submission of annual and final annual project reports. Such reports provide information on accomplishments, project
participants (individual and organizational), publications, and other specific products and impacts of the project.
Submission of the report via Research.gov constitutes certification by the PI that the contents of the report are accurate
and complete. The project outcomes report also must be prepared and submitted using Research.gov. This report serves
as a brief summary, prepared specifically for the public, of the nature and outcomes of the project. This report will be
posted on the NSF website exactly as it is submitted by the PI.

More comprehensive information on NSF Reporting Requirements and other important information on the
administration of NSF awards is contained in the *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) Chapter VII,
available electronically on the NSF Website at https://www.nsf.gov/publications/pub_summ.jsp?ods_key=pappg.

Awardees must report BPC activities and outcomes in the Special Reporting Requirements section of annual reports
submitted to NSF. That section of the annual report should include:

- A summary of what each PI and co-PI did, including any changes to the plan;
- Numbers of events, participants, and participant demographics (if there are barriers to collecting this data, describe those limitations and provide the best estimates possible); and
- A reflection (supported by data if available) on progress, an unexpected challenges or results, and anything planned.

VIII. Agency Contacts

Please note that the program contact information is current at the time of publishing. See program website for any updates to the points of contact.

General inquiries regarding this program should be made to:

- Daniela A. Oliveira, Lead Program Director, CISE/CNS, telephone: (703) 292-4352, email: satc@nsf.gov
- Daniel R. Cosley, Program Director, CISE/IIS, telephone: (703) 292-8832, email: satc@nsf.gov
- Jeremy J. Epstein, Program Director, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, telephone: (703) 292-8910, email: satc@nsf.gov
- Karen Karavanic, Program Director, CISE/CNS, telephone: (703) 292-2594, email: satc@nsf.gov
- Sara Kiesler, Program Director, SBE/SES, telephone: (703) 292-8643, email: satc@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, telephone: (703) 292-4878, email: satc@nsf.gov
- Phillip A. Regalia, Program Director, CISE/CCF, telephone: (703) 292-2981, email: satc@nsf.gov
- Ambareen Siraj, Program Director, EDU/DGE, telephone: (703) 292-8182, email: satc-edu@nsf.gov
- Anna Squicciarini, Program Director, CISE/CNS, telephone: (703) 292-5177, email: satc@nsf.gov
- Selcuk Uluagac, Program Director, CISE/CNS, telephone: (703) 292-4540, email: satc@nsf.gov
- Xiaogang (Cliff) Wang, Program Director, CISE/CNS, telephone: (703) 292-2812, email: satc@nsf.gov
- Emily E. Witt, Program Director, MPS/DMS, telephone: (703) 292-5111, email: ewitt@nsf.gov
- ChunSheng (Sam) Xin, Program Director, EDU/DGE, telephone: (703) 292-7353, email: satc-edu@nsf.gov
- Li Yang, Program Director, EDU/DGE, telephone: (703) 292-2677, email: satc-edu@nsf.gov
- Qiaoyan Yu, Program Director, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov
- Nan Zhang, Expert, CISE/CNS, telephone: (703) 292-8950, email: satc@nsf.gov

For questions related to the use of NSF systems contact:

- NSF Help Desk: 1-800-381-1532
- Research.gov Help Desk e-mail: rgov@nsf.gov

For questions relating to Grants.gov contact:

- Grants.gov Contact Center: If the Authorized Organizational Representatives (AOR) has not received a confirmation message from Grants.gov within 48 hours of submission of application, please contact via telephone: 1-800-518-4726; e-mail: support@grants.gov.

SaTC Questions: satc@nsf.gov

IX. Other Information

The NSF website provides the most comprehensive source of information on NSF Directorates (including contact information), programs and funding opportunities. Use of this website by potential proposers is strongly encouraged. In

addition, "NSF Update" is an information-delivery system designed to keep potential proposers and other interested parties apprised of new NSF funding opportunities and publications, important changes in proposal and award policies and procedures, and upcoming NSF Grants Conferences. Subscribers are informed through e-mail or the user's Web browser each time new publications are issued that match their identified interests. "NSF Update" also is available on NSF's website.

Grants.gov provides an additional electronic capability to search for Federal government-wide grant opportunities. NSF funding opportunities may be accessed via this mechanism. Further information on Grants.gov may be obtained at https://www.grants.gov.

About The National Science Foundation

The National Science Foundation (NSF) is an independent Federal agency created by the National Science Foundation Act of 1950, as amended (42 USC 1861-75). The Act states the purpose of the NSF is "to promote the progress of science; [and] to advance the national health, prosperity, and welfare by supporting research and education in all fields of science and engineering."

NSF funds research and education in most fields of science and engineering. It does this through grants and cooperative agreements to more than 2,000 colleges, universities, K-12 school systems, businesses, informal science organizations and other research organizations throughout the US. The Foundation accounts for about one-fourth of Federal support to academic institutions for basic research.

NSF receives approximately 55,000 proposals each year for research, education and training projects, of which approximately 11,000 are funded. In addition, the Foundation receives several thousand applications for graduate and postdoctoral fellowships. The agency operates no laboratories itself but does support National Research Centers, user facilities, certain oceanographic vessels and Arctic and Antarctic research stations. The Foundation also supports cooperative research between universities and industry, US participation in international scientific and engineering efforts, and educational activities at every academic level.

Facilitation Awards for Scientists and Engineers with Disabilities provide funding for special assistance or equipment to enable persons with disabilities to work on NSF-supported projects. See Grant Proposal Guide Chapter II, Section D.2 for instructions regarding preparation of these types of proposals.

The National Science Foundation has Telephonic Device for the Deaf (TDD) and Federal Information Relay Service (FIRS) capabilities that enable individuals with hearing impairments to communicate with the Foundation about NSF programs, employment or general information. TDD may be accessed at (703) 292-5090 and (800) 281-8749, FIRS at (800) 877-8339.

The National Science Foundation Information Center may be reached at (703) 292-5111.

The National Science Foundation promotes and advances scientific progress in the United States by competitively awarding grants and cooperative agreements for research and education in the sciences, mathematics, and engineering.
To get the latest information about program deadlines, to download copies of NSF publications, and to access abstracts of awards, visit the NSF Website at https://www.nsf.gov.

- **Location:**   2415 Eisenhower Avenue, Alexandria, VA 22314

- **For General Information**   (703) 292-5111
  (NSF Information Center):

- **TDD (for the hearing-impaired):**   (703) 292-5090

- **To Order Publications or Forms:**

Send an e-mail to:	nsfpubs@nsf.gov
or telephone:	(703) 292-8134
• **To Locate NSF Employees:**	(703) 292-5111

Privacy Act And Public Burden Statements

The information requested on proposal forms and project reports is solicited under the authority of the National Science Foundation Act of 1950, as amended. The information on proposal forms will be used in connection with the selection of qualified proposals; and project reports submitted by proposers will be used for program evaluation and reporting within the Executive Branch and to Congress. The information requested may be disclosed to qualified reviewers and staff assistants as part of the proposal review process; to proposer institutions/recipients to provide or obtain data regarding the proposal review process, award decisions, or the administration of awards; to government contractors, experts, volunteers and researchers and educators as necessary to complete assigned work; to other government agencies or other entities needing information regarding proposers or nominees as part of a joint application review process, or in order to coordinate programs or policy; and to another Federal agency, court, or party in a court or Federal administrative proceeding if the government is a party. Information about Principal Investigators may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See System of Record Notices, NSF-50, "Principal Investigator/Proposal File and Associated Records," and NSF-51, "Reviewer/Proposal File and Associated Records." Submission of the information is voluntary. Failure to provide full and complete information, however, may reduce the possibility of receiving an award.

An agency may not conduct or sponsor, and a person is not required to respond to, an information collection unless it displays a valid Office of Management and Budget (OMB) control number. The OMB control number for this collection is 3145-0058. Public reporting burden for this collection of information is estimated to average 120 hours per response, including the time for reviewing instructions. Send comments regarding the burden estimate and any other aspect of this collection of information, including suggestions for reducing this burden, to:

Suzanne H. Plimpton
Reports Clearance Officer
Policy Office, Division of Institution and Award Support
Office of Budget, Finance, and Award Management
National Science Foundation
Alexandria, VA 22314