Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 18-572

REPLACES DOCUMENT(S):
NSF 17-576

National Science Foundation

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

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

Directorate for Mathematical & Physical Sciences
- Division of Mathematical Sciences

Directorate for Engineering
- Division of Electrical, Communications and Cyber Systems

Directorate for Education & Human Resources
- Division of Graduate Education

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

Proposals Accepted Anytime

MEDIUM Projects

Proposals Accepted Anytime

SMALL Projects

Proposals Accepted Anytime

EDU Projects

IMPORTANT INFORMATION AND REVISION NOTES

- There are no proposal submission deadlines for all designations and size categories in SaTC.
- An individual can participate as a PI, co-PI or senior personnel on no more than three SaTC proposals (one designated as CORE, one designated as TTP, one designated as EDU).
- The Frontier competition will not be held in FY 2019. The Frontier competition is expected to return in FY 2020 subject to availability of funds.
- The STARSS designation has been removed. Proposals with a hardware focus can be submitted to the CORE designation.
- The EDU designation maximum budget increased to $500,000 with durations of up to 3 years.
- There is a new requirement that all proposals must include a list of 1-3 keywords in the Project Summary corresponding to the topic areas listed in Section V. A. Proposal Preparation Instructions. Proposals without these keywords will be returned without review.
- There is a new requirement that all proposals must have a separate section titled “Relevance to Secure and Trustworthy Cyberspace” that should discuss the potential impact of the research with respect to the goals of the SaTC program, and clearly justify the keywords selected in the Project Summary with respect to the research plan. Proposals without this section will be returned without review.
- Additional information about topic areas of interest to the program has been added.
- Eligibility requirements for PIs, co-PIs, and senior personnel are clarified.
- Broadening Participation in Computing plans are strongly encouraged for Medium proposals, and approved plans are required before award.
- Proposers are asked to avoid requesting start dates between July 2 and September 30 of a given year.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 18-1), which is effective for proposals submitted, or due, on or after January 29, 2018.

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Secure and Trustworthy Cyberspace (SaTC)

Synopsis of Program:

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

The goals of the SaTC program are aligned with the Federal Cybersecurity Research and Development Strategic Plan (RDSP) and the National Privacy Research Strategy (NPRS) to protect and preserve the growing social and economic benefits of cyber systems while ensuring security and privacy. The RDSP identified six areas critical to successful cybersecurity research and development: (1) scientific foundations; (2) risk management; (3) human aspects; (4) transitioning successful research into practice; (5) workforce development; and (6) enhancing the research infrastructure. The NPRS, which complements the RDSP, identifies a framework for privacy research, anchored in characterizing privacy expectations, understanding privacy violations, engineering privacy-protecting systems, and recovering from privacy violations. In alignment with the objectives in both strategic plans, the SaTC program takes an interdisciplinary, comprehensive and holistic approach to cybersecurity research, development, and education, and encourages the transition of promising research ideas into practice.

The SaTC program welcomes proposals that address cybersecurity and privacy, and draw on expertise in one or more of these areas: computing, communication and information sciences; engineering; economics; education; mathematics; statistics; and social and behavioral sciences. **Proposals that advance the field of cybersecurity and privacy within a single discipline or interdisciplinary efforts that span multiple disciplines are both encouraged.**

Proposals must be submitted pursuant to one of the following designations, each of which may have additional restrictions and administrative obligations as specified in this program solicitation.

- CORE: This designation is the main focus of the SaTC research program, spanning the interests of NSF's Directorates for Computer and Information Science and Engineering (CISE), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral and Economic Sciences (SBE).
- EDU: The Education (EDU) designation will be used to label proposals focusing entirely on cybersecurity education.
- TTP: The Transition to Practice (TTP) designation will be used to label proposals that are focused exclusively on transitioning existing research results to practice.

CORE and TTP proposals may be submitted in one of the following project size classes:

- Small projects: up to $500,000 in total budget, with durations of up to three years;
- Medium projects: $500,001 to $1,200,000 in total budget, with durations of up to four years;

EDU proposals are limited to $500,000 in total budget, with durations of up to three years.

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.

- Nina Amla, Program Director, CISE/CCF, telephone: (703) 292-7991, email: namla@nsf.gov
- Dan Cosley, Program Director, CISE/IIS, telephone: (703) 292-8491, email: dcosley@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, telephone: (703) 292-8910, email: sgreensp@nsf.gov
- Timothy Hodges, Program Director, MPS/DMS, telephone: (703) 292-2113, email: thodges@nsf.gov
- Sara Kiesler, Program Director, SBE/SES, telephone: (703) 292-8643, email: skiesler@nsf.gov
- Sandip Kundu, Program Director, CISE/CNS, telephone: (703) 292-8950, email: skundu@nsf.gov
- Jenshan Lin, Program Director, ENG/ECCS, telephone: (703) 292-7950, email: jenlin@nsf.gov
- Victor P. Piotrowski, Program Director, EHR/DGE, telephone: (703) 292-5141, email: vpiotrow@nsf.gov

- Andrew D. Pollington, Program Director, MPS/DMS, telephone: (703) 292-4878, email: adpollin@nsf.gov
- Indrajit Ray, Program Director, CISE/CNS, telephone: (703) 292-8950, email: iray@nsf.gov
- Phillip A. Regalia, Program Director, CISE/CCF, telephone: (703) 292-2981, email: pregalia@nsf.gov
- Kevin Thompson, Program Director, CISE/OAC, telephone: (703) 292-4220, email: kthompso@nsf.gov
- Susanne Wetzel, Program Director, CISE/CNS, telephone: (703) 292-4642, email: swetzel@nsf.gov

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

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

Award Information

Anticipated Type of Award: Standard Grant or Continuing Grant

Estimated Number of Awards: 93

In FY 2019, NSF anticipates approximately 10 EDU awards, 55 Small awards, and 28 Medium awards.

Anticipated Funding Amount: $68,000,000

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 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 subawards 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 labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Who May Serve as PI:

As of the submission deadline, PIs, co-PIs, or other senior project personnel must hold primary, full-time, paid appointments in research or teaching positions at US-based campuses/offices of organizations eligible to submit to this solicitation (see above), with exceptions granted for family or medical leave, as determined by the submitting institution. Individuals with primary appointments at for-profit, non-academic organizations, or overseas branch campuses of US IHEs are not eligible, even if they also have an appointment at a US campus.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or Co-PI: 3

An individual can participate as a PI, co-PI or senior personnel on no more than three SaTC proposals. There is a limit of:

- one proposal designated as CORE (across Small and Medium);
- one proposal designated as TTP (across Small and Medium); and
- one proposal designated as EDU.

These limits apply for the period from Oct 1st to Sept 30th of the following year to all proposals in response to this solicitation, and are unrelated to any limits imposed in other NSF solicitations.

These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. In the event that an individual exceeds this limit, proposals received within the limit will be accepted based on earliest date and time of proposal submission. **No exceptions will be made.**

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 FastLane: *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 Deadline(s)** (due by 5 p.m. submitter's local time):

  Proposals Accepted Anytime

  MEDIUM Projects

  Proposals Accepted Anytime

  SMALL Projects

  Proposals Accepted Anytime

  EDU Projects

Proposal Review Information Criteria

Merit Review Criteria:

National Science Board approved criteria. Additional merit review considerations 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:

Standard NSF reporting requirements apply.

TABLE OF CONTENTS

I. INTRODUCTION

Making cyberspace secure and trustworthy is a critical challenge confronting society. The fragility and vulnerability of cyberspace have exposed societies and individuals to untold risks with severe consequences. Achieving a more secure cyberspace demands overcoming major scientific challenges, and realizing privacy and trust in cyberspace requires reconciling technology with human and societal needs. New advances in technology for cyberspace, changes in society, and adoption in new domains will also necessitate a rethinking of the interplay between security, privacy, and trust in cyberspace. The multi-disciplinary SaTC program seeks fundamentally new, principled approaches to protect and defend cyberspace against harmful actions by determined adversaries, and to assess their effectiveness. The SaTC program also seeks to explore innovative approaches for growing a capable, next-generation cyber workforce, and for accelerating the transition of successful cybersecurity research into practice and useful products and services.

The NSTC released the Federal Cybersecurity RDSP, a broad, coordinated Federal strategic plan for cybersecurity research and development, in order to preserve the growing social and economic benefits by thwarting adversaries and strengthening public trust of cyber systems. The plan calls for sound mathematical and scientific foundations, principled design methodologies, and metrics for evaluating success or failure for securing cyberspace. Highlighted in the plan is the need for socio-technical approaches that consider human, social, organizational, economic, and technical factors, and the complex interaction among them in the creation, maintenance, and operation of secure systems and infrastructure. The plan underscores the need for rapid transfer of research results to potential users, including the dissemination of best practices, outreach activities, and research infrastructure. Finally, the plan calls for research in cybersecurity education to satisfy the present and future workforce demands for qualified cybersecurity professionals.

The NSTC also announced the NPRS with the goal of enabling individuals, companies, and the government to benefit from cyber systems while effectively balancing those benefits with their risks to privacy. The strategy calls for characterizing key socio-technical issues that challenge privacy, and articulating goals for research in social, behavioral, and economic sciences needed for designing, using, and evaluating these socio-technical systems. The NPRS highlights the need for networking and information technology research for underlying privacy-enhancing technologies and related topics.

This solicitation supports these NSTC strategies for a secure and trustworthy cyberspace with privacy imperatives, which are critical to our national priorities in commerce, education, energy, financial services, healthcare, manufacturing, and defense. In strong alignment with the objectives in these plans, the SaTC program, in collaboration with industrial and international partners, takes an interdisciplinary, comprehensive and holistic approach to cybersecurity and privacy research, development, technology transfer, and education. SaTC leverages the disciplines of computing, communications and information sciences; economics; education; engineering; mathematics; statistics; and social and behavioral sciences.

II. PROGRAM DESCRIPTION

Cyberspace is a complex ecosystem that involves computer hardware, software, networks, data, people, and integration with the physical world. Society's overwhelming reliance on this complex cyberspace, however, has exposed its fragility and vulnerabilities that defy existing cyber-defense measures: corporations, agencies, national infrastructure, and individuals continue to suffer cyber-attacks. Achieving cybersecurity while protecting the privacy of individuals requires not only understanding the technical weaknesses of components of a system and how they can be addressed, but also understanding the human-centric aspects of secure cyber systems. Examining the fundamentals of security and privacy from many different perspectives can, in turn, lead to fundamentally new ways to design, build, and operate cyber systems, protect existing infrastructure, and motivate and educate individuals about security and privacy.

The SaTC program welcomes proposals that address cybersecurity and privacy, and that draw on expertise in one or more of these areas: computing, communications, and information sciences; engineering; economics; education; mathematics; statistics; and social and behavioral sciences. **Proposals that advance the field of cybersecurity and privacy within a single discipline or**

interdisciplinary efforts that span multiple disciplines are both encouraged.

Proposals must be submitted pursuant to one of the following designations, each of which may have additional restrictions and administrative obligations:

- CORE: This designation is the main focus of the SaTC research program, spanning the interests of NSF's Directorates for Computer and Information Science and Engineering (CISE), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral and Economic Sciences (SBE).
- EDU: The Education (EDU) designation will be used to label proposals focusing entirely on cybersecurity education.
- TTP: The Transition to Practice (TTP) designation will be used to label proposals that are focused exclusively on transitioning existing research results to practice.

Core and TTP proposals may be submitted in either of the following project size classes:

- Small projects: up to $500,000 in total budget, with durations of up to three years;
- Medium projects: $500,001 to $1,200,000 in total budget, with durations of up to four years;

EDU proposals are limited to $500,000 in total budget, with durations of up to three years.

PROJECT CLASSES

Any proposal submitted to the **CORE or TTP** designation for this solicitation must be consistent with one of the two project classes defined below. Proposals will be considered for funding within their project class.

1. **SMALL Projects:** Small projects, **with total budgets up to $500,000 for durations of up to three years,** are well suited to one or two investigators (PI and one co-PI or other Senior Personnel) and at least one student and/or postdoc.
2. **MEDIUM Projects:** Medium projects, **with total budgets ranging from $500,001 to $1,200,000 for durations of up to four years**, are well suited to one or more investigators (PI, co-PI and/or other Senior Personnel) and several students and/or postdocs.

    - Medium project descriptions must be comprehensive and well-integrated, and should make a convincing case that the collaborative contributions of the project team will be greater than the sum of each of their individual contributions. Rationale must be provided to explain why a budget of this size is required to carry out the proposed work.
    - Since the success of collaborative research efforts is known to depend on thoughtful coordination mechanisms that regularly bring together the various participants of the project, a separate Collaboration Plan is required for all Medium proposals with more than one investigator. Up to 2 pages are allowed for a Collaboration Plan and it must be submitted as a Supplementary Document. The length of, and level of detail provided in, the Collaboration Plan should be commensurate with the complexity of the proposed project. Collaboration plans and proposed budgets should demonstrate that 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. **If a Medium proposal with more than one investigator does not include a Collaboration Plan, that proposal will be returned without review.** Please see *Proposal Preparation Instructions* Section V.A for additional submission guidelines.

EDU Projects: EDU projects have **total budgets up to $500,000 for durations of up to three years.**

BROADENING PARTICIPATION IN COMPUTING

CISE has long been committed to Broadening Participation in Computing (BPC). The under-representation of many groups—including women, African Americans, Hispanics, American Indians, Alaska Natives, Native Hawaiians, Native Pacific Islanders, and persons with disabilities—in computing deprives large segments of the population of the opportunity to be creators of technology and not only consumers. Ending underrepresentation will require a range of measures, including institutional programs and activities as well as culture change across colleges, departments, classes, and research groups.

With this solicitation, CISE is expanding a pilot effort started last year encouraging the research community to engage in meaningful BPC activities. This new activity builds on many of the programs, research, and resources created in CISE's long history of support for BPC, and it aligns with the recommendations of the Strategic Plan for Broadening Participation produced by the CISE Advisory Committee in 2011. Specifically:

- **Each Medium project *must*, by the time of award, have in place an approved BPC plan.** In this ongoing pilot phase, CISE will work with each PI team following merit review and prior to making an award to ensure that plans are meaningful and include concrete metrics for success. CISE will also provide opportunities for PIs to share BPC experiences and innovations through program PI meetings. **PIs of Medium proposals are therefore strongly encouraged to consider this eventual requirement as they develop their proposals, and to include one- to three-page descriptions of their planned BPC activities under Supplementary Documents in their submissions.** Feedback will be provided on such plans.
- PIs submitting to the Small size class should note that CISE intends to conduct an evaluation of the effectiveness of the above approach and determine appropriate next steps, including potential further expansion of this effort in future years. **PIs of Small proposals are therefore strongly encouraged to include plans, or begin preparing to include plans, for broadening participation activities in their proposals.**

More information, including examples of BPC activities and metrics, can be found at: https://www.nsf.gov/cise/bpc/.

DESIGNATIONS

All SaTC proposals must be submitted to one of the following designations: CORE, EDU, or TTP. The focus of each designation is described below, along with any additional restrictions and administrative obligations.

All proposals ***must*** have a separate section titled “Relevance to Secure and Trustworthy Cyberspace” that discusses the potential

impact of the research with respect to the goals of the SaTC program, and clearly justifies the keywords selected in the Project Summary with respect to the research plan.

Secure and Trustworthy Cyberspace core research (CORE) designation

The scope of the SaTC core research program is broad and interdisciplinary, and welcomes foundational research on security and privacy from researchers in computer science, engineering, mathematics, and social, behavioral, and economic sciences. SaTC views cybersecurity as a socio-technical challenge and encourages proposals that advance the field of cybersecurity within a single discipline or multiple disciplines.

This solicitation focuses only on research directly supporting a safe, secure, resilient, and trustworthy cyberspace, conducted ethically with the highest scientific standards. Of special interest are proposals that are transformative, forward-looking, and offer innovative or clean-slate approaches that provide defenders a distinct advantage. Proposals whose security science exposes underlying principles having predictive value that extends across different security domains are especially encouraged. The program discourages proposals that address a sole vulnerability or device without advancing security science or considering the broader consequences of the proposed remedy. The SaTC program likewise discourages research focused primarily on the design and development of offensive techniques for exploiting vulnerabilities of systems that could be harmful to the operation of existing cyberinfrastructure.

All proposals should (a) include a clear and concise description of the threat model (if appropriate) and its relation to the proposed research; (b) discuss the generalizable theories and research methods that will be developed; and (c) discuss the tradeoffs and risks involved in the research plan.

Some specific research topics of interest for CORE proposals include, but are not limited to:

Authentication and Biometrics: Topics of interest include continuous authentication methods, remote authentication, multi-factor authentication, geolocation authentication, password-based methods, device technology, mobile authentication, identity and credential management, verifiers, robustness of authentication, and reverse engineering of electronic authentication credentials. Biometric authentication methods are also of interest. However, such methods that are based on human characteristics (such as physiological, neurological, and behavioral) must exhibit strong security guarantees, and be evaluated in the context of properly defined attack models.

Cryptography, Applied and Theory: Topics of interest include all applications of cryptography, especially in networks, cloud computing, electronic commerce, or in any other real-world setting. Symmetric and asymmetric encryption methods such as attribute-based encryption, functional encryption, fully homomorphic encryption, program obfuscation, information theoretic security, steganography, cryptanalysis and post-quantum cryptography are also of interest. Research on side channel and leakage resilience, memory-hard functions, secure multi-party computation, verifiable computation, non-malleable codes, computer-aided cryptographic proofs, and digital currencies are also in scope.

Cyber-Physical Systems (CPS): Topics of interest include research on security and privacy of cyber-physical systems that integrate sensing, computation, control, and networking into physical objects and infrastructure, connecting them to other systems, to users, and to each other. Systems of interest may or may not include humans in the loop. Also of interest are techniques for leveraging fundamental physical properties to improve security or privacy; system vulnerabilities and mitigations; system models; measuring and assessing security or privacy characteristics of systems; as well as human usability of system protection mechanisms.

Data Science: Topics of interest include advances in data analytics techniques for assessing, predicting, and enhancing aspects of systems and human behavior that are relevant to security and privacy; this includes applications, tools, and infrastructures at the level of individual systems, organizations, and social networks. Also of interest are advances in statistical and computational methods relevant to secure computational infrastructure for data science (e.g., secure and/or privacy-aware management, retrieval, analytics, and publishing of structured or unstructured data).

Formal Methods and Language-based Security: Topics of interest include formal definitions, models, and frameworks for security, privacy, and trust; security-preserving composition; and principled, secure design, analysis, verification, and synthesis techniques that bridge the gap between high-level security model and code development. Also of interest are information flow, programming language-based approaches, secure compilation, verification techniques for cryptography and other security protocols, and secure-by-construction techniques. All applications of formal techniques, especially those applied in distributed, operating, networked and hardware systems, are of special interest.

Hardware Security Architecture: Topics of interest include architectural support for authenticating devices and firmware, secure booting, secure firmware/software update, secure execution environments, multi-party computation, information flow tracking, privacy protection, and acceleration of security primitives and protocols. Also of interest are detection and mitigation of cache/memory side channels, covert channels, instruction-set architecture (ISA) to support security and privacy, identification/mitigation of security vulnerabilities in emerging technologies and paradigms, and hardware-assisted techniques for the security of systems including the Internet of Things (IoT) and software.

Hardware Security Design: Topics of interest include techniques for the development of secure and tamper-resistant hardware; identification, detection, and mitigation of Trojans; watermarking; side channels attacks; reverse engineering of hardware designs; and hardware obfuscation. Also of interest are hardware implementations of cryptography, acceleration of security primitives, modeling attacks and countermeasures, proximity verification, security metrics, trusted manufacturing, and tamper proofing and securing the hardware supply chain.

Information Authenticity: Topics of interest include emerging threat models stemming from unverifiable information provenance; measuring, assessing, predicting, and demonstrating how people decide that information is trustworthy; studying and modeling the methods and beliefs of actors in the creation, dissemination, consumption, sharing, and evolution of information online; imbalance, polarization, and/or lack of accountability; studying and modeling methods, evolution, and impact of data/information injection; computational techniques and systems for mitigating risks of information overload in specific security and privacy related domains, and enhancing authenticity in cyberspace as a whole.

Intrusion Detection: Topics of interest include detection of malicious attacks on systems, networks, datasets, algorithms, software, sensors, or other system-critical elements. Also of interest are techniques for profiling normal or abnormal system behaviors, the role of

human cognition in the detection of attacks, techniques for improving human usability of intrusion detection systems, metrics of attack severity or attacker effort, and methods of evaluating effectiveness of intrusion detection techniques.

Mathematics and Statistics: Topics of interest include research on the mathematical foundations of cryptographic protocols. In particular, research into the questions arising out of the development of secure post-quantum cryptographic methods such as those based on lattices, codes, multivariate functions, and supersingular isogenies; research into cryptographically effective multilinear maps; and novel applications of statistics and probability to security and privacy problems, such as intrusion detection and differential privacy. SaTC encourages collaborations between security researchers and mathematical scientists.

Networking, Wired and Wireless: Topics of interest include research on communication and network system security, including but not limited to information-theoretic security for wireless systems; jamming attack and defense; covert channel detection; anonymization and privacy methods; secure localization and location privacy; cross-layer methods for enhancing security and privacy; distributed denial-of-service (DDoS) attack and defense; key management and public key infrastructure (PKI) for networks; security and privacy in the home, enterprise, data center, cloud networks, software-defined networking (SDN), optical and Internet-scale and IoT-scale networks; as well as security and privacy in wireless networks, mobile sensing systems, cognitive radio, and dynamic spectrum access systems. Also of interest are anonymizing (e.g., onion routing) networks, anti-censorship, crowdsourcing security and privacy, network measurement and modeling for advancing security and privacy, networked systems and mobile applications that rely on a secure communication substrate. Research on analysis techniques and large-scale measurement of the security and privacy associated with social networking applications, tools, and infrastructures are also in scope.

Privacy, Applied and Theory: Topics of interest include a range of privacy-related subjects: from theoretical to experimental, from computational to social and behavioral, from usability to accountability, and from understanding the human perception of privacy to devising practical tools and systems that mitigate privacy concerns. There are many types of private information that may be of concern, ranging from personal health records to online activities and social media postings, from the anonymity of network communications to the anonymity of financial transactions, and from structured relational records to spatial-temporal data to unstructured text. The broad spectrum of private data in turn calls for a wide variety of scientific methods that are often interdisciplinary in nature, spanning mathematical, statistical, computational, social, behavioral, and economic sciences. Research on privacy that addresses not only the proper understanding, management, and protection of private information, but also the interplay of privacy and other complex social and technological challenges in building a secure and trustworthy cyberspace is also of interest. Examples include privacy issues arising from identity management, cloud computing, big data applications, surveillance, forensics, censorship, crowdsourcing, social networks, and behavioral targeting, among many others.

Social, Behavioral, and Economic Sciences: SaTC supports research on ethical, political, legal, cultural, or societal dimensions of security and privacy. Topics of interest include predicting and mitigating destructive online behavior (such as trolling, spamming, cyber-bullying, and ransoming); privacy, security, and trustworthiness associated with creating, sharing, disseminating, and filtering of information; intended and unintended consequences of security or privacy practices and policies; predicting effective responses by individuals or organizations to cyber-attacks and threats; cyber-security organizational strategies, investments, or governance; risks and benefits for security, privacy, or trust arising from new cyber-technologies. Approaches to these and other topics may include economic analyses of incentive structures and mechanisms, sociological research on demographic, structural, and cultural dimensions; behavioral science research on individual, group, and organizational behavior, or cognitive, statistical, or computational modeling and analyses of the behavior of individuals, groups, organizations, or networks. Proposals addressing social, behavioral, policy, organizational, economic, or governance dimensions of cybersecurity, privacy, and trust should build on the existing scientific literature, and contribute to fundamental principles and insights on the human aspects of cybersecurity and privacy.

Software: Topics of interest include techniques, methods, and tools for detecting and mitigating software vulnerabilities and malware through software analysis and testing; methods and tools for programmers and programming environments to design-in security and privacy capabilities during software development; and improvements to security and privacy in ubiquitous computing environments such as mobile, web, and domain-specific platforms. Also of interest are the incorporation of security and privacy requirements and validation into the software development process, principled techniques for composing security and privacy mechanisms, and methods to design security and privacy properties into components and systems.

Systems: Topics of interest include research on security and privacy of systems for computation or storage of data. Systems of interest range from small, stand-alone devices through smart phones, general-purpose computers, and networked systems at the enterprise or cross-enterprise levels, as well as browsers, application-based platforms, cloud computing systems, virtualized systems, and databases large or small. Also of interest are system vulnerabilities and mitigations; policy enforcement; accountability (e.g., logging, audit, provenance); system models; techniques supporting system design or implementation; and techniques for measuring and assessing security or privacy characteristics of systems and human usability of system protection mechanisms. Forensic techniques for identifying, preserving, recovering, and analyzing digital artifacts in host and virtual computing systems, memory, storage systems, computer and communications networks, mobile systems, cloud-based systems, and applications such as social media are of interest.

Usability and Human Interaction: Topics of interest include the analysis, design, implementation, and evaluation of user-facing/interface aspects of online systems that have significant privacy and security components or implications. These include design research and needs analyses to create or improve applications, devices, and tools that help end users and other stakeholders accomplish privacy- and security-related goals; the application of data analytic and social science techniques and theories to the design of these interfaces and tools; and the analysis and evaluation of their usability, utility, and effects around privacy and security at the level of individuals, dyads, groups, organizations, and societies. Also of interest is socio-technical research aimed at improving access to and accessibility of security and privacy supporting technologies and interfaces for special populations, broadly construed as people or groups with diverse characteristics that might affect cybersecurity risks and needs.

Transition to Practice (TTP) Designation

The objective of the TTP designation is to support the development, implementation, and deployment of later-stage and applied security or privacy research into an operational environment in order to bridge the gap between research and production. A TTP-designated proposal must specifically describe how the successful research results will be operationally deployed into an organization or technology. Collaborations with industry are strongly encouraged. The outcome of a TTP project is not solely intended to be commercialization, although the TTP may be a stepping-stone to a Small Business Innovation Research (SBIR) proposal or a commercial venture. A TTP may transition later-stage research by other means such as licensing to commercial or government end users or deployment into scientific research cyberinfrastructure or Research and Education Networks. Proposals that target the security of the scientific research cyberinfrastructure, and enable robust and reliable science through advances in reproducibility, provenance,

and privacy are highly encouraged. Topics of interest include: tools to detect behavioral anomalies across cyberinfrastructure systems, including detecting the tools and techniques of an attack and methods to mitigate security threats; tools to ensure the integrity of data as it traverses multiple environments such as mobile, cloud(s), and networks.

A TTP proposal must include a project plan that addresses major tasks and system development milestones as well as an evaluation plan for the working system.

In addition, TTP proposals will be evaluated with careful attention to the:

- Description of the problem being solved or need being addressed;
- Identification of a target user group or organization that will serve as an early adopter of the technology; if no early adopter is identified by the time the proposal is submitted, the proposal must specify milestones as to when an early adopter will be named;
- Deployment plan for implementing the pilot or prototype system into an operational environment;
- Novelty of the intended system, software, or architecture;
- Composition of the proposal team, which should demonstrate not only technical expertise in areas such as software engineering, but also skills in project management and systems development;
- Explanation of the post-grant, long-term software and/or system sustainability;
- Appropriateness of the budget for the effort; and
- Extent of collaboration with the university Technology Transfer Office (TTO) or similar organization from the PI's institution (a letter from the TTO or similar organization indicating its willingness to support the proposal is strongly encouraged).

Software developed under the TTP designation is not required to be open source. However, if open source software is developed, it should be released under an open source license listed by an Open Source Initiative (http://www.opensource.org/). If software will not be open source, a strong case must be provided justifying this approach. Software developers must demonstrate utilization of vulnerability analysis scanning tools throughout the development process and describe the software assurance best practices that will be followed.

Questions regarding the Transition to Practice (TTP) designation should be addressed directly to SaTC Program Officer Kevin Thompson (kthompso@nsf.gov) in the Office of Advanced Cyberinfrastructure (OAC).

Cybersecurity Education (EDU) Designation

The results of SaTC-funded research lead to widespread changes in our understanding of the fundamentals of cybersecurity. These new research outcomes, in turn, lead to fundamentally new ways to motivate and educate students about cybersecurity. The EDU designation is interested in the development of evidence-based and evidence-generating approaches that will improve cybersecurity education. EDU supports projects that: improve cybersecurity learning and learning environments, develop new curricular materials and methods of instruction, develop new assessment tools to measure student learning, promote teacher recruitment and training in the field of cybersecurity, and improve the diversity of the cybersecurity workforce. In addition to innovative work at the frontier of cybersecurity education, the program also encourages replications of research studies at different types of institutions and with different student bodies to produce deeper knowledge about the effectiveness and transferability of findings.

Proposals submitted to the EDU designation are expected to leverage successful results from previous and current basic research in cybersecurity and research on student learning, both in terms of intellectual merit and broader impacts, to address the challenge of expanding existing educational opportunities and resources in cybersecurity. This might include, but is not limited to, the following efforts:

- Improve teaching methods for delivering cybersecurity content to K-12 students that promote correct and safe online behavior, and the understanding of the foundational principles of cybersecurity;
- Develop and implement conferences to help K-12 teachers to integrate cybersecurity into computing courses;
- Support institutional collaborations between community colleges and four-year colleges or universities;
- Based on the results of previous and current basic research in cybersecurity, define a cybersecurity body of knowledge and establish curricular activities for new courses (both traditional and online), degree programs, and educational pathways leading to wide adoption nationally;
- Evaluate the effects that new and existing curricula have on student learning;
- Develop partnerships between centers of research in cybersecurity and institutions of higher education that lead to improved models for the integration of research experiences into cybersecurity degree programs;
- Conduct research that advances improvements in teaching and student learning in cybersecurity and, where possible, focuses on the participation of a broad and diverse population in cybersecurity education and workforce;
- Contribute to the implementation and sustainability of effective evidence-based curricular and co-curricular activities (e.g., evidence-based practices; professional and workforce development activities) for students studying cybersecurity at the K-12, undergraduate, or graduate level; and
- Develop and evaluate the effectiveness of cybersecurity competitions, games, and other outreach and retention activities.

Proposals must have clear and specific plans for assessment and evaluation. The evaluation should include formative evaluation for project improvement and summative evaluation to assess and document project outcomes, accomplishments, and lessons learned. At a minimum, the evaluator must be external to the project, but not necessarily to the institution. The evaluator cannot be a co-PI or other Senior Personnel on the project. The proposal must identify appropriate assessment and evaluation plans for project improvement, as well as plans for programmatic evaluation at the end of the project for accountability purposes. The evaluation plans must clearly align with the stated goals of the project. 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.

EDU projects are expected to contribute to the cybersecurity education knowledge base. The complexity, scope, and size of those contributions should be commensurate with the relevant experience and expertise of the project team and the institution. The publication, Common Guidelines for Education Research and Development, offers guidance on building the evidence base in STEM learning and is available at https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf13126. 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.

EDU proposal budgets are limited to $500,000 and their durations are limited to three years.

Questions about Cybersecurity Education proposals should be addressed directly to EDU Program Officer Victor Piotrowski (vpiotrow@nsf.gov) in the Directorate for Education and Human Resources.

SaTC PI MEETINGS

The SaTC program plans to host PI meetings every other year with participation from all active SaTC 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 expected to participate in these meetings. The next SaTC PI meeting is expected to be held in Fall 2019.

For all awards, one or more project representatives (PI/co-PI/senior researcher, or NSF-approved replacement) must attend the first PI meeting held after the beginning of the award. These requirements apply to a project, rather than to an institution. That is, participation of one of the representatives from a collaborative project is required, but attendance of a representative from every institution participating in that collaborative project is welcomed but not required.

SaTC FORUM

The SaTC program sponsors the SaTC Forum, a community forum for SaTC researchers, developers, and educators. All SaTC funded PIs are encouraged to maintain the project page corresponding to their SaTC project on the SaTC Forum. For the PI meeting, principal investigators or other project representatives **must** also provide a poster for the poster session and a slide describing their project(s), which will be made available on the SaTC Forum.

START DATES

In order to avoid overdue reports blocking award actions during the end of a fiscal year, institutions are discouraged from seeking project start dates between July 2 and September 30 of a given year. Awardee institutions 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.

III. AWARD INFORMATION

In FY 2019, NSF anticipates approximately 10 EDU awards, 55 Small awards and 28 Medium awards.

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 US, 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 subawards 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 labs, professional societies and similar organizations in the U.S. associated with educational or research activities.

Who May Serve as PI:

As of the submission deadline, PIs, co-PIs, or other senior project personnel must hold primary, full-time, paid appointments in research or teaching positions at US-based campuses/offices of organizations eligible to submit to this solicitation (see above), with exceptions granted for family or medical leave, as determined by the submitting institution. Individuals with primary appointments at for-profit, non-academic organizations, or overseas branch campuses of US IHEs are not eligible, even if they also have an appointment at a US campus.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or Co-PI: 3

An individual can participate as a PI, co-PI or senior personnel on no more than three SaTC proposals. There is a limit of:

- one proposal designated as CORE (across Small and Medium);
- one proposal designated as TTP (across Small and Medium); and
- one proposal designated as EDU.

These limits apply for the period from Oct 1st to Sept 30th of the following year to all proposals in response to this solicitation, and are unrelated to any limits imposed in other NSF solicitations.

These eligibility constraints will be strictly enforced in order to treat everyone fairly and consistently. In the event that an individual exceeds this limit, proposals received within the limit will be accepted based on earliest date and time of proposal submission. **No exceptions will be made.**

Additional Eligibility Info:

Subawards 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 Grants.gov or via the NSF FastLane system.

- Full proposals submitted via FastLane: Proposals submitted in response to this program solicitation should be prepared and submitted in accordance with the general guidelines contained in the *NSF Proposal & Award Policies & 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) 292-7827 or by e-mail from nsfpubs@nsf.gov. Proposers are reminded to identify this program solicitation number in the program solicitation block on the NSF Cover Sheet For Proposal to the National Science Foundation. Compliance with this requirement is critical to determining the relevant proposal processing guidelines. Failure to submit this information may delay processing.

- 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) 292-7827 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 the NSF FastLane system. PAPPG Chapter II.D.3 provides additional information on collaborative proposals.

See PAPPG Chapter II.C.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 following information SUPPLEMENTS (note that it does NOT replace) the guidelines provided in the NSF *Proposal & Award Policies & Procedures Guide (PAPPG)*.

All proposals must be submitted to the CNS division, regardless of the proposal's designation.

Proposal Titles:

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

- Secure and Trustworthy Cyberspace core research designation: **CORE**;
- Transition to Practice designation: **TTP**; or
- Cybersecurity Education designation: **EDU**.

CORE proposals can be Small or Medium. The acronym, CORE, should be followed by a colon, then the project class (Small or Medium) followed by a colon, and then the title of the proposed project. For example, if you are submitting a CORE Small proposal, the title of your proposal would be **SaTC: CORE: Small: Title**.

If you submit a proposal as part of a set of collaborative proposals, the title of the proposal should begin with the acronym that indicates the relevant designation followed by a colon, then the project class followed by a colon, then "Collaborative" followed by a colon, and then the title. For example, if you are submitting a collaborative set of proposals for a Medium project to the SaTC TTP designation, the title of each proposal would be **SaTC: TTP: Medium: Collaborative: Title**. The titles of Cybersecurity Education proposals must contain EDU. For example, the title of a collaborative EDU proposal should be **SaTC: EDU: Collaborative: Title.**

Project Summary:

SaTC proposals are grouped into "review panels" of related proposals for merit review and discussion. Panelists are selected for their expertise in the panel topic area. The suggested topic areas indicate the areas of panelist expertise that are most important for

understanding the innovative aspects of the proposal.

All proposals **must** include a prioritized list of 1-3 keywords separated by ";". The keywords must be drawn from the list of topic areas listed below, described in detail in Section II. Program Description, that best characterizes the project. **Proposals submitted to the EDU designation must choose Cybersecurity Education as one of the keywords, and proposals submitted to the TTP designation must choose Transition to Practice as one of the keywords.**

- Authentication and Biometrics
- Cryptography, Applied
- Cryptography, Theory
- Cyber-Physical Systems
- Cybersecurity Education
- Data Science
- Formal Methods and Language-based Security
- Hardware Security Architecture
- Hardware Security Design
- Information Authenticity
- Intrusion Detection
- Mathematics and Statistics
- Networking, Wired
- Networking, Wireless
- Privacy, Applied
- Privacy, Theory
- Social, Behavioral and Economic Sciences
- Software
- Systems
- Transition to Practice
- Usability and Human Interaction

Project Description:

Describe the research and education activities to be undertaken in **up to 15 pages for all proposal designations**.

Supplementary Documents:

In the Supplementary Documents Section, upload the following:

1. *A list of Project Personnel and Partner Institutions (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 Personnel, paid/unpaid Consultants or Collaborators, Subawardees, 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. Mary Smith; XYZ University; PI
   2. John Jones; University of PQR; Senior Personnel
   3. Jane Brown; XYZ University; Postdoc
   4. Bob Adams; ABC Community College; Paid Consultant
   5. Susan White; DEF Corporation; Unpaid Collaborator
   6. Tim Green; ZZZ University; Subawardee
2. *Collaboration Plans:*

   Since 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 Medium proposals that include more than one investigator 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, institutions, and/or disciplines; 3) identification of the specific coordination mechanisms that will enable cross-investigator, cross-institution, and/or cross-discipline scientific integration (e.g., yearly conferences, graduate student exchange, project meetings at conferences, use of the grid for videoconferences, software repositories, etc.), and 4) specific references to the budget line items that support collaboration and coordination mechanisms. **If a Medium proposal with more than one investigator does not include a Collaboration Plan of up to 2 pages, that proposal will be returned without review.**

   Small or EDU proposals that include more than one institution may include a Collaboration Plan of up to 2 pages.

3. *Data Management Plan (required):*

   Proposals must include a Supplementary Document of no more than two pages labeled "Data Management Plan." The data management 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 Plan should address the following topics if they are relevant to the project:

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

See Chapter II.C.2.j of the PAPPG for full policy implementation.

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

4. *Broadening Participation in Computing (BPC) Plans for Medium projects:*

   Each Medium project must, by the time of award, have in place an approved BPC plan. In this ongoing pilot phase, CISE will work with each PI team prior to making an award to ensure that plans are meaningful and include concrete metrics for success. CISE will also provide opportunities for PIs to share BPC experiences and innovations through program PI meetings. PIs of Medium proposals are therefore strongly encouraged to consider this eventual requirement as they develop their proposals, and to include descriptions (of one to three pages) of their planned BPC activities under Supplementary Documents in their submissions. Feedback will be provided on such plans.

No other Supplementary Documents, except as permitted by the NSF Proposal & Award Policies & Procedures Guide, are allowed.

Single Copy Documents:

Collaborators and Other Affiliations Information: Proposers should follow the guidance specified in Chapter II.C.1.e of the NSF PAPPG.

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.

Collaborators and Other Affiliations due to participants listed on item (1) under Supplementary Documents above who are not PIs, co-PIs, or Senior Personnel can be uploaded under Additional Single Copy Documents using Transfer File.

Submission Checklist:

In an effort to assist proposal preparation, the following checklists are provided as a reminder of the items that should be checked before submitting a SaTC proposal to this solicitation. These are a summary of the requirements described above. For the items marked with (RWR), the proposal will be returned without review if the required item is noncompliant as of the date of proposal submission.

- (RWR) The last line of the Project Summary **must** consist of the word "Keywords" followed by a colon and between 1-3 keywords, separated by semi-colons, corresponding to the list of topic areas (listed above).
- (RWR) The Project Description **must** have a section labeled “Relevance to SaTC” that discusses the potential impact of the research with respect to the goals of the SaTC program, and justifies the selection of the keywords.

- (RWR) Maximum budget shown on the Cover Sheet and on the budget sheets **must** not exceed $500,000 for Small proposals, $1,200,000 for Medium proposals, and $500,000 for EDU proposals.
- (RWR) If more than one PI is involved, a collaboration plan (up to 2 pages) **must** be provided for Medium projects as a Supplementary Document, even if all investigators are affiliated with the same institution.
- A Project Personnel and Partner Institutions list as a Supplementary Document should be included.

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:

Budgets for Education, Small, and Medium projects 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 in Fall 2019. 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 Deadline(s)** (due by 5 p.m. submitter's local time):

Proposals Accepted Anytime

MEDIUM Projects

Proposals Accepted Anytime

SMALL Projects

Proposals Accepted Anytime

EDU Projects

D. FastLane / Grants.gov Requirements

For Proposals Submitted Via FastLane:

To prepare and submit a proposal via FastLane, see detailed technical instructions available at: https://www.fastlane.nsf.gov/a1/newstan.htm. For FastLane user support, call the FastLane Help Desk at 1-800-673-6188 or e-mail fastlane@nsf.gov. The FastLane Help Desk answers general technical questions related to the use of the FastLane 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 webpage: http://www.grants.gov/web/grants/applicants.html. 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 the NSF FastLane system for further processing.

Proposers that submitted via FastLane are strongly encouraged to use FastLane 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 acknowledgement 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 *Building the Future: Investing in Discovery and Innovation - NSF Strategic Plan for Fiscal Years (FY) 2018 – 2022*. 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.C.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.C.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 underrepresented minorities 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 Plan and the Postdoctoral Researcher Mentoring Plan, as appropriate.

Additional Solicitation Specific Review Criteria

For multi-investigator **Medium** proposals, reviewers will be asked to:

- Comment on the extent to which the project scope justifies the level of investment requested, and the degree to which the Collaboration Plan adequately demonstrates that the participating investigators will work synergistically to accomplish the project objectives.
- Comment on 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.

Proposals submitted with the **Transition to Practice (TTP) designation** will be evaluated with careful attention to the following:

- The degree to which the project plan addresses system development milestones and an evaluation plan for the working system;
- The degree to which a target user group or organization who (that) will serve as an early adopter of the technology is identified;
- The deployment plan for implementing the capability or prototype system into an operational environment;
- The novelty of the intended system, software, or architecture;
- The composition of the proposal team, which should demonstrate not only technical expertise but also skills in project management and systems development;
- The appropriateness of the budget for the effort; and
- The extent of collaboration with the university TTO or similar organization from the PI's institution.

B. Review and Selection Process

Proposals submitted in response to this program solicitation will be reviewed by Ad hoc Review and/or Panel 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 applicants whether their proposals have been declined or recommended for funding within six months. Large or particularly complex proposals or proposals from new awardees 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 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 a Grants Officer in the Division of Grants and Agreements. 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)*; or Research Terms and Conditions* 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) 292-7827 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.

Special Award Conditions:

For Education, Small, and Medium 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 2019.

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 project report, and a project outcomes report for the general public.

Failure to provide the required annual or final 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 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.

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:

- Nina Amla, Program Director, CISE/CCF, telephone: (703) 292-7991, email: namla@nsf.gov
- Dan Cosley, Program Director, CISE/IIS, telephone: (703) 292-8491, email: dcosley@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, telephone: (703) 292-8910, email: sgreensp@nsf.gov
- Timothy Hodges, Program Director, MPS/DMS, telephone: (703) 292-2113, email: thodges@nsf.gov
- Sara Kiesler, Program Director, SBE/SES, telephone: (703) 292-8643, email: skiesler@nsf.gov
- Sandip Kundu, Program Director, CISE/CNS, telephone: (703) 292-8950, email: skundu@nsf.gov
- Jenshan Lin, Program Director, ENG/ECCS, telephone: (703) 292-7950, email: jenlin@nsf.gov
- Victor P. Piotrowski, Program Director, EHR/DGE, telephone: (703) 292-5141, email: vpiotrow@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, telephone: (703) 292-4878, email: adpollin@nsf.gov
- Indrajit Ray, Program Director, CISE/CNS, telephone: (703) 292-8950, email: iray@nsf.gov
- Phillip A. Regalia, Program Director, CISE/CCF, telephone: (703) 292-2981, email: pregalia@nsf.gov
- Kevin Thompson, Program Director, CISE/OAC, telephone: (703) 292-4220, email: kthompso@nsf.gov
- Susanne Wetzel, Program Director, CISE/CNS, telephone: (703) 292-4642, email: swetzel@nsf.gov

For questions related to the use of FastLane, contact:

- FastLane Help Desk, telephone: 1-800-673-6188; e-mail: fastlane@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 http://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** (NSF Information Center)**:** (703) 292-5111
- **TDD (for the hearing-impaired):** (703) 292-5090
- **To Order Publications or Forms:**

  Send an e-mail to: nsfpubs@nsf.gov

  or telephone: (703) 292-7827

- **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 awardees 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/grantees 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 applicants 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 Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records," 69 Federal Register 26410 (May 12, 2004), and NSF-51, "Reviewer/Proposal File and Associated Records," 69 Federal Register 26410 (May 12, 2004). 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
Office of the General Counsel
National Science Foundation
Alexandria, VA 22314