Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION
NSF 16-580

REPLACES DOCUMENT(S):
NSF 15-575

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
Division 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

Semiconductor Research Corporation

Submission Window Date(s) (due by 5 p.m. submitter's local time):

October 12, 2016 - October 19, 2016

October 12 - October 19, Annually Thereafter

LARGE Projects

October 12, 2016 - October 19, 2016

October 12 - October 19, Annually Thereafter

MEDIUM Projects

November 02, 2016 - November 16, 2016

November 2 - November 16, Annually Thereafter

SMALL Projects

December 01, 2016 - December 15, 2016

December 1 - December 15, Annually Thereafter

CYBERSECURITY EDUCATION Projects

IMPORTANT INFORMATION AND REVISION NOTES

Revision Summary: This is a revision of NSF 15-575, the solicitation for the SaTC Program. The revisions include:

1. Revisions to the submission deadline windows;
2. Revisions to the SaTC program description, including (a) replacement of perspectives with designations; (b) addition of topic areas; and (c) change to STARSS procedure to include parallel submission to and review by SRC;
3. Revisions to the Proposal Preparation Instructions;
4. Changes to eligibility information regarding (a) who may submit a proposal and (b) number of proposals per PI or Co-PI; and
5. Under Additional Solicitation Specific Review Criteria, reviewers are now asked to provide specific evaluation of 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.

The following recent revisions to the *Grant Proposal Guide* (GPG) will be closely observed for all submissions to this solicitation:

- GPG Chapter II.C.2.d.i requires that, “The Project Description must contain, as a separate section within the narrative, a section labeled 'Broader Impacts'."

- GPG Chapter II.C.2.f clarifies the requirements for Biographical Sketch(es).
- GPG Chapter II.C.2.h revises requirements for reporting Current and Pending Support.
- GPG Chapter II.C.2.j, Special Information and Supplementary Documentation, specifies the proper scope for letters of collaboration.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised *NSF Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 16-1), which is effective for proposals submitted, or due, on or after January 25, 2016.

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 has, however, exposed its fragility and vulnerabilities: corporations, agencies, national infrastructure and individuals have been victims of cyber-attacks. Achieving a truly secure cyberspace requires addressing both challenging scientific and engineering problems involving many components of a system, and vulnerabilities that arise 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 Secure and Trustworthy Cyberspace (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 R&D: (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 may be submitted in one of the following three 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;
- Large projects: $1,200,001 to $3,000,000 in total budget, with durations of up to five years.

In addition to the project size classes, 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: 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). Interdisciplinary proposals are welcomed to CORE.
- EDU: The Education (EDU) designation will be used to label proposals focusing entirely on cybersecurity education. *Note that proposals that are designated as EDU have budgets limited to $300,000 and durations of up to two years.*
- STARSS: The Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) designation will be used to label proposals that are submitted to the joint program focused on hardware security with the Semiconductor Research Corporation (SRC). *The STARSS designation may only be used for Small proposals. This designation has additional administrative obligations.*
- TTP: The Transition to Practice (TTP) designation will be used to label proposals that are focused exclusively on transitioning existing research results to practice. *The TTP designation may only be used for Small and Medium proposals.*

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, 1110, telephone: (703) 292-8910, email: namla@nsf.gov
- Dan Cosley, Program Director, CISE/IIS, 1125, telephone: (703) 292-8491, email: dcosley@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: sgreensp@nsf.gov
- Timothy Hodges, Program Director, MPS/DMS, 1020, telephone: (703) 292-2113, email: thodges@nsf.gov

- Sara Kiesler, Program Director, SBE/SES, 995, telephone: (703) 292-8643, email: skiesler@nsf.gov
- Wenjing Lou, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: wlou@nsf.gov
- Anita Nikolich, Program Director, CISE/ACI, 1145, telephone: (703) 292-8970, email: anikolic@nsf.gov
- Victor P. Piotrowski, Program Director, EHR/DGE, 865, telephone: (703) 292-5141, email: vpiotrow@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, 1025, telephone: (703) 292-4878, email: adpollin@nsf.gov
- Deborah Shands, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: dshands@nsf.gov
- Yan Solihin, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: ysolihin@nsf.gov
- Chengshan Xiao, Program Director, ENG/EECS, ENG/ECCS, 525, telephone: (703) 292-8339, email: cxiao@nsf.gov
- Nan Zhang, Program Director, CISE/IIS, 1125, telephone: (703) 292-8930, email: nanzhang@nsf.gov
- Celia Merzbacher, Semiconductor Research Corporation, telephone: (919) 941-9413, email: celia.merzbacher@src.org

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: 88

In FY 2017, NSF anticipates approximately 10 Education awards, 50 Small awards, 25 Medium awards and 3 Large awards.

Anticipated Funding Amount: $68,300,000

per year, dependent on the availability of funds.

Eligibility Information

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Universities and Colleges - Universities and two- and four-year colleges (including community colleges) accredited in, and having a campus located in, the US acting on behalf of their faculty members. Such organizations also are referred to as academic institutions.
- 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:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or Co-PI: 5

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

- two proposals designated as CORE and/or STARSS (across Small, Medium, and Large); and
- two proposals designated as TTP (either Small or Medium); and
- one proposal designated as EDU.

These limits apply per year to Small, Medium, Large and Education proposals in response to this particular solicitation, and are unrelated to any limits imposed in other NSF solicitations. Note, for example, that you may NOT submit two proposals to SaTC CORE, and three to STARSS, but you may submit one proposal to SaTC CORE, another to STARSS, two to TTP and one to EDU.

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, Part I: Grant Proposal Guide (GPG) Guidelines apply. The complete text of the GPG is available electronically on the NSF website at: http://www.nsf.gov/publications/pub_summ.jsp?ods_key=gpg.
  - 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: http://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

- **Submission Window Date(s)** (due by 5 p.m. submitter's local time):

  October 12, 2016 - October 19, 2016

  October 12 - October 19, Annually Thereafter

  LARGE Projects

  October 12, 2016 - October 19, 2016

  October 12 - October 19, Annually Thereafter

  MEDIUM Projects

  November 02, 2016 - November 16, 2016

  November 2 - November 16, Annually Thereafter

  SMALL Projects

  December 01, 2016 - December 15, 2016

  December 1 - December 15, Annually Thereafter

  CYBERSECURITY EDUCATION 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

Summary of Program Requirements

I. Introduction

II. Program Description

III. Award Information

IV. **Eligibility Information**

V. **Proposal Preparation and Submission Instructions**
- A. Proposal Preparation Instructions
- B. Budgetary Information
- C. Due Dates
- D. FastLane/Grants.gov Requirements

VI. **NSF Proposal Processing and Review Procedures**
- A. Merit Review Principles and Criteria
- B. Review and Selection Process

VII. **Award Administration Information**
- A. Notification of the Award
- B. Award Conditions
- C. Reporting Requirements

VIII. **Agency Contacts**

IX. **Other Information**

I. INTRODUCTION

Making cyberspace secure and trustworthy is one of the most important challenges 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 significant scientific challenges, and realizing privacy and trust in cyberspace requires a delicate balancing of technology with human and societal needs. Recognizing future advances in technologies for cyberspace, changes in society, and adoption in new domains will necessitate a rethinking of the relationships among security, privacy, and trust in cyberspace. The multi-disciplinary Secure and Trustworthy Cyberspace (SaTC) program seeks fundamentally new, principled approaches to protect and defend cyberspace against harmful actions by determined adversaries, and to measure their effectiveness. The SaTC program also seeks to explore innovative new approaches for growing a capable, next-generation cyber workforce, and for accelerating the transition of successful cybersecurity research into practice and useful products.

In February 2016, the National Science and Technology Council (NSTC) released the Federal Cybersecurity Research and Development Strategic Plan (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. 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 and outreach activities, and research infrastructure. Finally, the plan calls for research in cybersecurity education to satisfy present and future workforce demand of qualified cybersecurity professionals.

The NSTC also announced a National Privacy Research Strategy (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 is supportive of these NSTC strategies for a secure and trustworthy cyberspace with privacy imperatives, 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 that 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 cyberspace has, however, exposed its fragility and vulnerabilities: corporations, agencies, national infrastructure and individuals have been victims of 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 Secure and Trustworthy Cyberspace (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 within a single disciple or efforts that span multiple disciplines are both encouraged.**

Proposals may be submitted in one of the following three 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;
- Large projects: $1,200,001 to $3,000,000 in total budget, with durations of up to five years.

In addition to the project size classes, proposals must be submitted pursuant to one of the following designations, each of which may have additional restrictions and administrative obligations.

- CORE: The main focus of the SaTC research program, spanning CISE, ENG, MPS and SBE interests. Interdisciplinary proposals are welcomed to CORE.
- EDU: The Education (EDU) designation will be used to label proposals focusing entirely on cybersecurity education. *Note that proposals that are designated as EDU have budgets limited to $300,000 and durations of up to two years.*
- STARSS: The Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) designation will be used to label proposals that are submitted to the joint program focused on hardware security with the Semiconductor Research Corporation (SRC). *The STARSS designation may only be used for Small proposals. This designation has additional administrative obligations regarding SRC.*
- TTP: The Transition to Practice (TTP) designation will be used to label proposals that are focused exclusively on transitioning existing research to practice. *The TTP designation may be used for Small and Medium proposals.*

PROJECT CLASSES

With the exception of Cybersecurity Education (EDU) proposals described below, any proposal submitted to this solicitation must be consistent with one of three project classes defined below. Proposals will be considered for funding within their project classes.

- **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.

  Small projects may be submitted with these designations: CORE, STARSS, and TTP.

- **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 Collaboration Plans and they must be submitted as a document under Supplementary Documentation. 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.

  Medium projects may only be submitted with these designations: CORE and TTP.

- **LARGE Projects:**

  Large Projects, with total budgets ranging from $1,200,001 to $3,000,000 for durations of up to five years, are well suited to two or more investigators (PI, co-PI(s) and/or other Senior Personnel), and a team of students and/or postdocs. They should be large, multi-disciplinary, multi-organizational, and/or multi-institution projects that provide high-level visibility to grand challenge research areas in cybersecurity. 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 the individual participants' 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 Large proposals**. Up to 2 pages are allowed for Collaboration Plans and they must be submitted as a document under Supplementary Documentation. 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 Large proposal 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.

  Large projects may be submitted with these designations: CORE.

  A Large proposal should have a long-term vision, with objectives that could not be attained simply by a collection of Small or Medium proposals provided similar resources. Such research may or may not be multi-disciplinary. A successful Large project could also be a deep, intensively focused effort on a single cybersecurity problem in a single discipline.

DESIGNATIONS

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

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. 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 distinctive advantage. SaTC views cybersecurity as a socio-technical challenge and encourages proposals that advance the field of cybersecurity within a single discipline, or efforts that span multiple disciplines.

Topics in the area of computer and information sciences and engineering include, but are not limited to, research on theoretical and practical methods to design, build, analyze and operate cyber systems that are secure, private, and usable. Of interest are techniques to reason about, and predict, system security trustworthiness, including formal models, observable metrics, analytical methods, simulation, experimental deployment and, when reasonable and safe, deployment on live testbeds for experimentation at scale. Research that studies the tradeoffs among trustworthy computing properties, such as security and usability or accountability

and privacy, as well as work that examines the tension between security and human values such as openness and transparency, is also welcomed. SaTC also welcomes research that advances the creation, management, robust understanding, and intelligent analysis of data and information that addresses the cybersecurity challenge. Proposals should, when appropriate, include a clear and concise description of the threat model and its relation to the proposed research. 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 is discouraged.

Topics in the area of social, behavioral and economic sciences include, but are not limited to, research identifying cybersecurity and privacy risks and exploring the feasibility of potential solutions at the individual, group, organizational, market, and societal levels. Proposals that seek to understand, predict and explain attack and/or defense behaviors as well as prevention, and that contribute to developing strategies for remediation are of interest. Related proposals that contribute to the design of incentives, markets or institutions to reduce either the likelihood of cyber attacks or the negative consequences of cyber attacks are welcomed, as are proposals that examine incentives and motivations of individuals. Proposals that advance social networking theories and methods are welcomed. All research approaches, including (but not limited to) theoretical, experimental, observational, statistical, survey, and simulation-based, are of interest. Expected contributions include identifying generalizable theories and advancing research methods that push the boundaries of our understanding of social, behavioral, or economic phenomena in cybersecurity, privacy, and attack and/or defense behaviors, prevention, and successful remediation strategies.

Topics in the area of statistical and mathematical sciences include, but are not limited to, research on mathematical foundations of cryptography; new algorithms, risk assessments and statistical methods in cybersecurity and privacy; and non-traditional constructive approaches for efficient hiding of digital information, building on recent mathematical advances making encryption schemes resistant to both classical and quantum attacks.

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

Access control: Topics of interest include language-based techniques and frameworks for specifying authorizations; access control models to support various computing environments and resource management conditions; techniques for automating policy generation or consistency checking; techniques for improving human usability of policy specification; and metrics and methods of evaluating characteristics related to access control.

Authentication, Biometrics and Forensics: Topics of interest include continuous authentication methods, remote authentication, multi-factor authentication, password-based methods, device technology, mobile authentication, identity and credential management, verifiers, robustness of authentication, and reverse engineering of electronic authentication credentials. Biometrics authentication is a form of identification based on human characteristics such as physiological, neurological and behavioral. Also of interest are device technology, robustness, cancelable biometrics, and privacy risks.

Cryptography and cryptanalysis (theory and applied): Topics of interest include symmetric and asymmetric encryption methods such as attribute-based encryption, functional encryption, fully homomorphic encryption, program obfuscation, information theoretic security, steganography and post-quantum cryptography. Also of interest are side channel and leakage resilience, secure multi-party computation, verifiable computation, computer-aided cryptographic proofs, and digital currencies. All applications of cryptography, especially those applied in networks, cloud computing, electronic commerce, and other realistic settings, are of special interest.

Cyber-Physical Systems (CPS) and the Internet of Things (IoT): Topics of interest include techniques leveraging fundamental physical properties and control laws in the context of their use to increase security, protect privacy, ensure resiliency, improve usability, and support scalability with extreme heterogeneity and mobility. Potential areas of application are agriculture, emergency services, energy, healthcare, manufacturing, participatory science, robotics, social media, and transportation.

Data analytics and data science: Topics of interest include data analytics techniques for assessing, predicting and enhancing system trustworthiness, as well as statistical and computational methods for enabling the secure management, exploration and analytics of sensitive data. Also of interest are the detection of adversarial and harmful behavior through data science methods such as machine learning, data mining, natural language processing, etc.; and the design of 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 techniques: Topics of interest include formal definitions, models, frameworks for security, privacy and trust; security-preserving composition; and principled, secure design, analysis and verification 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 and networked systems, are of special interest.

Hardware security: Topics of interest include techniques for the development of secure and tamper-resistant hardware, as well as hardware and hardware-assisted techniques for the security of systems (including IoT) and software. Topics of interest include, but are not limited to, the identification, detection and mitigation of Trojans, side channels attacks, reverse engineering of hardware designs, and hardware obfuscation. Also of interest are hardware implementations of cryptography, architectural support and acceleration of security primitives, security metrics, trusted manufacturing, and securing the hardware supply chain.

Human aspects: There are a wide range of topics that systematically address the human implications of cybersecurity and privacy, particularly the social, behavioral, ethical, policy, organizational, economic, and governance issues that arise in connection with efforts to maintain or to improve cybersecurity and privacy. Topics of interest include, but are not limited to, economic analysis of incentives to explain why individuals and organizations do (and do not) take action to respond to cybersecurity threats; behavioral research on persuasion to train, incentivize, or influence end users to improve their cybersecurity positions; sociological research to understand how the legal system (including legal institutions and actors) adapts to increasing calls for cybersecurity; organizational research to identify organizational strategies for advancing cybersecurity; as well as socio-technical research to develop cybersecurity technologies, policies, and processes with diverse individuals in mind, including children and teens, the elderly, low-income families, and people with visual and physical impairments.

Intrusion detection: Topics of interest include research into the detection of malicious attacks on systems, networks, datasets, algorithms, software, sensors or other system-critical elements. Also of interest are techniques for detecting attacks (before, during or after), profiling normal or abnormal system behaviors, forensics, 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: Tools from a variety of mathematical science areas have been critical in security. Some areas are statistics, probability, logic, combinatorics, number theory, graph theory, mathematical modeling, arithmetic and algebraic geometry, lattice theory and algebra. For example probability and statistics are relevant to intrusion detection, cryptographic protocols are often built on hard mathematical schemes, and understanding the vulnerabilities and structures in the Internet provides a number of serious mathematical challenges. SaTC encourages collaborations between security researchers and mathematical scientists.

Networks: Topics of interest include research on communication and network system security, including but not limited to physical layer security; anonymization and privacy methods; cross-layer methods for enhancing security and privacy; availability of communications and survivability of networks in the presence of attacks; key management and public key infrastructure (PKI) for networks; security and privacy in the home, enterprise, data center, cloud networks, SDN, optical and Internet-scale and IoT-scale networks; as well as security and privacy in wireless networks, such as cellular, vehicular, mesh, sensor, cognitive radio networks, millimeter wave (mmWave) and photonic wireless networks. Also of interest are TOR 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.

Privacy: Topics of interest include research on 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 inter-disciplinary 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, and behavioral targeting, among many others.

Social networks: Topics of interest include research on analysis techniques and large-scale measurement of the security and privacy associated with social networking applications, tools and infrastructures. Also of interest are privacy issues that surround the personal information extracted by social network tools and applications, cyber threats that emerge as a result of social network usage, and defenses against attacks on social networking applications and tools. Additionally, anonymization and anti-censorship techniques and privacy-preserving techniques for social networks are welcomed.

Software engineering: 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); system models; techniques supporting system design or implementation; metrics; and techniques for measuring and assessing security or privacy characteristics of systems, and human usability of system protection mechanisms.

Usability: Topics of interest include novel methods that strike a balance between security, privacy and functionality of systems and devices, while keeping in mind the perspective of the end user. Topics include: improved interface design with ease of use; incorporation of affective, behavioral, cognitive and linguistic factors into the human decision making model associated with systems interfaces; and metrics to evaluate the effectiveness of improved usability features.

Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) Designation

STARSS is a joint effort of the National Science Foundation (NSF) and the Semiconductor Research Corporation (SRC). A STARSS proposal is similar to other Small proposals submitted to the SaTC program except that proposers must also submit the proposal to SRC according to SRC proposal and submission guidelines. It is expected that, at a minimum, the project summary, project description, and references cited will be identical in the proposals submitted separately to NSF and SRC. Additional proposal documentation and materials specific to SRC are required. Please see SRC STARSS Proposal Submission Guide.

Hardware is the foundation of electronic and IT systems that are essential to almost every aspect of daily life, business, the economy, and national security. Increasingly, these systems are part of the growing and dynamic web of interconnected systems with poorly understood security known as the “Internet of Things” (IoT). Any approach to incorporating security into the IoT must take into consideration (1) the diversity of systems and components that are interconnected and (2) the very low power (and other resources) available for any added functionality, especially at the “edge nodes”. Other trends that also are creating security risks include the increasing complexity of leading-edge systems; the lengthening and globalization of the supply chain; and the growth in use of third-party design IP.

STARSS seeks to enable greater security, trustworthiness, assurance and resilience in semiconductor-based systems. Making integrated circuit and systems secure by design is more effective than finding and addressing vulnerabilities, whether inadvertent or intentional, after deployment. The goal is to develop strategies, techniques and tools that avoid and mitigate vulnerabilities and lead to semiconductors and systems that are resistant and resilient to attack or tampering. The following topics are representative of relevant research areas:

- **Architecture and design**. Approaches, models and frameworks for reasoning about and specifying hardware-specific security properties. These design and architecture approaches should not be studied in isolation; the impact of security at the level of circuits and processors must be understood in terms of system-wide functionality, performance, and power goals.
- **Principles, properties and metrics.** Hardware security design principles and semiconductor-specific properties. Security metrics for evaluating or comparing designs, and that are extensible and potentially useful for privacy composition or for providing trust evidence at the system level.
- **Verification.** Tools, techniques, and methodologies for verifying hardware-specific security properties and enforcing security design principles. Innovative approaches to establish safety properties without knowing all aspects of the design, and thereby providing strong provable assurance. Approaches to increase automation of security verification and analysis.
- **Embedded software and firmware.** Strategies and techniques to reduce vulnerabilities in embedded software and firmware, and for providing updates to address known vulnerabilities discovered after deployment in the field.
- **Authentication and attestation.** Models for the insertion of artifacts or design elements that are verifiable during design and throughout the life cycle. Supporting issues, such as the generation, protection and establishment of trust models for hardware-implemented keys, are also of interest.

Small research proposals targeting hardware security may be submitted to the SaTC CORE designation. For topics within scope, STARSS provides an opportunity for close collaboration with industry through SRC. Hardware security proposals not specifically addressing STARSS criteria (see Section VI) should be submitted to the SaTC CORE designation. When considering topics for

research, proposers are encouraged to review past awards made by the STARSS activity and identify areas that are within the technical scope and not already the subject of study. Proposals in areas not already covered by prior projects are particularly encouraged. To find past STARSS awards, go to http://www.nsf.gov/awardsearch and search for "STARSS."

Questions regarding SRC policies and guidelines should be addressed directly to Celia Merzbacher, Semiconductor Research Corporation, at (919) 941-9413 or celia.merzbacher@src.org.

Transition to Practice (TTP) Designation

The objective of the Transition to Practice (TTP) designation is to support the development, implementation, and deployment of later-stage and applied security research into an operational environment. A TTP-designated proposal must specifically describe how the successful research results will be further developed and deployed in organizations or industries, including in networks and end systems. Collaborations with industry are strongly encouraged. The outcome of a TTP project is not intended to be solely commercialization. A TTP may be a stepping-stone to an Small Business Innovation Research (SBIR) activity by means of a proof of concept. A TTP may transition later-stage research by a number of other means.

A TTP proposal must include a project plan that addresses system development milestones and 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 capability 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 the open source license listed by the 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 are encouraged to 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 Anita Nikolich in the Division of Advanced Cyberinfrastructure (ACI) at anikolic@nsf.gov.

Cybersecurity Education (EDU) Designation

On occasion, the results of SaTC-funded research lead to widespread changes in our understanding of the fundamentals of cybersecurity that can, in turn, lead to fundamentally new ways to motivate and educate students about cybersecurity. Proposals submitted to this designation 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:

- Based on the results of previous and current basic research in cybersecurity, define a cybersecurity body of knowledge and establish curricular recommendations for new courses (both traditional and online), degree programs, and educational pathways leading to wide adoption nationally;
- Evaluate the effects of these curricula on student learning;
- Encourage the participation of a broad and diverse population in Cybersecurity Education;
- Develop virtual laboratories to promote collaboration and resource sharing in Cybersecurity Education;
- 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;
- Develop and evaluate the effectiveness of cybersecurity competitions, games, and other outreach and retention activities; and
- Conduct research that advances improvements in teaching and student learning in cybersecurity and, where possible, focuses on broadening participation.

Cybersecurity Education proposal budgets are limited to $300,000 and their durations are limited to two years.

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

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.

For Small, Medium and Education 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. For Large awards, one or more project representatives (PI/co-PI/senior researcher, or NSF-approved replacement) must attend **every** PI meeting held throughout the duration of the grant. These requirements apply to collaborative proposals as a whole, not to each institution within a project.

In addition, in years in which no SaTC PI meeting is held, SRC will hold a review of all Small STARSS-designated projects.

EMBEDDED REU SUPPLEMENTS

The *Research Experiences for Undergraduates (REU): Sites and Supplements* solicitation (NSF 13-542) gives instructions for embedding a request for a REU Supplement in a proposal. Proposers are invited to embed a request for a REU Supplement in the typical amount **for one year only** according to standard guidelines (detailed below). The amounts of the REU Supplements **do not** count against the budget limitations described in this solicitation for the Small, Medium, and Large project classes.

For single investigator projects, SaTC REU supplemental funding requests should typically be for no more than two students for one year. Research teams funded through multi-investigator projects may request support for a larger number of students, commensurate with the size and nature of their projects. For example, for projects involving two principal investigators, REU supplemental funding is typically requested for about four undergraduates for one year. Requests for larger numbers of students should be accompanied by detailed justifications.

SaTC expects to provide up to $8,000 per student per year through the REU supplemental support mechanism. As described in the REU program solicitation (NSF 13-542), indirect costs (F&A) are not allowed on Participant Support Costs in REU Site or REU Supplement budgets.

REU stipend support is one way to retain talented students in undergraduate education, while providing meaningful research experiences. The participation of students from groups underrepresented in cybersecurity -- underrepresented minorities, women and persons with disabilities -- is strongly encouraged. In addition, SaTC encourages REU supplements that specifically afford US veterans an opportunity to engage in meaningful research experiences.

SaTC REU supplemental funding requests must describe results of any previous such support, including students supported, papers published, etc. Other factors influencing the supplemental funding decisions include the number of REU requests submitted by any one principal investigator across all of her/his NSF grants.

Investigators are encouraged to refer to the REU program solicitation (NSF 13-542) for detailed information concerning submission requirements. For questions, contact one of the Cognizant Program Officers listed in this solicitation.

III. AWARD INFORMATION

In FY 2017, NSF anticipates approximately 10 Education awards, 50 Small awards, 25 Medium awards and 3 Large awards.

Small STARSS projects selected for joint funding by NSF and SRC will be funded through separate NSF and SRC funding instruments. For each such project, NSF support will be provided via an NSF grant and SRC support will be provided via an SRC contract. (Please note: The budget submitted with the proposal should include all necessary project funds without regard to the two funding organizations; NSF and SRC will inform selected PIs of the breakdown in funding between the two organizations, and will request revised budgets as appropriate).

IV. ELIGIBILITY INFORMATION

Who May Submit Proposals:

Proposals may only be submitted by the following:

- Universities and Colleges - Universities and two- and four-year colleges (including community colleges) accredited in, and having a campus located in, the US acting on behalf of their faculty members. Such organizations also are referred to as academic institutions.
- 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:

There are no restrictions or limits.

Limit on Number of Proposals per Organization:

There are no restrictions or limits.

Limit on Number of Proposals per PI or Co-PI: 5

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

- two proposals designated as CORE and/or STARSS (across Small, Medium, and Large); and
- two proposals designated as TTP (either Small or Medium); and
- one proposal designated as EDU.

These limits apply per year to Small, Medium, Large and Education proposals in response to this particular solicitation, and are unrelated to any limits imposed in other NSF solicitations. Note, for example, that you may NOT submit two proposals to SaTC CORE, and three to STARSS, but you may submit one proposal to SaTC CORE, another to STARSS, two to TTP and one to EDU.

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:

For U.S. universities and two- and four-year colleges with overseas campuses, this solicitation restricts eligibility to research activities using the facilities, equipment, and other resources of the campus(es) located in the U.S. only. Note: this restriction is directed at institutional eligibility only; it is not intended to restrict international collaborations or research activities by subsequent awardees.

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 Grant Proposal Guide (GPG). The complete text of the GPG is available electronically on the NSF website at: http://www.nsf.gov/publications/pub_summ.jsp?ods_key=gpg. Paper copies of the GPG 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: (http://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. Chapter II, Section D.5 of the Grant Proposal Guide provides additional information on collaborative proposals.

See Chapter II.C.2 of the GPG 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 GPG instructions.

The following information SUPPLEMENTS (note that it does NOT replace) the guidelines provided in the NSF Grant Proposal Guide (GPG).

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**;
- Secure, Trustworthy, Assured and Resilient Semiconductors and Systems designation: **STARSS**;
- Transition to Practice designation: **TTP**; and
- Cybersecurity Education designation: **EDU**.

CORE proposals can be Small, Medium or Large. The acronym, CORE, should be followed by a colon, then the project class (Small, Medium or Large) 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 Secure and Trustworthy Cyberspace Core research (CORE) designation, the title of each proposal would be **SaTC: CORE: Medium: Collaborative: Title**.

STARSS proposals must be in the Small project class. Therefore, valid STARSS-specific title styles are:

SaTC: STARSS: Small: Title
SaTC: STARSS: Small: Collaborative: Title

TTP proposals must be in the Small or Medium project classes. Therefore, valid TTP-specific title styles are:

SaTC: TTP: Small: Title
SaTC: TTP: Small: Collaborative: Title
SaTC: TTP: Medium: Title
SaTC: TTP: Medium: Collaborative: Title

The titles of Cybersecurity Education proposals must contain a single acronym: EDU. Thus, the only valid EDU-specific title styles are:

SaTC: EDU: Title
SaTC: EDU: Collaborative: Title

In addition to the above titles, proposals from PIs in institutions that have RUI (Research in Undergraduate Institutions) eligibility should include "RUI: " immediately before the proposal title, for example, **SaTC: CORE: Medium: RUI: Title**.

PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **SaTC: CORE: Small: GOALI: Title**.

Project Description:

Describe the research and education activities to be undertaken in **up to 15 pages for Small, Medium, and Education proposals and up to 20 pages for Large proposals**.

Proposers are reminded that, as specified in GPG Chapter II.C.2.d:

- The Project Description must contain, as a separate section within the narrative, a section labeled “Broader Impacts.”This section should provide a discussion of the broader impacts of the proposed activities. **Proposals without this clearly-identifiable section will be returned without review.**
- Results from Prior NSF Support: If any PI or co-PI identified on the proposal has received NSF funding with a start date in the past five years (including any current funding and no cost extensions), information on the award is required for each PI and co-PI, regardless of whether the support was directly related to the proposal or not. In cases where the PI or co-PI has received *more than one award* (excluding amendments), they need only report on the one award most closely related to the proposal. Funding includes not just salary support, but any funding awarded by NSF. Please refer to the GPG for details about the information that must be provided. Further requirements for this section of the proposal are in the GPG. **Note that these results from prior NSF support must be separately described under two distinct headings, “Intellectual Merit” and “Broader Impacts.” Please address how the proposed research differs from the work conducted under this prior NSF support.**

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 conflicts of interest. The list should 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 for Small and Medium (if applicable) and Large Proposals:

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 and all Large proposals 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 workshops, 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 Large proposal, or 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 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." This supplementary document should describe how the proposal will conform to NSF policy on the dissemination and sharing of research results.

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

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

For specific guidance for Data Management Plans submitted to the Directorate for Computer and Information Science and Engineering (CISE) see: http://www.nsf.gov/cise/cise_dmp.jsp.

For specific guidance for proposals submitted to the Directorate for Social, Behavioral and Economic Sciences (SBE) see: http://www.nsf.gov/sbe/sbe_data_management_plan.jsp.

(4) Topic Areas:

SaTC proposals are grouped into "review panels" of related proposals for peer review and discussion. Panelists are selected for their expertise in the panel topic area. To help SaTC program officers select the most appropriate review panel for your proposal, PIs submitting Small, Medium or Large proposals (but **not** Cybersecurity Education projects) should identify a primary and, optionally, a secondary topic area. The suggested topic areas indicate the areas of panelist expertise that are most important for understanding the innovative aspects of the proposal.

For example, for a proposal that uses hardware to improve the security of wireless networking, the suggested topic areas might be "wireless networking" or "hardware," or both -- with one area as primary and the other as secondary. Choosing which area to recommend as primary would depend on whether the hardware aspect or the wireless networking aspect of the proposal is the more novel.

A supplementary document titled "Topic Areas" should identify a primary (and optionally a secondary) topic area from the following list:

- Access control

- Authentication
- Biometrics
- Cryptography, theory
- Cryptography, applied
- Cyber-physical systems (CPS)
- Data science
- Formal methods
- Hardware
- Intrusion detection
- Mathematics and statistics
- Privacy, theory
- Privacy, applied
- Programming languages
- Social networks
- Social, behavioral and economic science
- Software
- Systems
- Usability
- Wired networking
- Wireless networking

(5) Documentation of collaborative arrangements of significance to the proposal through Letters of Collaboration:

There are two types of collaboration, one involving individuals/organizations that are included in the budget, and the other involving individuals/organizations that are not included in the budget. Collaborations that are included in the budget should be described in the Project Description. Any substantial collaboration with individuals/organizations not included in the budget should be described in the Facilities, Equipment and Other Resources section of the proposal (see GPG Chapter II.C.2.i). In either case, whether or not the collaborator is included in the budget, **a letter of collaboration from each named participating organization *other than the submitting lead, non-lead, and/or subawardee institutions* must be provided at the time of submission of the proposal. Such letters must explicitly state the nature of the collaboration, appear on the organization's letterhead and be signed by the appropriate organizational representative. These letters must not otherwise deviate from the restrictions and requirements set forth in the GPG Chapter II.C.2.j.**

Please note that letters of support may not be submitted. Such letters do not document collaborative arrangements of significance to the project, but primarily convey a sense of enthusiasm for the project and/or highlight the qualifications of the PI or co-PI. **Reviewers will be instructed to ignore these letters of support in reviewing the merits of the proposal.**

(6) Other specialized information:

RUI Proposals: PIs from predominantly undergraduate institutions should include a Research in Undergraduate Institutions (RUI) Impact Statement and Certification of RUI Eligibility in this Section.

GOALI proposals: PIs submitting GOALI proposals should include industry-university agreement letters on intellectual property in this section.

No other Supplementary Documents, except as permitted by the NSF** Grant Proposal Guide**, are allowed.

Single Copy Documents:

Collaborators and Other Affiliations Information: In lieu of the instructions in the GPG, Collaborators and Other Affiliations Information should be submitted as follows. (Note: In collaborative proposals, the lead institution should assemble and provide this information for all participants in the collaborative group):

Provide current, accurate information for all active or recent collaborators of personnel and institutions involved in the project. NSF staff will use this information in the merit review process to manage conflicts of interest. **This list is distinct from (1) above under Supplementary Documents in that it must include all active or recent Collaborators of all personnel involved with the proposed project.** Collaborators include any individual with whom any member of the project team -- including PIs, Co-PIs, Senior Personnel, paid/unpaid Consultants or Collaborators, Subawardees, Postdocs, and project-level advisory committee members -- has collaborated on a project, book, article, report, or paper within the preceding 48 months; or co-edited a journal, compendium, or conference proceedings within the preceding 24 months. This list should be numbered and include (in this order) Full name and Organization(s), with each item separated by a semi-colon. Each person listed should start a new numbered line. The following is a sample format; other similar formats are acceptable.

Collaborators for Mary Smith; XYZ University; PI

1. Helen Gupta; ABC University
2. John Jones; University of PQR
3. Fred Gonzales; DEF Corporation
4. Susan White; DEF Corporation

1. Collaborators for John Jones; University of PQR; Senior Personnel
    1. Tim Green; ZZZ University
    2. Ping Chang; ZZZ University
    3. Mary Smith; XYZ University
2. Collaborators for Jane Brown; XYZ University; Postdoc
    1. Fred Gonzales; DEF Corporation
3. Collaborators for Bob Adams; ABC Community College; Paid Consultant
    1. None
4. Collaborators for Susan White; DEF Corporation; Unpaid Collaborator
    1. Mary Smith; XYZ University
    2. Harry Nguyen; Welldone Institution
5. Collaborators for Tim Green; ZZZ University; Subawardee
    1. John Jones; University of PQR

NOTE: The list of collaborators includes all current and past (within above timelines) projects for all participants in the proposal. It is not a list of the collaborators for the given proposal; this should be provided pursuant to item (1) of Supplementary Documents above.

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. These are a summary of the requirements described above.

For all proposals, regardless of size or designation:

- Must include the Project Personnel and Partner Institutions list as a supplementary document. For collaborative proposals, the lead institution should include a combined list for all project personnel.
- Must include the List of Collaborators as a single copy document. For collaborative proposals, the lead institution should include this list for all project personnel.
- Should include Topic Areas as a supplementary document.
- Letters of Collaboration are permitted as supplementary documents. Letters of Support are not allowed; *reviewers will be instructed not to consider these letters in reviewing the merits of the proposal.*
- The following items are not specific to this solicitation, but are included as reminders, and apply to all NSF proposals unless otherwise noted by the solicitations (see the GPG for further information):
    - Within the Project Description, a section labeled “Broader Impacts of the Proposed Work”;
    - Within the Project Description, a description of Results from Prior NSF Support, including intellectual merit and broader impacts.
    - If the budget includes postdoctoral fellows, a one-page Postdoctoral Mentoring Plan must be included as a supplementary document.
    - A Data Management Plan, not to exceed two pages, must be included.
    - PIs from predominantly undergraduate institutions should include a Research in Undergraduate Institutions (RUI) Impact Statement and Certification of RUI Eligibility.

For Small proposals:

- The title must start with one of the following strings:
    - SaTC: CORE: Small:
    - SaTC: CORE: Small: Collaborative:
    - SaTC: STARSS: Small:
    - SaTC: STARSS: Small: Collaborative:
    - SaTC: TTP: Small:
    - SaTC: TTP: Small: Collaborative:
- In addition to the above title prefixes, proposals from PIs in institutions that have RUI (Research in Undergraduate Institutions) eligibility should include "RUI: " immediately before the proposal title, for example, **SaTC: CORE: Small: RUI: Title**. Similarly, PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **SaTC: CORE: Small: GOALI: Title**.
- Maximum budget shown on the cover page and on the budget sheets must not exceed $500,000, plus funds for embedded REU supplements.
- The Project Description is limited to no more than 15 pages.
- If more than one institution is involved, a collaboration plan (up to 2 pages) **may** be provided as a supplementary document.
- For STARSS-designated proposals, the proposal must also be submitted to NSF as well as the Semiconductor Research Corporation.

For Medium proposals:

- The title must start with one of the following strings:
    - SaTC: CORE: Medium:
    - SaTC: CORE: Medium: Collaborative:
    - SaTC: TTP: Medium:
    - SaTC: TTP: Medium: Collaborative:
- In addition to the above title prefixes, proposals from PIs in institutions that have RUI (Research in Undergraduate Institutions) eligibility should include "RUI: " immediately before the proposal title, for example, **SaTC: CORE: Medium: RUI: Title**. Similarly, PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **SaTC: CORE: Medium: GOALI: Title**.
- Maximum budget shown on the cover page and on the budget sheets must be at least $500,001 and must not exceed $1,200,000, plus funds for embedded REU supplements.
- The Project Description is limited to no more than 15 pages.
- If more than one PI is involved, a collaboration plan (up to 2 pages) **must** be provided as a supplementary document.

For Large proposals:

- The title must start with one of the following strings:
    - SaTC: CORE: Large:
    - SaTC: CORE: Large: Collaborative:
- In addition to the above title prefixes, proposals from PIs in institutions that have RUI (Research in Undergraduate Institutions) eligibility should include "RUI: " immediately before the proposal title, for example, **SaTC: CORE: Large: RUI: Title**. Similarly, PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **SaTC: CORE: Large: GOALI: Title**.
- Maximum budget shown on the cover page and on the budget sheets must be at least $1,200,001 and must not exceed $3,000,000, plus funds for embedded REU supplements.
- The Project Description is limited to no more than 20 pages.
- A collaboration plan (up to 2 pages) **must** be provided as a supplementary document.

For Education proposals:

- The title must start with one of the following strings:
    - SaTC: EDU:
    - SaTC: EDU: Collaborative:
- In addition to the above title prefixes, proposals from PIs in institutions that have RUI (Research in Undergraduate Institutions) eligibility should include "RUI: " immediately before the proposal title, for example, **SaTC: EDU: RUI: Title**. Similarly, PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **SaTC: EDU: GOALI: Title**.
- Maximum budget shown on the cover page and on the budget sheets must not exceed $300,000, plus funds for embedded REU supplements.
- The Project Description is limited to no more than 15 pages.

- If more than one institution is involved, a collaboration plan (up to 2 pages) **may** be provided as a supplementary document. If only one institution is involved, a collaboration plan is **not** permitted.

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. Budgets for Large projects must include funding for one or more project representatives (PI/co-PI/senior researcher or NSF-approved replacement) to attend a SaTC PI meeting to be held every other year for the duration of the project. The first PI meeting for awards made under this solicitation is expected in 2019. These requirements for PI meeting attendance apply to collaborative proposals as a whole, not to each part of a project.

C. Due Dates

- **Submission Window Date(s)** (due by 5 p.m. submitter's local time):

  October 12, 2016 - October 19, 2016

  October 12 - October 19, Annually Thereafter

  LARGE Projects

  October 12, 2016 - October 19, 2016

  October 12 - October 19, Annually Thereafter

  MEDIUM Projects

  November 02, 2016 - November 16, 2016

  November 2 - November 16, Annually Thereafter

  SMALL Projects

  December 01, 2016 - December 15, 2016

  December 1 - December 15, Annually Thereafter

  CYBERSECURITY EDUCATION 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 the GPG as Exhibit III-1.

A comprehensive description of the Foundation's merit review process is available on the NSF website at: http://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 *Investing in Science, Engineering, and Education for the Nation's Future: NSF Strategic Plan for 2014-2018*. 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. (GPG 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 GPG 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 **Large** and relevant **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 (if required) 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 **Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) designation** will be evaluated with careful attention to the following:

- A primary focus on hardware-related problems and approaches, which may include the software-hardware interface, at levels that may range from device to system;
- The risk that the proposed solution has potential to address; and
- The economic and business context in which the proposed solution will be implemented.

Proposals submitted with the **Transitions 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 Technology Transfer Office (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.

For proposals submitted to the STARSS designation, NSF will manage and conduct the review process of proposals submitted in accordance with NSF standards and procedures. The review and award recommendations will be coordinated by a Joint NSF and SRC Working Group (JWG) of program officers from both NSF and SRC. Relevant information about proposals and reviews of proposals will be shared between the participating organizations as appropriate. The JWG will recommend meritorious proposals for award at appropriate funding levels.

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 http://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 *Award & Administration Guide* (AAG) Chapter II, available electronically on the NSF Website at http://www.nsf.gov/publications/pub_summ.jsp?ods_key=aag.

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. For Large 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 a SaTC PI meeting to be held every other year, for the duration of the project. The first PI meeting for awards made under this solicitation is expected in 2019.

For STARSS awards, projects selected for joint funding by NSF and SRC will be funded through separate NSF and SRC funding instruments. For each such project, NSF support will be provided via an NSF grant and SRC support will be provided via an SRC contract. Either organization may supplement a project without requiring the other party to provide any additional funds. As noted above, the budget submitted with the proposal should include all necessary project funds without regard to the two funding organizations; NSF and SRC will inform selected PIs of the breakdown in funding between the two organizations, and will request revised budgets as appropriate. All joint or separate awards involving SRC funds must also include an executed agreement on intellectual property signed by the representatives of the awardee organization and SRC. SRC contracts provide for non-exclusive, royalty-free rights to all SRC members for any intellectual property generated as a result of the SRC-funded research.

For STARSS awards, special award conditions will require that one or more project representatives (PI, co-PI, senior researcher or NSF-approved replacement) must 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 2019. In addition, in years in which no SaTC PI meeting is held, SRC will hold a review of all STARSS projects.

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 *Award & Administration Guide* (AAG) Chapter II, available electronically on the NSF Website at http://www.nsf.gov/publications/pub_summ.jsp?ods_key=aag.

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, 1110, telephone: (703) 292-8910, email: namla@nsf.gov
- Dan Cosley, Program Director, CISE/IIS, 1125, telephone: (703) 292-8491, email: dcosley@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: sgreensp@nsf.gov
- Timothy Hodges, Program Director, MPS/DMS, 1020, telephone: (703) 292-2113, email: thodges@nsf.gov
- Sara Kiesler, Program Director, SBE/SES, 995, telephone: (703) 292-8643, email: skiesler@nsf.gov
- Wenjing Lou, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: wlou@nsf.gov
- Anita Nikolich, Program Director, CISE/ACI, 1145, telephone: (703) 292-8970, email: anikolic@nsf.gov
- Victor P. Piotrowski, Program Director, EHR/DGE, 865, telephone: (703) 292-5141, email: vpiotrow@nsf.gov
- Andrew D. Pollington, Program Director, MPS/DMS, 1025, telephone: (703) 292-4878, email: adpollin@nsf.gov
- Deborah Shands, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: dshands@nsf.gov
- Yan Solihin, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: ysolihin@nsf.gov
- Chengshan Xiao, Program Director, ENG/EECS, ENG/ECCS, 525, telephone: (703) 292-8339, email: cxiao@nsf.gov
- Nan Zhang, Program Director, CISE/IIS, 1125, telephone: (703) 292-8930, email: nanzhang@nsf.gov
- Celia Merzbacher, Semiconductor Research Corporation, telephone: (919) 941-9413, email: celia.merzbacher@src.org

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.

About the Semiconductor Research Corporation:

The Semiconductor Research Corporation (SRC) is a nonprofit industry consortium that invests, often in partnership with government, in basic university research driven by the science and technology needs of its member companies. Awarded the National Medal of Technology, America's highest recognition for contributions to technology, SRC supports research that advances knowledge related to semiconductors and semiconductor-based systems and insures a pipeline of relevantly educated students. Through sustained funding since 1982, SRC has helped create and maintain a robust university research enterprise focused on an industry that is vital to the U.S. economy. For more information, go to https://www.src.org/.

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 http://www.nsf.gov

- **Location:** 4201 Wilson Blvd. Arlington, VA 22230
- **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
Arlington, VA 22230