# Secure and Trustworthy Cyberspace (SaTC)

## PROGRAM SOLICITATION
NSF 15-575

## REPLACES DOCUMENT(S):
NSF 14-599

**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. proposer's local time)**:**

September 10, 2015 - September 16, 2015

September 10 - September 16, Annually Thereafter

MEDIUM Projects

September 18, 2015 - September 24, 2015

September 18 - September 24, Annually Thereafter

LARGE Projects

November 04, 2015 - November 18, 2015

November 4 - November 18, Annually Thereafter

SMALL Projects

December 03, 2015 - December 16, 2015

December 3 - December 16, Annually Thereafter

CYBERSECURITY EDUCATION Projects

## IMPORTANT INFORMATION AND REVISION NOTES

**Revision Summary:** This is a revision of NSF 14-599, the solicitation for the SaTC Program. The revisions include:

1. Revisions to the submission deadline windows;
2. Revisions to the eligibility information for institutions with overseas campuses;
3. Revisions to the SaTC program description, including (a) replacement of the Transition to Practice (TTP) option with a TTP perspective, and (b) clarification of the relationship between Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective proposals and other hardware proposals; and
4. Revisions to the Proposal Preparation Instructions, including (a) a requirement for a section titled "Broader Impacts of the Proposed Work" within the Project Description section of a proposal, (b) clarification of what must be included as part of "Results from Prior NSF Support" within the Project Description section, (c) clarification of what should be submitted as a Letter of Collaboration and/or Commitment in the Supplementary Documents section, (d) the addition of a request to specify topic area(s) in the Supplementary Documents, and (e) the addition of a checklist for each project class to aid in ensuring all required materials are included with a proposal submission.

Any proposal submitted in response to this solicitation should be submitted in accordance with the revised NSF Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 15-1), which is effective for proposals submitted, or due, on or after December 26, 2014. The PAPPG is consistent with, and, implements the new Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (Uniform Guidance) (2 CFR § 200).

## SUMMARY OF PROGRAM REQUIREMENTS

### General Information

**Program Title:**

Secure and Trustworthy Cyberspace (SaTC)

**Synopsis of Program:**

Cyberspace has transformed the daily lives of people for the better. The rush to adopt cyberspace, however, has exposed its fragility and vulnerabilities: corporations, agencies, national infrastructure and individuals have been victims of cyber-attacks. In December 2011, the National Science and Technology Council (NSTC) with the cooperation of NSF issued a broad, coordinated Federal strategic plan for cybersecurity research and development to "change the game," minimize the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. This challenge requires a dedicated approach to research, development, and education that leverages the disciplines of mathematics and statistics, the social sciences, and engineering together with the computing, communications and information sciences.

The Secure and Trustworthy Cyberspace (SaTC) program welcomes proposals that address cybersecurity from:

- a Trustworthy Computing Systems (TWC) perspective and/or a Social, Behavioral and Economic Sciences (SBE) perspective;
- the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective; or
- the Transition to Practice (TTP) perspective.

In addition, we welcome proposals that integrate research addressing all of these perspectives (see the Program Description below). Proposals may be submitted in one of the following three project classes (plus Cybersecurity Education; see below):

- 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; or
- Large projects: $1,200,001 to $3,000,000 in total budget, with durations of up to five years.

For Small hardware security proposals, the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective is focused specifically on hardware research innovation that addresses SaTC goals, and includes the opportunity to collaborate closely with industry. STARSS proposals may **not** include the TWC, SBE, or TTP perspectives. The STARSS perspective may **not** be used for Medium or Large proposals.

The Transition to Practice (TTP) perspective is focused exclusively on transitioning existing research to practice. TTP proposals may **not** include the TWC, SBE, or STARSS perspective. The TTP perspective may be used for Small and Medium proposals, but may **not** be used for Large proposals.

In addition, the SaTC program seeks proposals focusing entirely on Cybersecurity Education with total budgets limited to $300,000 and durations of up to two years. These cybersecurity education projects may **not** include any of the perspectives named above.

**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.*

- Jeremy Epstein, Program Director, CISE/CNS, 1175, telephone: (703) 292-8338, email: jepstein@nsf.gov
- Nina Amla, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: namla@nsf.gov
- Christopher Clifton, Program Director, CISE/IIS, 1125, telephone: (703) 292-8930, email: cclifton@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: sgreensp@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
- Deborah Shands, Program Director, CISE/CNS, 1175, telephone: (703) 292-4505, email: dshands@nsf.gov
- Ralph Wachter, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: rwachter@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
- Chengshan Xiao, Program Director, ENG/EECS, 525, telephone: (703) 292-8339, email: cxiao@nsf.gov
- Heng Xu, Program Director, SBE/SES, 995, telephone: (703) 292-8643, email: hxu@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:** 85

In FY 2016, NSF anticipates approximately 8 Education awards, 51 Small awards, 20 Medium awards and 6 Large awards.

**Anticipated Funding Amount:** $68,300,000

Up to $68,300,000 in FY 2016, subject to the availability of funds and receipt of sufficient meritorious proposals.

## Eligibility Information

**Who May Submit Proposals:**

The categories of proposers eligible to submit proposals to the National Science Foundation are identified in the Grant Proposal Guide, Chapter I, Section E.

**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:** 3

An individual can participate as a PI, co-PI or Senior Personnel on **no more than three proposals, of which no more than two can be for Small, Medium, or Large projects (collectively, the TWC, SBE, STARSS and TTP perspectives), and no more than one can be a Cybersecurity Education project**. (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.)

**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 (e.g., the first two proposals received for the TWC, SBE, STARSS, and/or TTP perspectives will be accepted and the remainder will be returned without review). **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. proposer's local time)**:**

September 10, 2015 - September 16, 2015

September 10 - September 16, Annually Thereafter

MEDIUM Projects

September 18, 2015 - September 24, 2015

September 18 - September 24, Annually Thereafter

LARGE Projects

November 04, 2015 - November 18, 2015

November 4 - November 18, Annually Thereafter

SMALL Projects

December 03, 2015 - December 16, 2015

December 3 - December 16, 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

## I. INTRODUCTION

Cyberspace -- a virtual global village enabled by hyper-connected digital infrastructures -- has transformed the daily lives of people for the better. Families and friends regardless of distance and location can see and talk with one another as if in the same room. Cyber economies create new opportunities. Every sector of society and nearly every discipline has been, and will continue to be, transformed by cyberspace. Today it is no surprise that cyberspace is critical to our national priorities in commerce, education, energy, financial services, healthcare, manufacturing, and defense.

The rapidly increasing importance of cyberspace, however, has exposed its fragility. The risks of hyper-connectedness have become painfully obvious to all. The privacy of personally identifiable information is often violated on a massive scale by unknown persons. Our competitive advantage is eroded by the exfiltration of significant intellectual property. Law enforcement is hobbled by the difficulty of attribution, national boundaries, and uncertain legal and ethical frameworks. All these concerns now affect the public's trust of cyberspace and the ability of institutions to fulfill their missions.

In 2011, the National Science and Technology Council (NSTC) with the cooperation of NSF put forward a strategic plan titled Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program. The plan identifies a broad, coordinated research agenda to make cyberspace secure and trustworthy. Research in cybersecurity must "change the game," minimize the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. The goal is to make cyberspace worthy of the public's trust.

This solicitation is supportive of the NSTC strategic plan for a trustworthy cyberspace. It recognizes that cyberspace will continue to grow and evolve, and that advances in science and engineering will create new "leap-ahead" opportunities expanding cyberspace. It further recognizes that cybersecurity must also grow and co-evolve, and that a secure and trustworthy cyberspace will ensure continued economic growth and future technological innovation.

## II. PROGRAM DESCRIPTION

Cybersecurity is one of the most important challenges confronting society in the information age. No one -- whether government, business, or individual -- is exempt from the ravages of malicious cyber acts upon imperfect technologies. Cybersecurity, broadly defined, concerns the protection of the information infrastructure as well as the protection of the content and discourse space, long the domain of the social, behavioral and economic sciences, the critical infrastructures that made modern society possible, and the Internet of Things (IoT) that will remake these critical infrastructures. Cyberspace is a vast domain for interaction, offering many actors and their agents the ability to affect and influence at scales large and small. Posing cyber conflict solely in terms of classic attackers and defenders does not fully capture the diversity and subtlety of the motivations, incentives, ethics, asymmetries, and strategies of the constituent actors and players in cyberspace. The intelligent adversary, whether human or software, learns, evolves, and co-evolves to exploit, disrupt, and overpower existing protection mechanisms. Addressing this challenge requires a coordinated multi-disciplinary approach, contributing to the body of knowledge about cybersecurity in the respective disciplines, and leading to practical, usable, deployable technologies. It also requires education and outreach activities that are focused on developing the next generation of scientists in computational and data science approaches to cybersecurity.

The Secure and Trustworthy Cyberspace (SaTC) program welcomes proposals that address cybersecurity from:

- a Trustworthy Computing Systems (TWC) perspective and/or a Social, Behavioral and Economic Sciences (SBE) perspective;
- the Secure, Trustworthy, Assured, and Resilient Semiconductors and Systems (STARSS) perspective; or
- the Transition to Practice (TTP) perspective.

Proposals may be submitted in one of the following three project classes (plus Cybersecurity Education; see below):

- 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; or
- Large projects: $1,200,001 to $3,000,000 in total budget, with durations of up to five years.

For Small hardware security proposals, the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective is focused specifically on hardware research innovation that addresses SaTC goals, and includes the opportunity to collaborate closely with industry. STARSS proposals may **not** include the TWC, SBE, or TTP perspectives. The STARSS perspective may **not** be used for Medium or Large proposals.

The Transition to Practice (TTP) perspective is focused exclusively on transitioning existing research to practice. TTP proposals may **not** include the TWC, SBE, or STARSS perspective. The TTP perspective may be used for Small and Medium proposals, but may **not** be used for Large proposals.

In addition, the SaTC program seeks proposals focusing entirely on Cybersecurity Education with total budgets limited to $300,000 and durations of up to two years. These cybersecurity education projects may **not** include any of the perspectives named above.

**PROJECT CLASSES**

With the exception of Cybersecurity Education 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 to the Trustworthy Computing Systems (TWC)**

**and/or the Social, Behavioral, and Economic Sciences (SBE) perspectives; or to the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective; or to the Transition to Practice (TTP) perspective.**

- **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. **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 be submitted to the Trustworthy Computing Systems (TWC) and/or the Social, Behavioral, and Economic Sciences (SBE) perspectives; or to the Transition to Practice (TTP) perspective.**

- **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 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. **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 to the Trustworthy Computing Systems (TWC) and/or the Social, Behavioral, and Economic Sciences (SBE) perspectives.**

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 multidisciplinary. A successful Large project could also be a deep, intensively focused effort on a single cybersecurity problem in a single discipline. We encourage both single perspective and multi-perspective Large proposals.

**PERSPECTIVES**

***Trustworthy Computing Systems (TWC) Perspective***

Proposals addressing cybersecurity with a Trustworthy Computing Systems (TWC) perspective aim to provide the basis for designing, building, and operating a cyberinfrastructure that is resistant and

resilient to attack, and that can be tailored to meet technical and policy security requirements, including both privacy and accountability. The scope of the research program ranges from the theoretical to the experimental, including usability research, which may involve human subjects. Theories, models, cryptography, algorithms, methods, architectures, languages, hardware, software, tools, systems, big data analytics, and evaluation frameworks are all of interest -- particularly that which is transformative, forward-looking, and offers innovative approaches to "change the game" by providing defenders a distinctive advantage. The scope of a proposal should include a clear and concise description of the threat model (e.g., threat actors, supply chain vulnerabilities, or threats to operations) and its relation to the proposed research.

The technical research program is broad and deep. Of particular interest is research addressing how better to design into components and systems desired security and privacy properties, as well as principled techniques for composing security mechanisms. Methods are sought for raising costs to attackers by incorporating diversity, misdirection/confusion, and change or self-adaptation into systems, while preserving system manageability. Approaches and methods for securing cyber-physical systems (CPS) and the Internet of Things (IoT) are also welcome, including, but not limited to, critical infrastructure such as power and water, health care, transportation, financial services, and manufacturing. Submissions relating to CPS should be specific about the threat model, in particular addressing the sophistication, intelligence, and resources of expected adversaries.

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. Also, methods to assess, reason about, and predict system trustworthiness, including observable metrics, analytical methods, simulation, experimental deployment and, where possible, deployment on live testbeds for experimentation at scale are considered. Statistical, mathematical, and computational methods in the area of cryptographic methods, new algorithms, risk assessments and statistical methods in cybersecurity are also welcome. In addition, research in the mathematics and statistics of security is welcome, particularly non-traditional constructive approaches for efficient hiding of digital information such as, e.g., building on arithmetic geometry or making encryption schemes resistant to both classical and quantum attacks.

***Social, Behavioral and Economic Sciences (SBE) Perspective***

Proposals addressing the Social, Behavioral and Economic Sciences (SBE) perspective of cybersecurity may include research at the individual, group, organizational, market, and societal levels, identifying cybersecurity risks and exploring the feasibility of potential solutions. All research approaches, including (but not limited to) theoretical, experimental, observational, statistical, survey, and simulation-based are of interest. A variety of methods can be used in research from the SBE perspective, including field data, laboratory experiments, observational studies, simulations, and theoretical development, among others.

Not all proposals that examine aspects involving people are from the SBE perspective. Proposals in which such aspects are not the primary focus of the proposal or that merely apply rather than make contributions to the SBE sciences might fit under "Trustworthy Computing Systems" as human factors research.

A proposal with SBE as its *primary* perspective must have SBE science as its main focus and must involve theoretical or methodological contributions to the SBE sciences. Contributions to the SBE sciences include identifying generalizable theories and regularities and "pushing the boundaries" of our understanding of social, behavioral, or economic phenomena in cybersecurity and beyond. We seek research that is generalizable, identifies scope conditions, or provides an advance in SBE science methods. We seek research that holds the promise of constructing new SBE theories that would apply to a variety of domains, or new generalizations of existing theory which clarify the conditions under which such generalizations hold (scope conditions). More inductive or interpretative approaches may contribute to the SBE sciences as well, especially if they set the groundwork for generalizable research or reveal broad connections that forward SBE science understandings. SBE / SaTC proposals should clearly state and elaborate how the proposed research will contribute to SBE sciences. A proposal that involves SBE, *but not as its primary perspective*, must include at least an application of the SBE sciences, but need not involve a theoretical or methodological contribution.

All SBE primary or non-primary proposals must, like all SaTC proposals, also contribute toward the goal of creating a secure and trustworthy cyberspace. The SBE science contribution of any SBE / SaTC proposal must be related to bringing about that goal. It is not sufficient for a proposal submitted under

SBE / SaTC to have an SBE science contribution alone or one that is not related to bringing about a secure and trustworthy cyberspace. Such proposals are perhaps best submitted to a standing (core) SBE program.

Strong proposals will demonstrate the capabilities of the research team to bring to bear state-of-the-art research in the human sciences. In particular, they will seek to understand, predict and explain prevention, attack and/or defense behaviors and contribute to developing strategies for remediation. Proposals that contribute to the design of incentives, markets or institutions to reduce either the likelihood of cyber attack or the negative consequences of cyber attack are especially welcome, as are proposals that examine incentives and motivations of individuals.

Proposals submitted with a Social, Behavioral & Economic Sciences perspective will be evaluated with careful attention to the following:

- The mutual application of, and contribution to, basic social, behavioral and economic sciences research;
- The generalizability of the research to multiple cyber security settings;
- The ultimate contribution to the construction of institutions that induce optimal behavior; and
- The value of the research toward creating a secure and trustworthy cyberspace.

Given the nascent state of SBE research in cybersecurity, we welcome proposals for workshops and other opportunities for intellectual engagements. Such proposals, however, should clarify how the efforts are likely to enable future SBE contributions, preferably from a range of social, behavioral and economic sciences. Infrastructure-oriented proposals should include components that go beyond merely providing a resource for other researchers and should contribute directly to research. PIs are encouraged to contact SBE program officers if interested in submitting such proposals.

***Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) Perspective***

The STARSS perspective 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 TWC and/or SBE perspective except that it must include a statement of consent authorizing NSF to share the proposal and any reviews and ancillary documents with SRC. As noted previously, STARSS proposals may **not** include the TWC, SBE, or TTP perspectives.

*Please note:* Small research proposals targeting hardware may be submitted either as TWC or STARSS perspectives. The STARSS perspective provides an opportunity for close collaboration with industry through SRC, for topics within scope. Hardware security proposals not specifically addressing STARSS criteria should be submitted to the TWC perspective. In addition, 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."

Trends in semiconductors and their application pose challenges to security and trustworthiness. On one hand, leading edge processors are the “brains” behind critically-important systems and infrastructure, including networking and communications, electric power grids, finance, military and aerospace systems. On the other hand, smaller embedded processors, sensors and other electronic components provide “smart” functionality and connectivity in a variety of applications, such as automotive braking and airbag systems, personal healthcare, industrial controls, and the rapidly growing list of other connected devices often referred to as the Internet of Things. The wide range of devices and applications and the exponential growth in the number of connected “things” has made security and trustworthiness a prime concern.

Design and manufacture of today’s complex semiconductor circuits and systems requires many steps and involves the work of hundreds of engineers, typically distributed across multiple locations and organizations worldwide. Moreover, today’s semiconductor chip is likely to include design modules or blocks (also referred to as intellectual property, or IP, blocks) from multiple sources. Detailed specifications are converted into schematic and then physical designs that may include billions of transistors. Many processes have been developed, and considerable resources are invested along the design and manufacture path to verify, test and validate that the product performs as intended.

However, to date, these processes do not provide confidence about whether the chip is altered such that it provides unauthorized access or control. Such undesirable behavior can be due to a weakness in the design that results in an unintentional side channel or due to maliciously inserted functionality or "Trojan" hardware.

Today, semiconductor circuits and systems are designed so as to make it feasible or easier to verify, manufacture and test during subsequent steps. What is needed is an understanding of Design for Assurance, with the objective of decreasing the likelihood of unintended behavior or access, increasing resistance and resilience to tampering and counterfeiting, and improving the ability to provide authentication in the field. Design for Assurance requires new strategies for architecture and specification, and tools for synthesis, physical design, test, and verification, especially at the stages of design in which formal methods are currently weak or absent. Methods and procedures targeting the early stages of design are likely to be more effective and affordable.

It is imperative to develop a theoretical basis for hardware security in order to design systems that are free of vulnerability and that are assured and resilient against attacks, even vulnerabilities and attacks that are not (yet) known. Ideally, such a mathematical model would abstract the environment of threats and responses and formalize precisely engineering concepts of system security, such as closeness, safeness, vulnerability, attack, etc. Metrics for assessing system security and quantify assurance could be developed from such a formal model. Existing and new automation and design tools may use the abstraction and metrics to specify security primitives as numeric attributes and allow trade-off with other design primitives of the system under design.

A successful Design for Assurance solution needs to be integrated with other design features and considerations, taking into account competing demands from system designers and manufacturers. For example, as system complexity grows, the demand for greater observability and controllability during manufacture and in the post manufacturing and integration environments leads to increased risk of side channel attack. Designing capabilities that allow for on-line self-test, recovery, adaptation or reconfiguration also increases the risk of side channel attack. The risks associated with these design and manufacturing techniques need to be carefully studied and mitigated or neutralized.

Threats and challenges to assurance include, but are not limited to, those listed below.

- Unwanted functionality in specification, design or implementation at the behavioral, register-transfer level (RTL), logical or physical level. Unwanted functionality may be malicious or inadvertent. This includes incomplete and ambiguous specifications or implementations.
- Dependencies at interfaces that lead to leakage of sensitive information or weakness to attack. This includes time-dependent behavior or improper reliance of timeouts on external signals.
- Counterfeiting of semiconductor-based parts/products.
- Unauthorized access to sensitive data or control functions. This includes access to keys or sensitive internal data.
- Maliciously inserted hardware Trojans and other forms of tampering with a design at any stage of the design cycle, including during manufacturing.
- Tampering with an electronic circuit while in operation, e.g., via a side channel.
- Identification of poor resistance to tampering, whether at a functional, logical or electrical level. In particular, resistance to known tampering methods, such as power, thermal or irradiation attacks.
- Hardware authentication and fingerprinting.
- Provenance of circuitry, including verification and tracking of IP blocks and of lack of tampering.
- Dependence on external components that are not verifiable and hence vulnerable to attack.
- A formal and quantifiable specification of security and/or baselines that enable integrity checking at run time.

**With this solicitation, NSF and SRC seek to support research on Secured, Assured and Resilient Semiconductors and Systems (STARSS), with a focus on Design for Assurance. 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 & Design:** Architectural and design approaches, models and frameworks for both reasoning about, as well as specifying, hardware-specific security properties for first-order security architecture elements as well as second and third-order functionality -- i.e., ensuring that the security-specific IP block is not only secure, but that there are no security-related

vulnerabilities resulting from side effects related to any other IP blocks or semiconductor pervasive logic. Novel, security-aware and security-driven design or specification languages. Approaches for design with configurable IP blocks that go beyond establishing the initial Trusted Computing Base (TCB) to maintaining TCB assurance through the platform lifetime. Components with such properties are critical for the next generation of applications, including heterogeneous, interconnected systems. 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.

- **Properties, Principles & Metrics:** Going beyond high-level security properties such as confidentiality, integrity and availability of security-sensitive assets and access mechanisms to derive a set of hardware security design principles and semiconductor-specific properties, along with the development of a knowledge base of concrete examples, scenarios, and other empirical evidence. Ultimately, it is desirable to have not only principles, but also metrics that provide a measure of the security of a particular design. Security metrics should be extensible and potentially useful for privacy composition or to provide trust evidence at the system level.
- **Security Verification & Analysis:** Tools, techniques, and methodologies for verifying hardware-specific security properties and enforcing the security design principles described above. Innovative approaches to establish important safety properties without knowing all aspects of the design, and thereby providing strong provable assurance. The tools and techniques should ensure coverage and equivalency between various design, implementation, integration, and manufacturing phases and can be extensions and/or enhancements to existing tools and methodologies, intersecting existing design and verification process flows, as well as regression and other testing methodologies. Decomposition of systems with an explicit performance (including side channels) model and re-composition to assure safety properties are maintained are examples of useful approaches. An analogy from software development is Control Flow Integrity (CFI) techniques that modify software to ensure conformance to some clear properties without knowing all the program details and without the ability to influence the design from the start. Approaches in hardware could include explicit side channel contracts (on power and timing), and novel techniques that discover and analyze “unexpected” behavior.
- **Tools & Frameworks:** In order to utilize the Design for Assurance techniques that emerge, there is need for the semiconductor design and manufacturing equivalent of leading software security engineering models, such as Microsoft’s Security Development Lifecycle, IBM’s Secure Engineering Framework, and the Building Security In Maturity Model (BSIMM). Such a semiconductor security development model would be targeted at guiding the semiconductor workforce of today as well as of tomorrow -- e.g., academic and industrial curricula targeted at instructing architects, designers, and engineers, responding to vulnerabilities (internally and externally discovered), measuring organizational maturity and product/IP block assurance over time, etc. (Note that development of such models will likely be best facilitated by providing researchers access to current industry processes.)
- **Authentication & Attestation:** Models are needed for the insertion of artifacts and/or design elements that are verifiable during design and implementation, but also during manufacture and finally support in-field dynamic verification and non-destructive authentication, with the latter establishing a basis for dynamic/on-demand supply chain assurance at the component level. This research would focus on a semiconductor provenance model and related design artifacts, including but not limited to hardware fingerprinting and third party design element model checking. Supporting issues, such as the generation, protection and establishment of trust models for hardware-implemented keys, are also of interest.

In addition to these research topics, there is a need to identify, classify, analyze and share information about hardware security threats, which are constantly evolving, in support of research and development broadly. Abstract models of attacks based on formality of system security would also be useful.

Of particular interest are strategies for designing hardware that is less likely to include vulnerabilities, either inadvertent or intentional. Approaches implemented in earlier phases of the design, manufacture and product lifecycle are likely to have the greatest impact.

Ultimately, concepts addressing the research areas described above must be practical and capable of being implemented in a cost-effective manner. The effectiveness and applicability of any of the strategies and techniques being solicited depend on the business and economic environment in which they operate. Taking economic and business constraints into consideration is likely to add strength to any resulting technology innovation.

***Transition to Practice (TTP) Perspective***

The objective of the Transition to Practice (TTP) perspective is to support the development, implementation, and deployment of applied security research into an operational environment. The operational environment may be a single campus, multiple campuses, NSF-funded cyberinfrastructure, or a government agency. A TTP perspective 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.

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

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

- Identification of a target user group or organization that will serve as an early adopter of the technology;
- 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 but also skills in project management and systems development;
- 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 indicating its willingness to support the proposal is strongly encouraged).

Software developed in this program is not required to be open sourced. However, if open sourced 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.

*Please note:* TTP perspective proposals count as one of the two proposals that may be submitted to the SaTC program for the Small, Medium, and Large project classes (although TTP perspective proposals may only be submitted to the Small or Medium project classes). A PI can submit both a basic research proposal as well as a TTP perspective proposal in the same year.

Questions regarding the Transition to Practice (TTP) perspective should be addressed directly to SaTC Program Officer Anita Nikolich in the Division of Advanced Cyberinfrastructure (ACI) at anikolic@nsf.gov.

***Cybersecurity Education Proposals***

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 perspective leverage successful results from previous and current basic research in cybersecurity and research on student learning, both in terms of intellectual merit and broader impact, 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 student 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 the teaching and student learning in cybersecurity.

Any software developed in this program area is required to be released under an open source license listed by the Open Source Initiative (http://www.opensource.org/).

Cybersecurity Education proposal budgets are limited to $300,000 and their durations are limited to two years. Cybersecurity Education proposals may **not** include any of the other perspectives.

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 aims to further and expand its research community. In this spirit, the program plans to host PI meetings every other year with participation from all funded projects and other representatives from the research community, government and industry. Principal investigators from all perspectives 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 perspective 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 2016, NSF anticipates approximately 8 Education awards, 51 Small awards, 20 Medium awards and 6 Large awards totaling up to $68,300,000, subject to the availability of funds and receipt of sufficient meritorious proposals.

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:**

The categories of proposers eligible to submit proposals to the National Science Foundation are identified in the Grant Proposal Guide, Chapter I, Section E.

**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:** 3

An individual can participate as a PI, co-PI or Senior Personnel on **no more than three proposals, of which no more than two can be for Small, Medium, or Large projects (collectively, the TWC, SBE, STARSS and TTP perspectives), and no more than one can be a Cybersecurity Education project**. (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).

**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 (e.g., the first two proposals received for the TWC, SBE, STARSS, and/or TTP perspectives will be accepted and the remainder will be returned without review). **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 U.S. campus(es) only.

## 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 perspective(s).***

**Proposal Titles:**

Proposal titles must begin with an acronym that indicates the most relevant perspective. Select an acronym from the following list:

- Trustworthy Computing Systems perspective: **TWC**;
- Social, Behavioral and Economic Science perspective: **SBE**;
- Secure, Trustworthy, Assured and Resilient Semiconductors and Systems perspective: **STARSS**;
- Transition to Practice perspective: **TTP**; and
- Cybersecurity Education project: **EDU**.

The TWC and SBE acronyms may be used together, separated by spaces, but no other combinations are permitted. The first acronym should indicate the primary focus of the proposal. The acronym(s) should be followed by a colon, then the project class (Small, Medium or Large) followed by a colon, then the title of the proposed project. For example, if you are submitting a Small proposal to the Trustworthy Computing Systems perspective, the title of your proposal would be **TWC: Small: Title**. If you are submitting a Small proposal to the Trustworthy Computing Systems and the Social Behavioral and Economic Sciences perspectives, the title of your proposal would be **TWC SBE: 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 perspectives 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 Trustworthy Computing Systems (TWC) perspective, the title of each proposal would be **TWC: Medium: Collaborative: Title**.

STARSS proposals must be in the Small project class. They may not include any other perspectives besides STARSS. Therefore, valid STARSS-specific title styles are:

**STARSS: Small: Title**
**STARSS: Small: Collaborative: Title**

TTP proposals must be in the Small or Medium project classes. They may not include any other perspectives besides TTP. Therefore, valid TTP-specific title styles are:

**TTP: Small: Title**
**TTP: Small: Collaborative: Title**
**TTP: Medium: Title**
**TTP: Medium: Collaborative: Title**

The titles of Cybersecurity Education proposals must contain a single acronym: EDU. They may **not** include a project class or any other perspective. Thus, the only valid EDU-specific title styles are:

**EDU: Title**
**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, **TWC: Medium: RUI: Title**.

PIs submitting Grant Opportunities for Academic Liaison with Industry (GOALI) proposals should include "GOALI: " immediately before the proposal title, for example, **TWC SBE: 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 of the Proposed Work."** This section should provide a discussion of the broader impacts of the proposed activities.
- **Results from Prior NSF Support: If any PI or co-PI identified on the project has received NSF funding (including any current funding) in the past five years, the Project Description must contain information on the award(s), irrespective 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. **Note that these results from prior NSF support must be separately described under two distinct headings, "Intellectual Merit" and "Broader Impacts."**

**Proposals without these two distinct sections (including the heading "Broader Impacts of the Proposed Work") within the Project Description may be returned without review.**

**Supplementary Documents:**

In the Supplementary Documents Section, upload the following:

*(1) For Small projects with STARSS perspectives only, proposals must include a statement of consent that indicates NSF may share with SRC the proposal, reviews, and any related information.* ***STARSS perspective proposals that do not contain this statement will be returned without review.***

*(2) 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

*(3) A list of past and present Collaborators not related to this proposal (Note: In collaborative proposals, the lead institution should provide this information for all participants):*

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 -- distinct from (2) above -- 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 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.

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

**NOTE: The list of collaborators includes all current and past (see 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 (2) of Supplementary Documents above.**

*(4) Collaboration Plans for 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.

*(5) 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, see: http://www.nsf.gov/bfa/dias/policy/dmp.jsp.

For specific guidance for proposals 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.

***Proposals that include Data Management Plans exceeding two pages in length will be returned without review.***

*(6) 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 most novel.

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

- Access control
- Anti-censorship
- Authentication
- Biometrics
- Cloud
- Cryptography, theory
- Cryptography, applied
- Cyber-physical systems (CPS)
- Data science
- Formal methods
- Hardware
- Internet of Things (IoT)
- Intrusion detection
- Location privacy
- Privacy, theory
- Privacy, applied
- Social networks

- Social science
- Software
- Systems
- Trust
- Usability
- Wired networking
- Wireless networking

*(7) Documentation of collaborative arrangements of significance to the proposal through Letters of Collaboration and/or Commitment:*

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 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.**

**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 not to consider these letters of support in reviewing the merits of the proposal.**

*(8) 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.***

**Allowed Combinations of Perspectives and Option:**

Not all combinations of perspectives are allowed. The following table is a synopsis of the above.

| Size | Single Perspectives Allowed | Double Perspectives Allowed | Base Max | Project Description Page Limit | Collaboration Plan |
|---|---|---|---|---|---|
| Education | EDU | None | $300K | 15 | Permitted but not required |
| Small | TWC<br>SBE<br>STARSS<br>TTP | TWC SBE or<br>SBE TWC | $500K | 15 | Permitted but not required |
| Medium | TWC<br>SBE<br>TTP | TWC SBE or<br>SBE TWC | $1.2M | 15 | Required for proposals with > 1 PI |

| | | | | | |
|---|---|---|---|---|---|
| Large | TWC<br>SBE | TWC SBE or<br>SBE TWC | $3M | 20 | Required |

**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 perspective:*

- 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 supplementary document. For collaborative proposals, the lead institution should include this list for all project personnel.
- Must include Topic Areas as a supplementary document.
- Letters of Collaboration and/or Commitment 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 Grant Proposal Guide 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 must 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:
  - TWC: Small:
  - TWC: Small: Collaborative:
  - SBE: Small:
  - SBE: Small: Collaborative:
  - TWC SBE: Small:
  - TWC SBE: Small: Collaborative:
  - SBE TWC: Small:
  - SBE TWC: Small: Collaborative:
  - STARSS: Small:
  - STARSS: Small: Collaborative:
  - TTP: Small:
  - 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, **TWC: 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, **TWC SBE: 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 perspective proposals, a letter authorizing NSF to share the proposal and reviews with Semiconductor Research Corporation must be included as a supplementary document.

*For Medium proposals:*

- The title must start with one of the following strings:
  - TWC: Medium:
  - TWC: Medium: Collaborative:
  - SBE: Medium:
  - SBE: Medium: Collaborative:
  - TWC SBE: Medium:
  - TWC SBE: Medium: Collaborative:
  - SBE TWC: Medium:
  - SBE TWC: Medium: Collaborative:
  - TTP: Medium:
  - 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, **TWC: 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, **TWC SBE: 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:
  - TWC: Large:
  - TWC: Large: Collaborative:
  - SBE: Large:
  - SBE: Large: Collaborative:
  - TWC SBE: Large:
  - TWC SBE: Large: Collaborative:
  - SBE TWC: Large:
  - SBE TWC: 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, **TWC: 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, **TWC SBE: 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:
  - EDU:
  - 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, **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, **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 2017. 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. proposer's local time)**:**

  September 10, 2015 - September 16, 2015

  September 10 - September 16, Annually Thereafter

  September 18, 2015 - September 24, 2015

  September 18 - September 24, Annually Thereafter

  LARGE Projects

  November 04, 2015 - November 18, 2015

  November 4 - November 18, Annually Thereafter

  SMALL Projects

  December 03, 2015 - December 16, 2015

  December 3 - December 16, 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://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**

Proposals may be submitted with one or both of the following perspectives: TWC and/or SBE; or with the STARSS perspective (Small proposals only); or with the TTP perspective (Small and Medium proposals only).

Proposals submitted with a **Social, Behavioral and Economic Sciences (SBE) perspective** will be evaluated with careful attention to the following:

- The mutual application of, and contribution to, basic social, behavioral and economic sciences research;
- The generalizability of the research to multiple cyber security settings;
- The ultimate contribution to the construction of institutions that induce optimal behavior; and
- The value of the research toward creating a secure and trustworthy cyberspace.

Proposals submitted with the **Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective** 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) perspective** 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 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 perspective, 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 2017.

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 2017. 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 at least 90 days prior to the end of the current budget period. (Some programs or awards require submission of more frequent project reports). Within 90 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:

- Jeremy Epstein, Program Director, CISE/CNS, 1175, telephone: (703) 292-8338, email: jepstein@nsf.gov
- Nina Amla, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: namla@nsf.gov
- Christopher Clifton, Program Director, CISE/IIS, 1125, telephone: (703) 292-8930, email: cclifton@nsf.gov
- Sol Greenspan, Program Director, CISE/CCF, 1115, telephone: (703) 292-8910, email: sgreensp@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
- Deborah Shands, Program Director, CISE/CNS, 1175, telephone: (703) 292-4505, email: dshands@nsf.gov
- Ralph Wachter, Program Director, CISE/CNS, 1175, telephone: (703) 292-8950, email: rwachter@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
- Chengshan Xiao, Program Director, ENG/EECS, 525, telephone: (703) 292-8339, email: cxiao@nsf.gov
- Heng Xu, Program Director, SBE/SES, 995, telephone: (703) 292-8643, email: hxu@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 at https://public.govdelivery.com/accounts/USNSF/subscriber/new?topic_id=USNSF_179.

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