Trusted Computing (TC)

Program Announcement

NSF-01-160

DIRECTORATE FOR COMPUTER AND INFORMATION SCIENCE AND ENGINEERING
DIVISION OF COMPUTER-COMMUNICATIONS RESEARCH

FULL PROPOSAL DEADLINE(S) :

December 5, 2001; and first Wednesday of December annually thereafter.

NATIONAL SCIENCE FOUNDATION

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 Web Site 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:	pubs@nsf.gov
or telephone:	(301) 947-2722
• **To Locate NSF Employees:**	(703) 292-5111

SUMMARY OF PROGRAM REQUIREMENTS

GENERAL INFORMATION

Program Title: Trusted Computing (TC)

Synopsis of Program: The Trusted Computing program seeks to establish a sound scientific foundation and technological basis for managing privacy and security in a world linked through computing and communication technology. This research is necessary to build the secure and reliable systems required for today's and tomorrow's highly interconnected, information technology enabled society. The program funds innovative research in all aspects of secure, reliable information systems, including methods for assessing the trustworthiness of systems.

Cognizant Program Officer(s):

- Dr. Carl Landwehr, Trusted Computing, Program Director, CISE, C-CR, 1145, telephone: 703-292-8936, e-mail: clandweh@nsf.gov
- Ms. Carmen Whitson, Associate Program Director, CISE, C-CR, 1145, telephone: 703-292-8910, e-mail: vswales@nsf.gov .

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

- 47.070 --- Computer and Information Science and Engineering

ELIGIBILITY INFORMATION

- **Organization Limit:** None
- **PI Eligibility Limit:** None
- **Limit on Number of Proposals:** None

AWARD INFORMATION

- **Anticipated Type of Award:** Standard or Continuing Grant
- **Estimated Number of Awards:** 20-25
- **Anticipated Funding Amount:** Subject to the availability of funds, the anticipated funding for FY 2002 will be between $4Million - $6Million. Subject to availability of funds, it is anticipated that future year funding will be approximately the same.

PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

- **Full Proposals:** Supplemental Preparation Guidelines
    - The program announcement/solicitation contains supplements to the standard Grant Proposal Guide (GPG) proposal preparation guidelines. Please see the full program announcement/solicitation for further information.

B. Budgetary Information

- **Cost Sharing Requirements:** Cost Sharing is not required.
- **Indirect Cost (F&A) Limitations:** Not Applicable.
- **Other Budgetary Limitations:** Not Applicable.

C. Deadline/Target Dates

- **Letters of Intent (*optional*):** None
- **Preliminary Proposals (*optional*):** None
- **Full Proposal Deadline Date(s):**

December 5, 2001; and first Wednesday of December annually thereafter.

D. FastLane Requirements

- **FastLane Submission:** Required
- **FastLane Contact(s):**
    - Ms. Sharon Glivens, Program & Technical Specialist, CISE, C-CR, 1145, telephone: 703-292-8910, e-mail: sglivens@nsf.gov.

PROPOSAL REVIEW INFORMATION

- **Merit Review Criteria:** National Science Board approved criteria apply.

AWARD ADMINISTRATION INFORMATION

- **Award Conditions:** Standard NSF award conditions apply.
- **Reporting Requirements:** Standard NSF reporting requirements apply.

I. INTRODUCTION

As computer systems and computer networks are increasingly used to create, store, process, and transmit information that is critical to citizens, industry, government, and academia, the design and development of secure, safe software and systems has become a fundamental problem. Protection of hardware and software infrastructures is critical to the privacy of citizens, the safety of transportation systems, the financial health of business organizations, stability of the global economy, and national security. Continuing attacks on the Internet and e-Commerce web sites reveal that the software and information base employed by industry is highly vulnerable not only to security penetration, but also to denial of service attacks. Even individuals with relatively unsophisticated technical backgrounds and few resources beyond a personal computer and Internet connection have mounted successful large-scale attacks. Privacy of individuals is compromised through inappropriate access to information. The case is similar for safety. We are relinquishing control to rapidly increasing automation in our homes, automobiles, and environments. The safety consequences of failure range from inconvenient to life-threatening. We consider the qualities, such as security, privacy, safety, and reliability as aspects of the desideratum of trustworthiness of information systems.

While trustworthiness is a system property, today's large and complex systems are increasingly patched together from a variety of components, new and old. The economics of software development in today's marketplace dictate that few of these components will have been subjected to the kind of rigorous development techniques or test and verification disciplines that would support strong statements about their ability to meet a specific set of requirements or enforce a specific security, privacy, or safety policy.

Although security research has been ongoing for many years, new risks also continually present themselves due to the mounting level of connectivity enabled by the Internet and mobile code technologies. The nature of the challenge has changed from one primarily of concern to National Security professionals. As documented in studies such as Trust in Cyberspace (National Academy of Science, 1999), it is now an everyday problem that compromises the security and privacy, physical safety, and economic well-being of individual citizens as well as the information security of government and industry. Change and innovation in networking and communication technologies continue to produce the many benefits of interconnection. As this occurs, the specific security and privacy challenges also change. Research is required to build a scientific basis for the ongoing effort to keep systems safe and secure. This program in Trusted Computing seeks science and technology research to provide trustworthiness and information security on a National scale. The goal of the Trusted Computing program is to create and sustain the science and technology needed to discover, develop, and deploy strong security measures and tools. It must educate a new generation of researchers and specialists to meet the exploding demand for a skilled workforce in this field.

II. PROGRAM DESCRIPTION

The Trusted Computing program seeks to make systems trustworthy. Making large scale information systems robust and able to tolerate security breaches and hostile attacks without failing requires research on a number of issues, such as correctness, availability, reliability, authentication, access control, privacy and confidentiality. These dependent dimensions have broader implications for the overall trustworthiness of the system. Trustworthiness is holistic and multidimensional. For example, the means for achieving security interact with those for performance, reliability, and safety. The challenges in building trustworthy systems are much broader and deeper than those in enforcing security alone. However, security research needs must be understood within this context.

Research in this area confronts a range of difficult questions. The following are examples of current problems: How should protection mechanisms span the concerns of computer, communication, and storage? Where should the mechanisms be placed: applications, middleware, operating systems, or communications infrastructure? How can trustworthiness be achieved for large-scale, highly complex systems spanning multiple organizations? How can secure ubiquitous computing be provided that accommodates extremely small mobile devices, dynamic and ad hoc communications, mobile code, embedded computing, and electronic commerce applications? How can usability be improved, reducing the risks and consequences of human error? How can systems be made robust in the face of environmental disruption, attacks, and instability due to rapid growth? What are the interactions of privacy and security with other required system properties such as fault tolerance and safety? Can security be characterized as one aspect of a quality-of-service framework? How can end-to-end assurance be provided? What are the implications of current and emerging component technologies for traditional concerns: correctness, availability, reliability, authentication, cryptography, secure protocols, access control (both traditional and policy-based), and privacy and confidentiality?

Some specific areas in which research is needed include:

- Component technologies: what specification, design, development, test, verification methods can provide quantifiable assurance that specified properties are met? Ideally, such technologies should be flexible, so that they can be applied in accordance with the degree of trustworthiness required and the resources available. Methods are needed to identify particular components that provide a good basis on which to construct trustworthy systems.

- Composition (and decomposition) methods: how can components be assembled into subsystems and systems with known and quantifiable trustworthiness? Are there methods for identifying and minimizing the security assumptions made in a given security design? How can the existence of large numbers of untrustworthy computing platforms be exploited effectively to create secure or trustworthy multiparty computations?

- Methods for maintaining trustworthiness as systems adapt and evolve.

- Methods for improving human understanding of critical system behavior and control: How can system trustworthiness be visualized, particularly for operators of critical systems, including those that are geographically distributed? How can system security mechanisms be designed that are effective yet unobtrusive?

- Methods for assessing tradeoffs in trustworthy system design, for example between security and performance.

- Techniques for modeling, analyzing, and predicting trust properties of systems and components.

The list above is representative, not exhaustive. Expanding security research in scale and scope is essential to ensuring that large scale information systems of the future are trustworthy. The Trusted Computing program seeks to provide a scientific base and engineering expertise for the development of new paradigms for an integrated and comprehensive solution to the multifaceted problem of trustworthiness. It is a necessity to ensure that future information systems not only behave as expected, but, more importantly, continue to produce expected behavior and are not susceptible to subversion.

III. ELIGIBILITY INFORMATION

The categories of proposers identified in the Grant Proposal Guide are eligible to submit proposals under this program announcement/solicitation. Proposals may be submitted by universities in support of individual investigators or small groups. Synergistic collaboration among researchers and collaboration or partnerships with industry or government laboratories are encouraged when appropriate. Group and collaborative proposals may involve more than one institution.

IV. AWARD INFORMATION

Approximately 20-25 awards are expected, with a duration of 2-5 years. Expected award amounts range from $80,000-150,000 per year for single- and two-investigator proposals and $100,000-500,000 per year for collaborative and multi-investigator proposals. Subject to the availability of funds, the anticipated funding for FY 2002 will be at least $4 Million and up to $6 Million. Subject to availability of funds, it is anticipated that for future year competitions funding will be approximately the same. Number of awards and average award size and duration are also subject to the availability of funds.

V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

Full Proposal:

Proposals submitted in response to this program announcement/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 Web Site at: http://www.nsf.gov/cgi-bin/getpub?gpg. Paper copies of the GPG may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from pubs@nsf.gov.

When group and collaborative proposals are submitted by more than one institution, each of the collaborative proposals must contain identical technical content and the budget only for the participating institution. The titles must also be identical and must begin with the prefix "Collaborative Research:". Each proposal must identify all participating institutions. Group and collaborative proposals may also also be submitted as a single administrative package from one of the institutions involved.

Due to the limited availability of funds, prospective applicants are urged to contact one of the Program Officers listed at the end of this document for guidance.

Proposers are reminded to identify the program solicitation number (NSF-01-160) in the program announcement/solicitation block on the proposal Cover Sheet (NSF Form 1207). Compliance with this requirement is critical to determining the relevant proposal processing guidelines. Failure to submit this information may delay processing.

B. Budgetary Information

Cost sharing is not required in proposals submitted under this Program Announcement.

C. Deadline/Target Dates

Proposals must be submitted by the following date(s):

Full Proposals *by 5:00 PM local time*:

December 5, 2001; and first Wednesday of December annually thereafter.

D. FastLane Requirements

Proposers are required to prepare and submit all proposals for this Program Announcement through the FastLane system. Detailed instructions for proposal preparation and submission via FastLane are available at: http://www.fastlane.nsf.gov/a1/newstan.htm. For FastLane user support, call 1-800-673-6188 or e-mail fastlane@nsf.gov.

Submission of Signed Cover Sheets. The Authorized Organizational Representative (AOR) must electronically sign the proposal Cover Sheet to submit the required proposal certifications (see Chapter II, Section C of the Grant Proposal Guide for a listing of the certifications). The AOR must provide the required certifications within five working days following the electronic submission of the proposal. Further instructions regarding this process are available on the FastLane website at: http://www.fastlane.nsf.gov.

VI. PROPOSAL REVIEW INFORMATION

A. NSF Proposal Review Process

Reviews of proposals submitted to NSF are solicited from peers with expertise in the substantive area of the proposed research or education project. These reviewers are selected by Program Officers charged with the oversight of the review process. NSF invites the proposer to suggest at the time of submission, the names of appropriate or inappropriate reviewers. Care is taken to ensure that reviewers have no conflicts with the proposer. Special efforts are made to recruit reviewers from non-academic institutions, minority-serving institutions, or adjacent disciplines to that principally addressed in the proposal.

Proposals will be reviewed against the following general review criteria established by the National Science Board. Following each criterion are potential considerations that the reviewer may employ in the evaluation. These are suggestions and not all will apply to any given proposal. Each reviewer will be asked to address only those that are relevant to the proposal and for which he/she is qualified to make judgements.

> **What is the intellectual merit of the proposed activity?**
> How important is the proposed activity to advancing knowledge and understanding within its own field or across different fields? How well qualified is the proposer (individual or team) to conduct the project? (If appropriate, the reviewer will comment on the quality of the prior work.) To what extent does the proposed activity suggest and explore creative and original concepts? How well conceived and organized is the proposed activity? Is there sufficient access to resources?
>
> **What are the broader impacts of the proposed activity?**
> How well does the activity advance discovery and understanding while promoting teaching, training, and learning? How well does the proposed activity broaden the participation of underrepresented groups (e.g., gender, ethnicity, disability, geographic, etc.)? To what extent will it enhance the infrastructure for research and education, such as facilities, instrumentation, networks, and partnerships? Will the results be disseminated broadly to enhance scientific and technological understanding? What may be the benefits of the proposed activity to society?

Principal Investigators should address the following elements in their proposal to provide reviewers with the information necessary to respond fully to both of the above-described NSF merit review criteria. NSF staff will give these elements careful consideration in making funding decisions.

> ***Integration of Research and Education***
> One of the principal strategies in support of NSF's goals is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions provide abundant opportunities where individuals may concurrently assume responsibilities as researchers, educators, and students and where all can engage in joint efforts that infuse education with the excitement of discovery and enrich research through the diversity of learning perspectives.
>
> ***Integrating Diversity into NSF Programs, Projects, and Activities***
> Broadening opportunities and enabling the participation of all citizens -- women and men, underrepresented minorities, and persons with disabilities -- 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 summary rating and accompanying narrative will be completed and signed by each reviewer. In all cases, reviews are treated as confidential documents. Verbatim copies of reviews, excluding the names of the reviewers, are sent to the Principal Investigator/Project Director by the Program Director. In addition, the proposer will receive an explanation of the decision to award or decline funding.

B. Review Protocol and Associated Customer Service Standard

All proposals are carefully reviewed by at least three other persons outside NSF who are experts in the particular field represented by the proposal. Proposals submitted in response to this announcement/solicitation will be reviewed by Mail and/or panel review.

Reviewers will be asked to formulate a recommendation to either support or decline each proposal. The Program Officer assigned to manage the proposal's review will consider the advice of reviewers and will formulate a recommendation.

NSF is striving to be able to tell applicants whether their proposals have been declined or recommended for funding within six months for 70 percent of proposals. The time interval begins on the date of receipt. The interval ends when the Division Director accepts the Program Officer's recommendation.

In all cases, 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 and 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 its own risk.

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 Division 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.A. for additional information on the review process.)

B. Award Conditions

An NSF award consists of: (1) the award letter, 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 letter; (4) the applicable award conditions, such as Grant General Conditions (NSF-GC-1)* or Federal Demonstration Partnership (FDP) Terms and Conditions * and (5) any announcement or other NSF issuance that may be incorporated by reference in the award letter. Cooperative agreement awards also are administered in accordance with NSF Cooperative Agreement Terms and Conditions (CA-1). Electronic mail notification is the preferred way to transmit NSF awards to organizations that have electronic mail capabilities and have requested such notification from the Division of Grants and Agreements.

*These documents may be accessed electronically on NSF's Web site at http://www.nsf.gov/home/grants/grants_gac.htm. Paper copies may be obtained from the NSF Publications Clearinghouse, telephone (301) 947-2722 or by e-mail from pubs@nsf.gov.

More comprehensive information on NSF Award Conditions is contained in the NSF *Grant Policy Manual* (GPM) Chapter II, available electronically on the NSF Web site at http://www.nsf.gov/cgi-bin/getpub?gpm. The GPM is also for sale through the Superintendent of Documents, Government Printing Office (GPO), Washington, DC 20402. The telephone number at GPO for subscription information is (202) 512-1800. The GPM may be ordered through the GPO Web site at http://www.gpo.gov.

C. Reporting Requirements

For all multi-year grants (including both standard and continuing grants), the PI must submit an annual project report to the cognizant Program Officer at least 90 days before the end of the current budget period.

Within 90 days after the expiration of an award, the PI also is required to submit a final project report. Approximately 30 days before expiration, NSF will send a notice to remind the PI of the requirement to file the final project report. Failure to provide final technical reports delays NSF review and processing of pending proposals for that PI. PIs should examine the formats of the required reports in advance to assure availability of required data.

NSF has implemented an electronic project reporting system, available through FastLane. This system permits electronic submission and updating of project reports, including information on project participants (individual and organizational), activities and findings, publications, and other specific products and contributions. PIs will not be required to re-enter information previously provided, either with a proposal or in earlier updates using the electronic system.

VIII. CONTACTS FOR ADDITIONAL INFORMATION

General inquiries regarding Trusted Computing should be made to:

- Dr. Carl Landwehr, Trusted Computing, Program Director, CISE, C-CR, 1145, telephone: 703-292-8936, e-mail: clandweh@nsf.gov
- Ms. Velma Swales, Lead Program Assistant, CISE, C-CR, 1145, telephone: 703-292-8936, e-mail: vswales@nsf.gov .

For questions related to the use of FastLane, contact:

- Ms. Sharon Glivens, Program & Technical Specialist, CISE, C-CR, 1145, telephone: 703-292-8910, e-mail: sglivens@nsf.gov.

IX. OTHER PROGRAMS OF INTEREST

The NSF *Guide to Programs* is a compilation of funding for research and education in science, mathematics, and engineering. The NSF *Guide to Programs* is available electronically at http://www.nsf.gov/cgi-bin/getpub?gp. General descriptions of NSF programs, research areas, and eligibility information for proposal submission are provided in each chapter.

Many NSF programs offer announcements or solicitations concerning specific proposal requirements. To obtain additional information about these requirements, contact the appropriate NSF program offices. Any changes in NSF's fiscal year programs occurring after press time for the *Guide to Programs* will be announced in the NSF E-Bulletin, which is updated daily on the NSF web site at http://www.nsf.gov/home/ebulletin, and in individual program announcements/solicitations. Subscribers can also sign up for NSF's Custom News Service (http://www.nsf.gov/home/cns/start.htm) to be notified of new funding opportunities that become available.

Proposals concerning Trusted Computing research that are submitted to NSF-wide programs such as the Information Technology Research and CAREER programs, as well as those that can be considered for EPSCOR funding, should designate CISE/C-CR TC as the related program area.

The CISE Trusted Computing program operates in partnership with all other programs in C-CR. It also coordinates research with the following programs in CISE/ANIR which emphasize issues in Internet security: Network Centric Middleware (MWIR), Strategic Technologies for the Internet (STI), Networking Research (NR), and Special Projects in Networking (SPN); with the CISE/IIS Information and Data Management (IDM) program; and with the CISE/EIA Next Generation Software (NGS) program and infrastructure programs.

ABOUT THE NATIONAL SCIENCE FOUNDATION

The National Science Foundation (NSF) funds research and education in most fields of science and engineering. Awardees are wholly responsible for conducting their project activities and preparing the results for publication. Thus, the Foundation does not assume responsibility for such findings or their interpretation.

NSF welcomes proposals from all qualified scientists, engineers and educators. The Foundation strongly encourages women, minorities and persons with disabilities to compete fully in its programs. In accordance with Federal statutes, regulations and NSF policies, no person on grounds of race, color, age, sex, national origin or disability shall be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving financial assistance from NSF (unless otherwise specified in the eligibility requirements for a particular program).

Facilitation Awards for Scientists and Engineers with Disabilities (FASED) provide funding for special assistance or equipment to enable persons with disabilities (investigators and other staff, including student research assistants) to work on NSF-supported projects. See the program announcement/solicitation for further information.

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, FIRS at 1-800-877-8339.

The National Science Foundation is committed to making all of the information we publish easy to understand. If you have a suggestion about how to improve the clarity of this document or other NSF-published materials, please contact us at plainlanguage@nsf.gov.

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; 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 applicant 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 needing information as part of the review process or in order to coordinate programs; 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," 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records," 63 Federal Register 268 (January 5, 1998). Submission of the information is voluntary. Failure to provide full and complete information, however, may reduce the possibility of receiving an award.

Pursuant to 5 CFR 1320.5(b), an agency may not conduct or sponsor, and a person is not required to respond to an information collection unless it displays a valid 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 this burden estimate and any other aspect of this collection of information, including suggestions for reducing this burden, to: Suzanne Plimpton, Reports Clearance Officer, Information Dissemination Branch, Division of Administrative Services, National Science Foundation, Arlington, VA 22230, or to Office of Information and Regulatory Affairs of OMB, Attention: Desk Officer for National Science Foundation (3145-0058), 725 17th Street, N.W. Room 10235, Washington, D.C. 20503.

OMB control number: 3145-0058.