Cyber Trust

Program Solicitation
NSF 04-524

National Science Foundation
Directorate for Computer and Information Science and Engineering

Letter of Intent Due Date(s) ***(required for Center-Scale proposals only):***

January 23, 2004
Center-Scale Proposals Only

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

March 03, 2004
Single Investigator or Small Group Proposals and Team Proposals

March 31, 2004
Center-Scale Proposals

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Cyber Trust

Synopsis of Program:

Networked computers reside at the heart of systems on which people now rely, both in critical national infrastructures and in their homes, cars, and offices. Today, many of these systems are far too vulnerable to cyber attacks that can inhibit their function, corrupt important data, or expose private information.

Cyber Trust promotes a vision of a society in which these systems are:

- more predictable, more accountable, and less vulnerable to attack and abuse;
- developed, configured, operated and evaluated by a well-trained and diverse workforce; and
- used by a public educated in their secure and ethical operation.

To improve national cyber security and achieve the Cyber Trust vision, NSF will support a collection of projects that together:

- advance the relevant knowledge base;
- creatively integrate research and education for the benefit of technical specialists and the general populace; and
- integrate the study of technology with the policy, economic, institutional and usability factors that often determine its deployment and use.

Proposals funded will support single and multiple-investigator projects within the broad range of disciplines contributing to the Cyber Trust vision. Projects will be supported in three categories: Single Investigator or Small Group projects, Team projects, and Center-Scale projects. The resulting Cyber Trust award portfolio will: advance the cyber security research frontier; build national education and workforce capacity (including undergraduate, graduate, and faculty development and training); and ensure that new knowledge can be put into practice.

All awards made are subject to the requirements of P.L. 107-305, the Cyber Security Research and Development Act.

Cognizant Program Officer(s):

- Carl Landwehr, Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: clandweh@nsf.gov
- D. Helen Gill, Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: hgill@nsf.gov
- Taieb Znati, Senior Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: tznati@nsf.gov
- Bhavani Thuraisingham, Program Director, Directorate for Computer & Information Science & Engineering, Division of Information and Intelligent Systems, 1115 N, telephone: (703) 292-8930, fax: (703) 292-9073, email: bthurais@nsf.gov
- Harriet G. Taylor, Program Manager, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: htaylor@nsf.gov

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

- 47.070 --- Computer and Information Science and Engineering

Eligibility Information

- **Organization Limit:** None Specified.
- **PI Eligibility Limit:**

An individual may appear as PI, co-PI, or Senior Personnel on no more than two proposals.

- **Limit on Number of Proposals:** None Specified.

Award Information

- **Anticipated Type of Award:** Standard or Continuing Grant or Cooperative Agreement
- **Estimated Number of Awards:** 20 to 40 - Up to 3 center-scale awards, up to 10 team awards, and up to 30 Single Investigator or Small Group awards will be made, dependent on availability of funds.
- **Anticipated Funding Amount:** $30,000,000

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

- **Letters of Intent:** Submission of Letters of Intent is required for Center-Scale proposals only. Please see the full text of this solicitation for further information.
- **Full Proposal Preparation Instructions:** This solicitation contains information that supplements the standard Grant Proposal Guide (GPG) proposal preparation guidelines. Please see the full text of this solicitation for further information.

B. Budgetary Information

- **Cost Sharing Requirements:** Cost Sharing is required for Center-Scale proposals only (Percentage).
- **Cost Sharing Level/Amount:** 20%
- **Indirect Cost (F&A) Limitations:** Not Applicable.
- **Other Budgetary Limitations:** Not Applicable.

C. Due Dates

- **Letters of Intent *(required for Center-Scale proposals only)*:**
  January 23, 2004
  Center-Scale Proposals Only
- **Full Proposal Deadline Date(s)** (due by 5 p.m. proposer's local time):
  March 03, 2004
  Single Investigator or Small Group Proposals and Team Proposals
  March 31, 2004
  Center-Scale Proposals

Proposal Review Information

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

TABLE OF CONTENTS

I. INTRODUCTION

Today's computing systems comprise a broad range of processors, communication networks, and information repositories. They are increasingly ubiquitous, and consequently they are increasingly subject to attack, misuse, and abuse. Computing systems are vulnerable to these threats due to technical and economic factors and to policy decisions. For example, it is exceedingly difficult to reason precisely about the behavior of a complex digital system. It is an art to design usable control interfaces for complex systems. Specifications and designs often neglect privacy concerns. It is hard to find security policies that are simple and flexible enough for users to tolerate, yet clear enough to guide system design and implementation. Power and bandwidth limitations constrain the security features in lightweight wireless devices. Cost and time-to-market considerations limit the use of high assurance implementation methods. Economics dictates having bundled software distributions that include vulnerable functions many users may not need. The data needed to understand the range and severity of security problems and to evaluate the effectiveness of alternative solutions are lacking or closely held. Finally, insecure system designs impose costs on individuals and organizations who use them rather than on those who produce them.

The Cyber Trust program supports research and education activities that will lead to trustworthy computing *systems.* The Cyber Trust vision is of a society in which:

- *People can justifiably rely on computer-based systems to perform critical functions securely.* These systems include not only critical national-scale infrastructures--- such as the computer and communication networks, the electric power grid, gas lines, water systems, and air traffic control systems---but also more localized systems that perform safety-critical functions in aircraft, automobiles, and even home appliances. These systems must be dependable

even in the face of cyber attacks.

- *People can justifiably rely on systems to process, store, and communicate sensitive information securely.* Increasing volumes of information flow on our financial networks, health networks, and even our library systems, not to mention our conventional communication systems and our networked systems of personal and corporate computers. Confidence that these systems conform to policy (and that the policy is understood) even in the face of cyber attacks will permit people to make informed and rational decisions.

- *People can justifiably rely on a well-trained and diverse workforce to develop, configure, modify, and operate essential computer-based systems.* Educational systems must not only be able to graduate qualified technical specialists who can design, develop, and operate critical systems and investigate attacks on them, but they must also be able to educate the general public in secure and ethical use of technology.

II. PROGRAM DESCRIPTION

Trustworthiness is a system property, and many factors influence how systems are put together. Consequently, Cyber Trust covers both the full spectrum of information processing technologies and the social, legal, organizational, and economic factors surrounding the use of those technologies. To make progress towards the Cyber Trust vision requires

a) Advances in knowledge and technology. This need motivates basic research on ways to make computing systems more secure.

b) Improved understanding of the human, organizational, legal, and economic contexts in which trusted systems are developed and operated. This need motivates multi-disciplinary research to identify overall effects of technical developments.

c) Improved education both of those who will produce systems using new technology and those who will configure, operate, investigate, and use the systems produced. This need motivates activities to develop a diverse and robust workforce.

Research is needed in a wide range of areas, addressing trustworthiness at all levels of system design, implementation, and use. It is difficult enough to design and build digital systems that work properly in a benign environment. It is far harder to build systems that can withstand attack or abuse. To achieve the Cyber Trust vision, the science and technology of trustworthy systems must be developed, and it must be developed taking account of the social, economic, policy, and legal factors that determine whether and at what rate technology is deployed. Application domains span the scale from global networks and large-scale computing to the ever smaller processing and network elements finding their way into cars, buildings, and infrastructure systems of all types. Better abstractions are needed for reasoning about system behavior and attributing responsibility for system actions. Better means are needed for benchmarking, measurement, and data collection to build the empirical underpinnings of the field.

Innovative approaches are needed in education, so that capable students participate in research and research results are quickly integrated into the educational process. System trustworthiness considerations must be included throughout the computer and information science and engineering curriculum, not just in courses for specialists. The concepts of proper system operation and ethical use of technology must have even broader reach, to touch students throughout the academic enterprise and beyond.

Research Areas

Research is warranted in aspects of the entire system life cycle: development of security and privacy policies; definition of requirements; construction, validation and verification of components and systems; operation, monitoring, maintenance, and recovery after failures or incidents; and forensics, sanitization, and disposal. Research that spans the technical areas affecting integrated information technologies is strongly encouraged. This includes projects to advance or apply combinations of technologies to solve particularly challenging problems, to understand engineering tradeoffs among competing or complementary technical approaches, and to explore synergies among technologies.

Multi-disciplinary research that includes behavioral and social science disciplines is also strongly encouraged. System engineering tradeoffs are rarely based solely on technical issues. Social, organizational, economic, regulatory, and legal factors often play a major role in determining which technologies are developed, which ones are applied, and how they are used. These choices can have a major influence on overall system trustworthiness. Many technologies that hold great potential for increasing system trustworthiness have seen little use in practice because, for example, they are seen as too time-consuming or as imposing too great a performance penalty in relation to any expected market advantage. Through multi-disciplinary Cyber Trust projects, NSF seeks to increase understanding both of the technical implications and the role of social, economic and other factors in developing trustworthy systems.

The following paragraphs elaborate some areas that require investigation to achieve the Cyber Trust vision. They should be considered representative, not exhaustive.

The breadth of application of computers and communications continues to expand as computing and communication continues to become faster and cheaper. The needs and policies of applications—whether for computation, information processing, or real-time sensing and control—drive the trustworthiness requirements on lower system layers. Lower system layers cannot provide all the needed protection, because they lack knowledge of application semantics. At the same time, information systems and applications cannot stand alone: They need to be integrated securely with middleware, operating systems, and networks. A better understanding is needed of how to make engineering tradeoffs among these layers to achieve desired application security at acceptable cost and performance. Sample research areas include:

- authentication, access control, and privacy protection;
- technologies for policy specification, trust negotiation, collaboration;
- application information flow certification;
- audit and application forensics;
- security and privacy in databases and high interest applications (e.g., voting, healthcare, data mining, semantic web, digital libraries); and
- comprehensible user interfaces for trust and security management.

Systems software provides the basis on which future applications will be built, and it governs system behavior, yet cost, power, weight, and response-time constraints—as well as the complexity of the task—often inhibit the development of controls that might prevent misuse or abuse. Security mechanisms are needed that can protect both conventional computers and increasingly pervasive embedded systems at all scales, from lightweight protection for tiny embedded sensors to complex controls for systems that require end-to-end protection. While broadly applicable research results are always desired, progress in this area may sometimes come through detailed work in a particular platform or system context. Sample research areas include:

- trustworthy operating system architectures;

long-lived data archiving mechanisms;

- access control for real-time operating systems;
- combined software/hardware approaches to trustworthiness; and
- middleware for trustworthy software-controlled real-time systems.

The increasing scale and diversity of communication networks amplifies their vulnerability by expanding the number of possible failures and providing more points of access to attackers. Research to improve the trustworthiness of networks at all scales and to explore the evolving nature of the security protocols and policies in communications networks is of interest. Sample research areas include:

- design principles for secure network services and protocols;
- affordable network security designs;
- denial of service prevention and avoidance;
- security for collaborative environments and Grid computing;
- deployment, testing and validation of network security tools and mechanisms;
- anonymity and accountability in networks; and
- network forensics.

Research that establishes a sound scientific foundation and technological basis for computing and communications in a world that may include malicious actors is of interest. Foundational research in secure, dependable information systems and software-controlled systems, methods for assuring correct behavior of algorithms and protocols, assessing the trustworthiness of systems and certifying proper information flow, as may be required to enforce privacy and security policies. Results of fundamental research are expected to have broad application and not to be limited to a particular platform or operating system. Sample research areas include:

- methods for specifying, reasoning about, and developing trustworthy components and networks, including novel hardware/firmware designs;
- composition methods;
- evaluation and certification methods;
- maintaining trustworthiness as systems change and adapt;
- quantifying engineering trade-offs in trustworthy systems; and
- measuring, modeling, analyzing, and validating system trust properties.

Education and Workforce Development

Education to develop and maintain both a highly skilled Cyber Trust workforce and an informed populace is essential to the Nation. Capacity-building activities are essential to educate the experts who will design and develop future trusted systems, to provide a thorough background in cyber trust for those who will manage, configure, and operate such systems, and to provide fundamental cyber security education for all citizens to secure systems of the future.

To develop, maintain, and enhance this critical educational infrastructure, all proposals must include an educational and workforce component. Proposals must specifically describe their education and workforce development contributions, including the planned benefits and impact of the activities described. Appropriate goals for these activities include integration of research and education, promotion of knowledge transfer, reaching diverse populations and promoting diversity in the cyber security workforce, building capacity within educational institutions for cyber security education, faculty development, and building academic and/or industrial partnerships. Sample activities include:

- developing materials to integrate trustworthiness considerations into existing courses;
- disseminating best practices and models to the general public;
- having graduate students mentor technical support staff of K-12 institutions;
- offering summer industry internships for faculty and students;
- developing online resources for faculty; and
- developing student competitions to encourage more trustworthy programming practices.

Award Categories

Cyber Trust awards made will support single or multiple-investigator projects within the broad range of relevant disciplines.

Awards will be made in three categories: Single Investigator or Small Group awards, Team awards, and Center-Scale awards. Single Investigator or Small Group awards are expected to be small scale, focused, and intensive. Of particular interest are fresh starts that aim at developing new expertise or formulating new research and education directions. Team awards support intensive research and education activities undertaken by teams of researchers and educators. They will focus teams on challenging Cyber Trust problems that may cross disciplinary boundaries. Center-Scale awards promote synergy among academic, industrial and other partners. They address the combined needs for in-depth or multidisciplinary research investigations, education and workforce development, and incorporation of research results into deployed products and systems. Single Investigator or Small Group projects and Team projects will be supported as standard or continuing grants. Center-Scale projects will be supported as cooperative agreements.

Proposal preparation guidance for projects in each of these categories is elaborated in Section V. Proposal Preparation and Submission Instructions of this solicitation.

III. ELIGIBILITY INFORMATION

The categories of proposers identified in the Grant Proposal Guide are eligible to submit proposals under this program announcement/solicitation.

IV. AWARD INFORMATION

Awards funded under this theme may support projects working within a broad range of disciplines related to the Cyber Trust vision, including those that address, for example, usability, economics, or policy aspects in combination with technological aspects of Cyber Trust. There are three types of awards.

1) Single Investigator or Small Group awards last up to 3 years, average about $150,000 per year, and do not exceed $175,000 per year.

2) Team awards last up to 3 years and do not exceed $750,000 per year.

3) Center-scale awards range from $1 million to $2 million per year for 5 years.

Estimated program budget, number of awards, and average award size/duration are subject to the availability of funds.

V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

A. Proposal Preparation Instructions

Letters of Intent *(required for Center-Scale proposals only):*

For center-scale proposals only, a Letter of Intent, three pages or less, is required. It must include:

1. Name of the proposed activity, the name of the lead/submitting institution, and the names of any partner organizations.

2. Brief statement of the vision and goals of the activity and description of its research, education / workforce development, and external collaboration and technology transfer programs at a sufficient level of detail to permit identification of conflicts of interest and allow potential reviewers to be selected.

3. List of faculty participants, including full names, roles in the activity, departmental and institutional affiliations.

4. List of individuals, with organizational affiliations, who are not members of the proposing team and whose selection as reviewers might constitute a conflict of interest due to involvement in proposal development, thesis supervision, co-publication or authorship, co-PI relationships, etc.

5. List of suggested reviewers, with organizational affiliations, who have the expertise to review the proposal and have no affiliations that would cause conflicts.

Full Proposal Instructions:

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 Website at: http://www.nsf.gov/cgi-bin/getpub?gpg. Paper copies of the GPG may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 or by e-mail from pubs@nsf.gov.

Individual Investigator or Small Group Proposals

Proposals in this size class must specifically describe their integrated research and education and workforce development contributions, including the planned benefits and impact of the activities described.

Team Proposals

Proposals in this size class must describe substantial and ambitious research and education projects, either to focus a team of researchers and educators on a particularly challenging technical area or to create a multi-disciplinary team to address important cross-disciplinary challenges that will contribute to realization of the Cyber Trust vision.

Proposals for these projects should describe plans for distributing the research results and should strive to assist scientists and engineers to use their results in ways that go beyond traditional academic publications. They must also creatively address education and workforce development contributions, including the planned benefits and impact of the activities described.

The project description should explain why a budget of the requested size is required to carry out the proposed activities and why the work needs to be conducted as a team effort. Midterm external reviews and/or site visits may be expected at NSF's discretion.

Center-Scale Proposals

Center-scale projects promote synergy among academic, industrial and other partners. Proposals must address the combined needs for in-depth or multi-disciplinary research investigations, education and workforce development, and incorporation of research results into deployed products and systems that lead to the realization of the Cyber Trust vision.

The project description for a center-scale proposal must incorporate five main elements:

- *Research Plan*—Describe the research objectives of the project; objectives that bring diverse scientific, engineering, and other disciplines together to address fundamental research issues crucial to achieving the Cyber Trust vision. Provide a detailed research plan with a timeline for the activities proposed.

- *Education and Outreach*—Describe activities designed to create a culture in which graduate and undergraduate students of diverse backgrounds work in cross-disciplinary teams, in close collaboration with external partners. Integrate education and research and expose students to the integrative aspects of Cyber Trust-related systems and industrial practice to build competence for their future careers. Develop curriculum innovations derived from the activity's goals. Produce graduates with the depth and breadth of education needed to sustain leadership throughout their careers. Center-Scale Activities will include one or more community-extending concepts such as creative undergraduate education activities; programs to address the under-representation of women and minorities in the Cyber Trust workforce; links to institutions with strong traditions of teaching, mentoring, and workforce development; or participation by institutions in EPSCoR states.
- *Effective Partnership and Technology Transfer*—Describe activities designed to develop and sustain strong partnerships between academic and other partners. Activities may involve collaboration with partners in industry, including service industries, public agencies, or government laboratories. Partners may be involved through integral activities such as participation in strategic planning, joint research, mentoring students, and supporting proof-of-concept testbeds—-all modes that strengthen the partnership and speed technology transfer. Describe the intellectual foundation for partners to collaborate with faculty and students to address both long-range and shorter-

term challenges, producing the knowledge needed to ensure steady advances in technology and to speed their transition to the marketplace, while training graduates who are more effective in their subsequent careers.

- *Management Plan*—Describe the management and coordination of the proposed activities. The plan must identify the Project Director, the NSF Principal Investigator, responsible for leading the activity and administering the award in accordance with the terms and conditions of the Cooperative Agreement issued by the NSF in the event of an award. In addition, it should address the following needs:
  - A central point of communication with NSF,
  - Management of project activities,
  - Coordination of technology transfer activities,
  - Fulfillment of educational and workforce development responsibilities, and
  - An Advisory Board of outside experts to advise the Director.
- *Evaluation Plan*—Specify evaluation methods that will support assessment of both research results and the effectiveness of education and workforce development activities.

Proposers are reminded to identify the program announcement/solicitation number (04-524) in the program announcement/ solicitation block on the proposal Cover Sheet. 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 *(required for Center-Scale proposals only)*:

Applies to Center-Scale proposals only, see Section II.

Cost sharing at a level of 20 percent of the requested total amount of NSF funds is required for all proposals submitted in response to the *Center-Scale category* of this announcement/solicitation.

Only items which would be allowable under the applicable cost principles, if charged to the project, may be included in the awardee's contribution to cost sharing. Contributions may be made from any non-Federal source, including non-Federal grants or contracts, and may be cash or in kind (see OMB Circular A-110, Section 23). It should be noted that contributions counted as cost sharing toward projects of another Federal agency may not be counted towards meeting the specific cost sharing requirements of the NSF award.

All cost sharing amounts are subject to audit. Failure to provide the level of cost sharing reflected in the approved award budget may result in termination of the NSF award, disallowance of award costs and/or refund of award funds to NSF.

C. Due Dates

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

Letters of Intent *(required for Center-Scale proposals only)*:

January 23, 2004
Center-Scale Proposals Only

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

March 03, 2004
Single Investigator or Small Group Proposals and Team Proposals

March 31, 2004

D. FastLane Requirements

Proposers are required to prepare and submit all proposals for this announcement/solicitation 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 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 announcement/solicitation should be referred to the NSF program staff contact(s) listed in Section VIII of this announcement/solicitation.

Submission of Electronically 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 electronic certifications within five working days following the electronic submission of the proposal. Proposers are no longer required to provide a paper copy of the signed Proposal Cover Sheet to NSF. 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.

The National Science Board approved revised criteria for evaluating proposals at its meeting on March 28, 1997 (NSB 97-72). All NSF proposals are evaluated through use of the two merit review criteria. In some instances, however, NSF will employ additional criteria as required to highlight the specific objectives of certain programs and activities.

On July 8, 2002, the NSF Director issued Important Notice 127, Implementation of new Grant Proposal Guide Requirements Related to the Broader Impacts Criterion. This Important Notice reinforces the importance of addressing both criteria in the preparation and review of all proposals submitted to NSF. NSF continues to strengthen its internal processes to ensure that both of the merit review criteria are addressed when making funding decisions.

In an effort to increase compliance with these requirements, the January 2002 issuance of the GPG incorporated revised proposal preparation guidelines relating to the development of the Project Summary and Project Description. Chapter II of the GPG specifies that Principal Investigators (PIs) must address both merit review criteria in separate statements within the one-page Project Summary. This chapter also reiterates that broader impacts resulting from the proposed project must be addressed in the Project Description and described as an integral part of the narrative.

Effective October 1, 2002, NSF will return without review proposals that do not separately address both merit review criteria within the Project Summary. It is believed that these changes to NSF proposal preparation and processing guidelines will more clearly articulate the importance of broader impacts to NSF-funded projects.

The two National Science Board approved merit review criteria are listed below (see the Grant Proposal Guide Chapter III.A for further information). The criteria include considerations that help define them. These considerations are suggestions and

not all will apply to any given proposal. While proposers must address both merit review criteria, reviewers will be asked to address only those considerations that are relevant to the proposal being considered and for which he/she is qualified to make judgments.

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?

NSF staff will give careful consideration to the following 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.

Additional Review Criteria:

Additional criteria for center-scale proposals only:

Quality of research plan:
Are the identified research objectives of sufficient import, scale, and complexity to justify center-scale investment? Is the proposed timeline realistic?

Effectiveness of education and outreach:
Will the proposed activity make a special contribution to the achievement of a diverse, highly competent, and globally engaged technical and instructional workforce, and of an educated populace?

Effectiveness of partnership and technology transfer
Will any proposed new mechanisms, shared experimental facilities, and/or databases be of significant value to a broad community of researchers and/or users? Will the activity's external partnerships achieve significant intellectual exchange and resource linkage with the school, public, industry, federal, and/or international sectors and thereby foster more trustworthy computer-based systems throughout society?

Management plan:

Does the management plan and proposed management team convincingly demonstrate the vision, experience, and capacity to manage the proposed activities, including external partnerships?

Evaluation plan:
Does the evaluation plan provide measures of research success suited to the planned research? Can results be assessed incrementally? Are the education and workforce development evaluation methods appropriate to the proposed activities?

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 Ad Hoc 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.

A summary rating and accompanying narrative will be completed and submitted 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.

NSF is striving to be able to tell applicants whether their proposals have been declined or recommended for funding within six months. 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 their 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 Website at http://www.nsf.gov/home/grants/grants_gac.htm. Paper copies may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 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 Website 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 Website at http://www.gpo.gov.

Special Award Conditions:

Awards made under this announcement are subject to the stipulations of P.L. 107-305, the Cyber Security Research and Development Act.

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.

Center-scale awards may be site visited one or more times at NSF's discretion.

Within 90 days after the expiration of an award, the PI also is required to submit a final project report. Failure to provide final technical reports delays NSF review and processing of pending proposals for the PI and all Co-PIs. 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 FastLane, for preparation and submission of annual and final project reports. 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 this program should be made to:

- Carl Landwehr, Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: clandweh@nsf.gov
- D. Helen Gill, Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: hgill@nsf.gov
- Taieb Znati, Senior Program Director, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: tznati@nsf.gov

- Bhavani Thuraisingham, Program Director, Directorate for Computer & Information Science & Engineering, Division of Information and Intelligent Systems, 1115 N, telephone: (703) 292-8930, fax: (703) 292-9073, email: bthurais@nsf.gov

- Harriet G. Taylor, Program Manager, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: htaylor@nsf.gov

For questions related to the use of FastLane, contact:

- Cornell Davis, Program and Technology Specialist, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: cdavis@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 Website 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.

CAREER proposals to the Cyber Trust theme are encouraged; please see the CAREER announcement and contact one of the Cyber Trust Program Directors listed herein to confirm specific CAREER application procedures for Cyber Trust. Investigators also are encouraged to integrate Cyber Trust education in proposals submitted to other NSF programs that have an education or workforce focus, such as ADVANCE, REU sites, ITWF, CRCD/EI, IGERT, or GK-12.

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, although some programs may have special requirements that limit eligibility.

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 GPG Chapter II, Section D.2 for instructions regarding preparation of these types of proposals.

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 or (800) 281-8749
- **To Order Publications or Forms:**

  Send an e-mail to: pubs@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; 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.

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, Division of Administrative Services, National Science Foundation, Arlington, VA 22230.

OMB control number: 3145-0058.

The National Science Foundation
4201 Wilson Boulevard, Arlington, Virginia 22230, USA
Tel: 703-292-5111, FIRS: 800-877-8339 | TDD: 703-292-5090 or (800) 281-8749