Cyber Trust (CT)

Program Solicitation
NSF 07-500

Replaces Document(s):
NSF 06-517

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

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

January 08, 2007

Second Wednesday in November, Annually Thereafter

REVISION NOTES

In furtherance of the President's Management Agenda, NSF has identified programs that will offer proposers the option to utilize Grants.gov to prepare and submit proposals, or will require that proposers utilize Grants.gov to prepare and submit proposals. Grants.gov provides a single Government-wide portal for finding and applying for Federal grants online.

In response to this program solicitation, proposers may opt to submit proposals via Grants.gov or via the NSF FastLane system. 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.3 of the Grant Proposal Guide provides additional information on collaborative proposals.

SUMMARY OF PROGRAM REQUIREMENTS

General Information

Program Title:

Cyber Trust (CT)

Synopsis of Program:

Computers reside at the heart of systems on which people heavily rely. From critical national infrastructures

to personal computing devices, these systems are expected to work, and work as intended. Unfortunately, many of these systems are vulnerable to malicious acts that can inhibit operation, corrupt valuable data or expose private information. In fact, the news is replete with stories of vulnerabilities that were exploited for ill. Future advances in computing promise many substantial benefits for society and individuals; yet unless trust in computing can be instilled, assured, and verified, these benefits are at risk.

The NSF Cyber Trust (CT) program promotes a vision of a society in which people can justifiably rely on:

- computer systems to perform critical functions securely;
- computer systems to process, store and communicate sensitive information securely; and,
- a diverse, well-trained workforce able to use, develop, configure, modify and operate computer-based systems.

To achieve the CT vision and simultaneously improve the Nation's cybersecurity posture, CT will support a portfolio of projects that:

- contribute to the cybersecurity knowledge base and advance cybersecurity technologies;
- address trustworthiness at all levels of system design, implementation and use;
- consider the social, economic, organizational and legal factors influencing the successful adoption of new cybersecurity approaches and technologies; and,
- build national education and workforce capacity, addressing undergraduate, graduate, and faculty development and training.

Proposals funded will cover a broad range of disciplines contributing to the CT vision.

Three types of CT projects will be supported:

- Exploratory Research projects;
- Single Investigator or Small Group projects; and,
- Team projects.

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

Cognizant Program Officer(s):

- Karl Levitt, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: klevitt@nsf.gov
- David Du, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: ddu@nsf.gov
- Ralph Wachter, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: rwachter@nsf.gov
- Le Gruenwald, Program Director (Data Management Systems), 1125 S, telephone: (703) 292-8074, fax: (703) 292-9073, email: lgruenwa@nsf.gov
- William Steiger, Program Director, 1115 N, telephone: (703) 292-8910, fax: (703) 292-9059, email: wsteiger@nsf.gov

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

- 47.070 --- Computer and Information Science and Engineering

Award Information

Anticipated Type of Award: Standard Grant or Continuing Grant

Estimated Number of Awards: 80 total. Up to 15 Team awards, up to 50 Single Investigator and Small Group awards, and up to 20 Exploratory Research awards will be made, dependent on availability of funds and the quality of proposals received.

Anticipated Funding Amount: $34,000,000 in FY 2007 pending availability of funds.

Eligibility Information

Organization Limit:

Proposals may only be submitted by the following:

- Proposals may be submitted by U.S. academic institutions or non-profit research institutions with a strong educational component. For-profit organizations and other federal agencies may not apply directly; they may receive subcontracts, but such subcontracts must be justified by explaining the unique capability or expertise being provided.

PI Limit:

None Specified

Limit on Number of Proposals per Organization:

None Specified

Limit on Number of Proposals per PI: 2

An individual may appear as PI, co-PI, Senior Personnel, or Consultant on no more than two proposals submitted to each Cyber Trust competition.

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

- **Letters of Intent:** Not Applicable
- **Full Proposals:**
  - Full Proposals submitted via FastLane: 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/bfa/dias/policy/docs/grantsgovguide.pdf/)

B. Budgetary Information

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

C. Due Dates

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

January 08, 2007

Second Wednesday in November, Annually Thereafter

Proposal Review Information Criteria

Merit Review Criteria: National Science Board approved criteria apply.

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

Today's computing systems comprise a broad range of processors, communications networks, and information repositories. These systems are increasingly pervasive and persistent; unfortunately, they are often subject to attack, misuse and abuse. Computing systems are vulnerable due to technical, developmental, economic, policy, and scaling factors, among others. For example, power and bandwidth limitations constrain security features and capabilities in lightweight wireless devices; system specification and design often neglect security and privacy concerns until too late in the development and deployment cycle; time and expense of certification and the inherent performance penalty limit the use of high assurance methods for security; policies for enterprise-wide system security are difficult to define and implement with the right enforcements and protections that are simple and flexible enough for many different enterprise users; and, the increasing number of computing devices that are network-enabled is now beyond the capability of any organization to fully secure them. Unfortunately, the

consequences of insecure computer systems are borne by users, rather than by developers.

NSF's Cyber Trust (CT) program supports research and education activities that will lead to trustworthy computing systems. The CT vision is of a society in which people can justifiably rely on:

- *computer systems to perform critical functions securely.* These systems include not only critical national-scale infrastructures - such as 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. In a world of increasingly ubiquitous and pervasive computing, increasingly complex and large-scale computing systems must be dependable, even in the face of cyber attacks.

- *computer systems to process, store, and communicate sensitive information securely.* Increasing volumes of information flow on our financial networks, health networks, library systems and other public systems, as well as on networked systems of personal and corporate computers. Confidence that these systems conform to policy (and that the policy is understood) and that the information is secure in the face of cyber attacks, will permit people to make informed and rational decisions about their reliance on these systems.

- *a diverse, well-trained workforce able to use, develop, configure, modify and operate computer-based systems..* Educational organizations 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 computer technology.

II. PROGRAM DESCRIPTION

Trustworthiness is a system property, and many factors influence how systems are designed and implemented. Accordingly, CT covers both the full spectrum of computer technologies comprising computer systems, and the social, legal, organizational, and economic factors influencing the use of those technologies. To make progress towards the CT vision requires:

- advances in knowledge and technology. This need motivates basic research that promises more secure computer systems, and that is informed by the human, organizational, legal, and economic contexts in which trusted systems are developed and operated. Multi-disciplinary research is therefore essential to the successful adoption of new science and technology developments.
- focus on trustworthiness at all levels of system design, implementation, and use. It is difficult enough to design and build computer systems that work properly in a benign environment. It is far harder to build systems that can withstand attack or abuse. To achieve the CT vision, the science and technology of trustworthy systems must be developed. Application domains span the scale from global networks and large-scale computing, to the ever-smaller processing and network components 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 empirical underpinnings now missing in the cybersecurity field.
- consideration of the social, economic, organizational and legal factors influencing the successful adoption of new cybersecurity approaches and technologies. Improved understanding of the social, organizational, economic and legal contexts in which trusted systems are developed and operated must be developed, influencing whether and at what rate technology is deployed.
- building national education and workforce capacity, including undergraduate, graduate, and faculty development and training. Innovative approaches in education must be developed 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 individuals throughout the academic enterprise and beyond.

Research Areas

Research supported will address: all aspects of the computer system life cycle: development of security and privacy policies; definition of requirements; construction, evaluation and verification of components and systems; operation, monitoring, maintenance, and recovery after failures or incidents; and forensics, sanitization, and disposal in the aftermath of an incident. Research that spans the technical areas promoting the effective integration of 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 experts from the behavioral and social science disciplines is 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. Through multi-disciplinary CT projects, NSF seeks to increase understanding both of the technical implications and the role of social, economic and other factors in developing trustworthy computer systems.

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

Security for Applications

The application of computer systems continues to expand as computer technologies become simultaneously faster and cheaper. Application requirements and policies for use - whether for computation, information processing, or real-time sensing and control - determine trustworthiness requirements. In some cases, lower system layers can achieve these requirements on behalf of the applications. However in other cases, lower system layers cannot provide all the needed protection, because they lack knowledge of application semantics. In general, applications cannot stand alone; they need to be integrated securely with middleware, operating systems, networks and hardware. A better understanding is needed of how to make tradeoffs among computer system layers to achieve desired application security at acceptable cost and performance. Sample research areas include:

- authentication, access control, and privacy protection;
- technologies for policy discovery and specification, trust assessment, negotiation, and collaboration;
- security, trust and privacy in information flow management;
- audit and application forensics;
- security, trust and privacy in databases, data warehouses and other information sources;
- security, trust and privacy in high interest applications (e.g. healthcare, data mining, web services, digital libraries, e-government, e-commerce);
- comprehensible user interfaces and other mechanisms for trust, security and privacy management;
- autonomous adaptation of systems to changes in threats or in the application's environment;
- knowledge integration and management for applications; and
- artificial diversity to produce applications that survive attacks without increasing the burden of managing applications.

Security for Computer Systems

Computer systems are controlled by systems software that governs system behavior and provides the basis on which applications are built. However cost, power, weight, and response-time constraints - as well as the complexity of the task - often inhibit the development of controls that might prevent system misuse or abuse. Security mechanisms in system software 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. Broadly applicable research results are always desired, but progress in this area may sometimes come through detailed work on a particular platform or in a particular system context. Sample research areas include:

- trustworthy operating system architectures, including re-visiting the paradigm of separation kernels and other operating structures that localize security-critical functionality to foster understanding and evaluation;
- secure hierarchical control and trustworthy transaction processing for infrastructure systems;
- long-lived data archiving mechanisms;
- access control for specialized operating systems such as those that support real-time and sensor management;
- combined software/hardware approaches to trustworthiness;
- middleware for trustworthy systems in support of transaction processing, wireless and sensor systems, fault-tolerant systems, real-time systems and others; and
- virtualization mechanisms to support separation of processes, with an emphasis on the evaluation of such mechanisms.

To avoid performance degradation attendant to security solutions, special-purpose hardware devices can be provided as enhancements to conventional processing units such as:

- security co-processors to support critical security functions such as intrusion detection and the encryption of data;
- enhanced storage devices to support forensics and recoverability from attacks;
- devices and related technologies that support the attainment of accountability of actions; and
- devices to support guaranteed authentication.

Security for Networks

The increasing scale and diversity of the current Internet amplifies its vulnerability by expanding the number of possible failures and providing more points of access to attackers. Research is needed, not only to improve the security of the current Internet, but also to inform the design of a future Internet in which security and robustness are embedded from the ground up. Sample research areas include:

- creating secure networks from insecure components;
- network support for end-node security;
- development of security mechanisms that are robust to normal extensions to the technologies by users and operators (e.g. secure tunneling);
- creating secure approaches to network functions, such as addressing, routing, forwarding, naming, etc.;
- development of mechanisms that support security evaluation, by simulation, analytical reasoning (including formal methods), and emulation;
- approaches for the realistic empirical evaluation of the security of networks too large to be faithfully represented on size-limited testbeds (e.g. DETER/EMIST and GENI);
- designing mechanisms that enable socially aware trade-offs in security and privacy;
- design principles for secure network services and protocols that will yield more network structures than currently available;
- network security architectures for both wired and wireless systems;
- security for collaborative environments and grid computing;
- analytical or empirical methods to evaluate the capability of security solutions to prevent or recover from attacks;
- anonymity and accountability in networks;
- network forensics; and,
- artificial diversity to reduce the exposure of networks to scripted attacks.

PIs are encouraged to submit proposals on new network architectures that offer substantial improvements in security.

New Security Foundations

The CT program also supports research that establishes a sound scientific foundation and technological basis for computing and communications in a world that includes malicious actors. Research results are expected to have broad application, and not be limited to a particular platform or operating system. Sample research areas include:

- methods for specifying, reasoning about, and developing trustworthy components and systems, including novel hardware/firmware designs; of particular interest are lightweight methods to verification (such as static analysis) of program code and configuration files;
- the synergistic combination of static and dynamic evaluation methods;
- the use of static and dynamic evaluation methods to identify security flaws in the stages of the life-cycle;
- methods that effectively and efficiently address such problems as the identification of life-cycle vulnerabilities in a system;
- composition methods;
- automatic generation of security configurations;
- methods to assure that information flow in complex systems complies with security and privacy policies;
- maintaining trustworthiness as systems change and adapt;
- quantifying trade-offs in trustworthy systems for example between security and performance;
- measuring, modeling, analyzing, and validating system trust properties, for example the determination of the effort required by an attacker to defeat security features;
- new mechanisms that provide quantifiable guarantees of trust;
- methods to assure the trustworthiness of security features themselves; and
- methods to achieve trustworthiness in the presence of attacks more complex and lethal than those currently observed.

Securing complex systems requires attention to all components that are subject to attack or that support the management of attacks; it is not possible to attain security by focusing attention, for example, to just a single layer in a complex system organization. Sample research areas include:

- aggregation of alerts across layers;
- prediction of the path of an attack in progress;
- determination of possible remediation actions against an attack;
- efficient management of security mechanisms across a complex system; and,
- dynamic dispatching of security-enhancement actions.

Building Workforce Capacity

To develop, maintain, and enhance cybersecurity educational infrastructure, all CT projects must include educational synergy components that may take many forms. Educational synergy components should be natural extensions of the research activity, with CT investigators fully engaged. Collaboration between researchers and educators is strongly encouraged. Educational innovation and clear vision and linkage to the current state of CT research are essential.

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

In unusual circumstances, the CT program will entertain proposals that are beyond the scope and funding levels noted in this solicitation. Such proposals would be expected to explore groundbreaking or paradigm-changing ideas and/or to pursue a grand challenge requiring the work of a substantial number of researchers. Projects of this type might well include multidisciplinary investigators and be of interest to several or all CISE divisions or, even involve funding from other U.S. Government agencies. PIs who have in mind such a project must first contact via email Karl Levitt, a Cyber Trust program officer listed in this solicitation, to discuss the proposed project. PIs may submit a full proposal only after being given permission to do so. The contact must take place before the program solicitation deadline so the program can plan for the receipt and review of this kind of proposal.

III. AWARD INFORMATION

Three types of awards will be supported:

- Exploratory Research awards will last up to 2 years, with budgets not to exceed $250,000 total. In FY 2007, CISE expects to select for award up to 20 proposals in this category.
- Single Investigator and Small Group awards will last up to 3 years, with budgets not to exceed $500,000 total. In FY 2007, CISE expects to select for award up to 50 projects in this category.
- Team awards may last up to 4 years , with budgets not to exceed $2,000,000 total. In FY 2007, CISE expects to select for award up to 15 projects in this category.

Estimated program budget, number of awards, and award sizes are subject to the availability of funds.

IV. ELIGIBILITY INFORMATION

Organization Limit:

Proposals may only be submitted by the following:

- Proposals may be submitted by U.S. academic institutions or non-profit research institutions with a strong educational component. For-profit organizations and other federal agencies may not apply directly; they may receive subcontracts, but such subcontracts must be justified by explaining the unique capability or expertise being provided.

PI Limit:

None Specified

Limit on Number of Proposals per Organization:

None Specified

Limit on Number of Proposals per PI: 2

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

submitted to each Cyber Trust competition.

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 pubs@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/bfa/dias/policy/docs/grantsgovguide.pdf). 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 pubs@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.3 of the Grant Proposal Guide provides additional information on collaborative proposals.

The following instructions deviate from the GPG guidelines and the NSF Grants.gov Application Guide.

To assist NSF staff in sorting proposals for review, proposal titles MUST begin with an acronym that identifies the type of proposal being submitted. Use the following acronyms:

- Cyber Trust Exploratory Research proposal = CT-ER
- Cyber Trust Individual or Small Group proposal = CT-ISG
- Cyber Trust Team proposal = CT-T

For example, a Cyber Trust Team proposal might have a title such as "CT-T: New Methods for Assuring Privacy-Compliant Information Flow." Proposals without such acronyms may be returned without review.

Exploratory Research Proposals

Proposals in this category must specifically describe the innovative nature of the exploratory research ideas to be pursued, and the education and workforce development advances that will be undertaken as an integral part of the project. The planned benefits and impact of the proposed activities, even if long range, should be described.

Individual Investigator and Small Group Proposals

Proposals in this size class must specifically describe ambitious research goals and plans, and the anticipated workforce development contributions incorporated as an integral part of the proposed project.

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 contribute to realization of the CT vision.

Team proposals should describe plans for disseminating research results that go beyond traditional academic publications. Proposals should also describe education and workforce development contributions, including the anticipated 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 conducted at NSF's discretion.

B. Budgetary Information

Cost Sharing: Cost sharing is not required by NSF in proposals submitted to the National Science Foundation.

C. Due Dates

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

  January 08, 2007

  Second Wednesday in November, Annually Thereafter

D. FastLane/Grants.gov Requirements

- **For Proposals Submitted Via FastLane:**

  Detailed technical instructions regarding the technical aspects of preparation and submission via FastLane are 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.

  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. Further instructions regarding this process are available on the FastLane Website at: https://www.fastlane.nsf.gov/fastlane.jsp.

- **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. The Grants.gov's Grant Community User Guide is a comprehensive reference document that provides technical information about Grants.gov. Proposers can download the User Guide as a Microsoft Word document or as a PDF document. The Grants.gov User Guide is available at: http://www.grants.gov/CustomerSupport. In addition, the NSF Grants.gov Application Guide provides additional technical guidance regarding 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.

VI. NSF PROPOSAL PROCESSING AND REVIEW PROCEDURES

Proposals received by NSF are assigned to the appropriate NSF program and, if they meet NSF proposal preparation 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 who are experts in the particular fields represented by the proposal. These reviewers are selected by Program Officers charged with the 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 with the proposer.

A. NSF Merit Review Criteria

All NSF proposals are evaluated through use of the two National Science Board (NSB)-approved merit review criteria: intellectual merit and the broader impacts of the proposed effort. In some instances, however, NSF will employ additional criteria as required to highlight the specific objectives of certain programs and activities.

The two NSB-approved merit review criteria are listed below. 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 the reviewer 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?

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.

B. Review and Selection Process

Proposals submitted in response to this program solicitation will be reviewed by Adhoc Review 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.

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 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.

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 Officer. In addition, the proposer will receive an explanation of the decision to award or decline funding.

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 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 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 (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 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/general_conditions.jsp?org=NSF. 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 and other important information on the administration of NSF awards is contained in the NSF *Grant Policy Manual* (GPM) Chapter II, available electronically on the NSF Website at http://www.nsf.gov/publications/pub_summ.jsp?ods_key=gpm.

Special Award Conditions: To comply with section 16 of the Cyber Security Research and Development Act (15 U.S.C.A. 7410), the grantee will ensure that no grant funds go to:

1. any individual who is in violation of the terms of his or her status as a nonimmigrant; or
2. any alien from a country determined by the Secretary of State to be a state sponsor of international terrorism unless that individual has a visa permitting him or her to enter and remain in the United States.

The grantee must immediately notify NSF if its ability to receive nonimmigrant students or exchange visitor program participants has been suspended or terminated.

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 before the end of the current budget period. (Some programs or awards require more frequent project reports). Within 90 days after expiration of a grant, the PI also is required to submit a final project report.

Failure to provide the required annual or final project reports will delay NSF review and processing of any future funding increments as well as any pending proposals for that PI. 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. Such reports provide information on activities and findings, project participants (individual and organizational) 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. Submission of the report via FastLane constitutes certification by the PI that the contents of the report are accurate and complete.

VIII. AGENCY CONTACTS

General inquiries regarding this program should be made to:

- Karl Levitt, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: klevitt@nsf.gov
- David Du, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: ddu@nsf.gov
- Ralph Wachter, Program Director, 1175 N, telephone: (703) 292-8950, fax: (703) 292-9010, email: rwachter@nsf.gov
- Le Gruenwald, Program Director (Data Management Systems), 1125 S, telephone: (703) 292-8074, fax: (703) 292-9073, email: lgruenwa@nsf.gov
- William Steiger, Program Director, 1115 N, telephone: (703) 292-8910, fax: (703) 292-9059, email: wsteiger@nsf.gov

For questions related to the use of FastLane, contact:

- FastLane Help Desk, telephone: 1-800-673-6188; e-mail: fastlane@nsf.gov.
- Jamie Scipio, 1175 N, telephone: (703) 292-4675, fax: (703) 292-9010, email: jscipio@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.

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, MyNSF (formerly the Custom News Service)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 Regional 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. MyNSF also is available on NSF's Website at http://www.nsf.gov/mynsf/.

Grants.gov provides an additional electronic capability to search for Federal government-wide grant opportunities. NSF funding opportunities may be accessed via this new mechanism. Further information on Grants.gov may be obtained at http://www.grants.gov.

Investigators interested in the Cyber Trust program may also have interest in the following related NSF programs. Please note however that the NSF Grant Proposal Guide forbids the submission of duplicate proposals. Duplicate proposals will be returned without review.

- Networking Technology and Systems (NeTS)
- Computer Systems Research (CSR)
- Federal Cyber Service: Scholarships for Service
- Information and Intelligent Systems: Advancing Human-Centered Computing, Information Integration and Informatics, and Robust Intelligence

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 40,000 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 Antarctic research stations. The Foundation also supports cooperative research between universities and industry, US participation in international scientific and engineering efforts, and educational activities at every academic level.

Facilitation Awards for Scientists and Engineers with Disabilities provide funding for special assistance or equipment to enable persons with disabilities to work on NSF-supported projects. See Grant Proposal Guide Chapter II, Section D.2 for instructions regarding preparation of these types of proposals.

The National Science Foundation has Telephonic Device for the Deaf (TDD) and Federal Information Relay Service (FIRS) capabilities that enable individuals with hearing impairments to communicate with the Foundation about NSF programs, employment or general information. TDD may be accessed at (703) 292-5090 and (800) 281-8749, FIRS at (800) 877-8339.

The National Science Foundation Information Center may be reached at (703) 292-5111.

The National Science Foundation promotes and advances scientific progress in the United States by competitively awarding grants and cooperative agreements for research and education in the sciences, mathematics, and engineering.

To get the latest information about program deadlines, to download copies of NSF publications, and to access abstracts of awards, visit the NSF Website at 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: (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
Division of Administrative Services
National Science Foundation
Arlington, VA 22230