# Cyber Trust (CT)

## Program Solicitation

**NSF 06-517**
***Replaces Document* NSF 05-518**

**National Science Foundation**
Directorate for Computer and Information Science and Engineering
Division of Computer & Network Systems
Division of Computing & Communication Foundations
Division of Information and Intelligent Systems

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

March 06, 2006

First Monday in February Thereafter

## REVISIONS AND UPDATES

In furtherance of the President's Management Agenda, in Fiscal Year 2006, 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. A complete listing of these programs is available on the Policy Office website at: http://www.nsf.gov/bfa/dias/policy.

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:

A. Collaborative Proposals. All collaborative proposals must be submitted via the NSF FastLane system. This includes collaborative proposals submitted:

- by one organization (and which include one or more subawards); or
- as separate submissions from multiple organizations.

Proposers are advised that collaborative proposals submitted in response to this Program Solicitation via Grants.gov will be requested to be withdrawn and proposers will need to resubmit these proposals via FastLane. (Chapter II, Section D.3 of the Grant Proposal Guide provides additional information on collaborative proposals.)

B. All Other Types of Proposals That Contain Subawards. All other types of proposals that contain one or more subawards also must be submitted via the NSF FastLane system.

The following items are major revisions to the previous program solicitation:

1. The Center-scale category has been eliminated for the Fiscal Year 2006 solicitation. If the Center-scale category is added in Fiscal Year 2007, this solicitation will be revised.
2. Projects will be supported in three categories: (1) Exploratory Research projects, (2) Single Investigator or Small Group projects, and (3) Team projects.
3. Education-only proposals are not solicited. All proposals must have research and educational outreach components.

## SUMMARY OF PROGRAM REQUIREMENTS

### General Information

**Program Title:**

Cyber Trust (CT)

**Synopsis of Program:**

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 operation, corrupt valuable data, or expose private information. Future systems will include “sensors and computers everywhere”, exacerbating the attainment of security and privacy. Current security practices largely address current and known threats, but there is a need for research to take account of future threats.

Cyber Trust promotes a vision of a society in which networked computer 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 to 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
- effectively integrate the study of technology with the policy, economic, institutional and usability factors that often determine its deployment and use.

Proposals funded will cover a broad range of disciplines contributing to the Cyber Trust vision. Projects will be supported in three categories: Exploratory Research projects, Single Investigator or Small Group projects, and Team 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):**

- Karl Levitt, 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: klevitt@nsf.gov
- Darleen L. Fisher, 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: dlfisher@nsf.gov
- Brett D. Fleisch, 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: bfleisch@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
- Guru Parulkar, 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: gparulka@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
- Le Gruenwald, Program Director (Data Management Systems), Directorate for Computer & Information Science & Engineering, Division of Information and Intelligent Systems, 1125 S, telephone: (703) 292-8930, fax: (703) 292-9073, email: lgruenwa@nsf.gov
- Sol Greenspan, Program Director, Directorate for Computer & Information Science & Engineering, Division of

Computing and Communication Foundations, 1108 N, telephone: (703) 292-8910, fax: (703) 292-9059, email: sgreensp@nsf.gov

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

- 47.070 --- Computer and Information Science and Engineering

## Eligibility Information

- **Organization Limit:**

  Proposals may only be submitted by U.S. academic institutions or non-profit research institutions with a strong educational component. NSF FFRDCs may also submit proposals. For-profit organizations and government laboratories of other agencies may not apply directly; they may receive subcontracts, but such subcontracts should be justified by explaining what unique capability is being made accessible.

- **PI Eligibility Limit:** None Specified.
- **Limit on Number of Proposals:** An individual may appear as PI, co-PI, Senior Personnel, or Consultant on no more than two proposals submitted to each annual Cyber Trust competition.

## Award Information

- **Anticipated Type of Award:** Standard or Continuing Grant or Cooperative Agreement
- **Estimated Number of Awards:** 40 to 55 - Up to 15 team awards, and up to 20 single investigator and small team awards, and up to 20 exploratory research awards will be made, dependent on availability of funds
- **Anticipated Funding Amount:** $30,000,000 in FY 2006 pending availability of funds. Similar amounts are anticipated to be available in future fiscal years.

## Proposal Preparation and Submission Instructions

### A. Proposal Preparation Instructions

- Full proposals submitted via FastLane:
  - Grant Proposal Guide (GPG) Guidelines apply
- 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) To obtain copies of the Application Guide and Application Forms Package: click on the Apply tab on the Grants.gov website, 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.

### 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 Date(s)** (due by 5 p.m. submitter's local time):
  March 06, 2006
  First Monday in February Thereafter

## Proposal Review Information

- **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, 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 factors, to economic factors in that often security-enhancements can increase the ownership cost of systems and reduce performance, to policy decisions and to the inability of human administrators to manage complex systems. For example, it is exceedingly difficult to reason about the behavior of a complex digital system, particularly about its ability to withstand attacks. It is an art to design usable control interfaces for complex systems. Specifications and designs often neglect security and 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 often dictates having bundled software distributions that include vulnerable functions many users may not need or be aware. The data and technology needed to understand the range and severity of security problems and to evaluate the effectiveness of alternative solutions are lacking or closely held. Finally, the consequences of insecure system designs are borne by individuals and organizations that use them rather than by 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. Future systems, leading to the anticipated world of ubiquitous and pervasive computing, will have computers and sensors everywhere, thus providing ever-increasing openings for attack. 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 about their reliance on these systems.

- *People can justifiably rely on a well-trained and diverse workforce to develop, configure, modify, and operate essential 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 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:

- Advances in knowledge and technology. This need motivates basic research on ways to make computing systems more secure. 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. Improved education of both 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 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 now missing in the security field.
- Innovative approaches 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 must be considered in aspects of the entire 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 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 security 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.

**Security for Applications**

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—determine trustworthiness requirements. In some cases, lower system layers can achieve these requirements on behalf of the applications, but 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, networks and hardware. A better understanding is needed of how to make 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 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 can survive attacks without increasing the burden of managing the applications.

**Security for Computer Systems**

Computer systems are controlled by systems software that provides the basis on which applications are built, and 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 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 in a particular platform or 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, for example, transaction processing, wireless and sensor systems, fault-tolerant systems and real-time systems; and
- virtualization mechanisms to support separation of processes, with the 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. Sample research areas are concerned with the following hardware enhancements

- Security co-processors to support critical security functions such as intrusion detection and the encryption of storage;
- 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. Patching and retrofitting the networks today can work in the short term for some kinds of threats, but will not solve the growing security needs. NSF in its Networking Technology and Systems (NeTS) Future Internet Design (FIND) focus area (http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=12765&org=CNS) has initiated an initiative to design a "Future Internet" from core functionalities with the objectives of security and robustness, manageability, utility and social needs, new computing paradigms, integration of new network technologies, higher-level service architectures, and new theories of network architecture. Research is needed not only to improve the security of the current Internet; but also to help design the Future Internet with building-in security and robustness 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 new 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 necessarily size-limited testbeds (e.g. DETER/EMIST);
- Designing mechanisms that enable socially aware trade-offs in security and privacy;
- Design principles for secure network services and protocols that will yield network structures much more secure than current structures;
- 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;
- Artificial diversity to reduce the exposure of networks to scripted attacks.

**New Security Foundations**

The Cyber Trust program is also interested in research that establishes a sound scientific foundation and technological basis for computing and communications in a world that may include malicious actors. Results of fundamental research 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.

The attainment of security for complex systems will require 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.

**Education and Workforce Synergy Components**

To develop, maintain, and enhance the critical Cyber Trust educational infrastructure, all proposals must include an educational synergy component. The Cyber Trust Program seeks educational synergy components that will build the national capacity to educate the Cyber Trust experts needed to design, develop, manage, and operate secure systems of the future. All proposals must specifically describe their education synergy contributions, including the planned benefits and impact of the activities.

Educational synergy components may take many forms. However, there should be a strong research basis for synergy projects and Cyber Trust research faculty must participate. Educational synergy components should be natural extensions of the research activity and not simply detached activities. Collaboration between researchers and educators are encouraged. Innovation and clear vision and linkage to the current state of Cyber Trust research are essential.

**Award Categories**

Awards will be made in three categories: Exploratory Research Awards, Single Investigator or Small Group awards, and Team awards. Projects In the Exploratory Research category are supposed to be fresh starts that aim at developing new expertise or formulating new research and education directions; completion of these projects will position the PIs to prepare proposals for larger projects. The Single Investigator or Small Group awards are expected to be small scale, focused, and intensive. Team awards support intensive research and education activities undertaken by teams of researchers and educators. Team projects should focus on challenging Cyber Trust problems that may cross disciplinary boundaries.

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

**Organization Limit:** Proposals may only be submitted by U.S. academic institutions or non-profit research institutions with a strong educational component. NSF FFRDCs may also submit proposals. For-profit organizations and government laboratories of other agencies may not apply directly; they may receive subcontracts, but such subcontracts should be justified by explaining what unique capability is being made accessible.

**PI Eligibility Limit:** None Specified.

**Limit on Number of Proposals:** An individual may appear as PI, co-PI, Senior Personnel, or Consultant on no more than two proposals submitted to each annual Cyber Trust competition.

## IV. AWARD INFORMATION

Awards will support projects working within a broad range of disciplines contributing 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.

- Exploratory Research awards last up to 2 years and do not exceed $250,000 total.
- Single Investigator and Small Group awards last up to 3 years and do not exceed $500,000 total.
- Team awards last up to 4 years and do not exceed $2,000,000 total.

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

In unusual circumstances, the Cyber Trust program will entertain proposals that are beyond the scope and funding levels noted elsewhere 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 cross CISE divisions or, even involve funding from U.S. Government agencies beyond NSF. PIs who have in mind such a project must first contact the appropriate Cyber Trust program officers 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. It is recommended that the initial contact take place with the primary program officer, Karl Levitt via email at klevitt@nsf.gov.

## V. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS

### A. Proposal Preparation Instructions

**Full Proposal 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 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/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 announcement/solicitation number in the program announcement/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:

A. Collaborative Proposals. All collaborative proposals must be submitted via the NSF FastLane system. This includes collaborative proposals submitted:

   - by one organization (and which include one or more subawards); or
   - as separate submissions from multiple organizations.

   Proposers are advised that collaborative proposals submitted in response to this Program Solicitation via Grants.gov will be requested to be withdrawn and proposers will need to resubmit these proposals via FastLane. (Chapter II, Section D.3 of the Grant Proposal Guide provides additional information on collaborative proposals.)

B. All Other Types of Proposals That Contain Subawards. All other types of proposals that contain one or more subawards also must be submitted via the NSF FastLane system.

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 should begin with an acronym that identifies the category 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."

**Exploratory Research Proposals**

Proposals in this size class must specifically address the new innovative approach to be addressed in the research and the education and workforce development advances that could be an outgrowth of the project. The planned benefits and impact of the activities, even if long range, should be described.

**Individual Investigator and Small Group Proposals**

Proposals in this size class must specifically describe their integrated research and education and workforce development contributions. Proposals that offer research with innovative educational synergy are welcome in this award category.

**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 team 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.

## B. Budgetary Information

**Cost Sharing:**

Cost sharing is not required by NSF in proposals submitted under this Program Solicitation.

## C. Due Dates

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

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

March 06, 2006

First Monday in February Thereafter

## D. FastLane/Grants.gov Requirements

- **For Proposals Submitted Via FastLane:**

  Detailed technical instructions for proposal 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 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/

- **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. 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.

## 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 proposers whether their proposals have been declined or recommended for funding within six months. The time interval begins on the closing date of an announcement/solicitation, or the date of proposal receipt, whichever is later. 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 are administered in accordance with NSF Cooperative Agreement Financial and Administrative Terms and Conditions (CA-FATC). 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.

Consistent with the requirements of OMB Circular A-16, *Coordination of Geographic Information and Related Spatial Data Activities*, and the Federal Geographic Data Committee, all NSF awards that result in relevant geospatial data must be submitted to Geospatial One-Stop in accordance with the guidelines provided at: www.geodata.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/publications/pub_summ.jsp?ods_key=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/.

*These documents may be accessed electronically on NSF's Website at http://www.nsf.gov/awards/managing/. Paper copies of these documents may be obtained from the NSF Publications Clearinghouse, telephone (703) 292-7827 or by e-mail from pubs@nsf.gov.

**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 PI must submit an annual project report to the cognizant Program Officer at least 90 days before the end of the current budget period.

Within 90 days after the expiration of an award, the PI also is required to submit a final project report. 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:

- Karl Levitt, 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: klevitt@nsf.gov
- Darleen L. Fisher, 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: dlfisher@nsf.gov
- Brett D. Fleisch, 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: bfleisch@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
- Guru Parulkar, 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: gparulka@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
- Le Gruenwald, Program Director (Data Management Systems), Directorate for Computer & Information Science & Engineering, Division of Information and Intelligent Systems, 1125 S, telephone: (703) 292-8930, fax: (703) 292-9073, email: lgruenwa@nsf.gov
- Sol Greenspan, Program Director, Directorate for Computer & Information Science & Engineering, Division of Computing and Communication Foundations, 1108 N, telephone: (703) 292-8910, fax: (703) 292-9059, email: sgreensp@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.

For questions related to the use of FastLane, contact:

- Joan Goetzinger, Staff Assistant for Integrative Activities, Directorate for Computer & Information Science & Engineering, Division of Computer and Network Systems, 1175 N, telephone: (703) 292-8188, fax: (703) 292-9030, email: jgoetzin@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 MyNSF News Service (http://www.nsf.gov/mynsf/) to be notified of new funding opportunities that become available.

CAREER proposals that address Cyber Trust research and education issues 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, IGERT, and GK-12.

Other NSF programs welcome proposals that address security. This year's Research in Networking and Technology Systems (NeTS) (NSF 06-516) program welcomes proposals that offer innovative and unique approaches to the "new" architectures that offer security and resiliency not possible with current networking structures. If the proposal addresses primarily network architectural features, then it should be submitted to NeTS. On the other hand, if the proposal addresses the security aspects of the new mechanisms, their evaluation with respect to security requirements, or the management of the networks to address security policies, then the proposal can be submitted to Cyber Trust. PIs unsure of the appropriate program best suited for their proposal should contact a cognizant NSF program officer.

This year's Computer Systems Research (CSR) (NSF 05-629) program welcomes proposals that offer innovative approaches to computer system design, evaluation and usability with impact on four topical areas: Embedded and Hybrid Systems, Parallel and Distributed Operating Systems, Advanced Execution Systems, System Modeling and Analysis. Proposals in the area of computer systems that address new features in general, one of which is in support of security, should be submitted to CSR. On the other hand, if the proposal addresses primarily security requirements, or their implementation and evaluation, then the proposal should be submitted to Cyber Trust. PIs unsure of the appropriate program best suited for their proposal should contact a cognizant NSF program officer.

## 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
- **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.