Cyber Trust (CT)

Program Solicitation
NSF 08-521

Replaces Document(s):
NSF 07-500

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):

March 24, 2008

December 09, 2009

Second Wednesday in December, 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:

People depend on computers and communication, ranging from the networks for electronic mail, to systems

that monitor the nation's critical infrastructure, to embedded RFID devices for tracking in transportation systems. These systems are expected to work and work as intended without placing people at needless risks. Unfortunately, vulnerabilities still exist that allow attackers to corrupt or commandeer systems, including those that provide support for critical societal infrastructure. Moreover, many systems are vulnerable to actions 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 substantial benefits for society and individuals; yet, unless trust in computing and communications can be assured, these benefits are at risk.

The NSF Cyber Trust (CT) program promotes a vision of a society where trust enables technologies to support individual and societal needs without violating confidences and exacerbating public risks. It is a vision of cyber space that is supportive of our basic principles of fairness and safe information access. The goal of the NSF CT program is to develop new insights and fundamental scientific principles that lead to software and hardware technologies on which people can justifiably rely.

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, strengthen the foundations of cyber trust, and advance cybersecurity technologies;
- Define cyber trust broadly to include security, privacy, dependability, reliability, and usability;
- Address trustworthiness at all levels of system design, implementation, and use;
- Begin to integrate the technology produced by the research community, for example through novel security architectures;
- Consider social, economic, organizational and legal factors influencing cybersecurity;
- Validate theory through analysis, formal verification, experimentation and rigorous measurement;
- Explore innovative new concepts anticipating advances in technology and society;
- Encourage international collaborations; and,
- Educate and train a diverse workforce in cybersecurity and software technologies.

Proposals funded will cover a broad range of disciplines contributing to the CT vision. Four types of CT projects will be supported, as defined below.

- Exploratory Research projects typically explore new and untested ideas, have budgets of up to $200,000 total, and have durations of up to 2 years;
- Single Investigator and Small Group projects typically involve 1-2 PIs and their students, have budgets of up to $500,000 total, and have durations of up to 3 years;
- Medium projects demonstrate an active collaboration that brings together 2 or more PIs with complementary expertise to explore a common research problem, have budgets of up to $1,500,000 total, and have durations of up to 3 years; and,
- Large projects must focus on achieving a common goal or set of goals, articulate an effective collaboration and management plan, have budgets of up to $3,000,000 total, and have durations of up to 3 years.

Cognizant Program Officer(s):

- Karl Levitt, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: klevitt@nsf.gov
- David Du, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: ddu@nsf.gov
- Jim French, Program Director, Division of Information and Intelligent Systems, 1125S, telephone: (703) 292-8930, fax: (703) 292-9073, email: jfrench@nsf.gov
- Richard Beigel, Program Director, Division of Computing and Communication Foundations, 1115N, telephone: 703-292-8910, fax: (703) 292-9010, email: rbeigel@nsf.gov
- Kevin Thompson, Program Director, Office of Cyberinfrastructure, 1160N, telephone: 703-292-8962, fax: (703) 292-9010, email: kthompso@nsf.gov
- Ralph Wachter, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: rwachter@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: 87 total. Up to 2 Large awards, up to 15 Medium awards, up to 60 Single Investigator and Small Group awards, and up to 10 Exploratory Research awards will be made, dependent on availability of funds.

Anticipated Funding Amount: $34,000,000 in FY 2008 pending availability of funds.

Eligibility Information

Organization Limit:

None Specified

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. An individual may appear as PI, co-PI, Senior Personnel or Consultant on **no more than three proposals** submitted in total to the following NSF programs in each fiscal year: Cyber Trust (CT), Computer Systems Research (CSR), and Networking Technology and Systems (NeTS).

Proposal Preparation and Submission Instructions

A. Proposal Preparation Instructions

- **Letters of Intent:** Not Applicable
- **Preliminary Proposal Submission:** Not Applicable
- **Full Proposals:**
  - Full Proposals submitted via FastLane: NSF Proposal and Award Policies and Procedures Guide, Part I: Grant Proposal Guide (GPG) Guidelines apply. The complete text of the GPG is available electronically on the NSF website at: http://www.nsf.gov/publications/pub_summ.jsp?ods_key=gpg.
  - Full Proposals submitted via Grants.gov: NSF Grants.gov Application Guide: A Guide for the Preparation and Submission of NSF Applications via Grants.gov Guidelines apply (Note: The NSF Grants.gov Application Guide is available on the Grants.gov website and on the NSF website at: http://www.nsf.gov/bfa/dias/policy/docs/grantsgovguide.pdf)

B. Budgetary Information

- **Cost Sharing Requirements:** Cost Sharing is not required under this solicitation.

- **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):

  March 24, 2008

  December 09, 2009

  Second Wednesday in December, Annually Thereafter

Proposal Review Information Criteria

Merit Review Criteria: National Science Board approved criteria. Additional merit review considerations apply. Please see the full text of this solicitation for further information.

Award Administration Information

Award Conditions: Standard NSF award conditions apply

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

TABLE OF CONTENTS

I. INTRODUCTION

Computers permeate our world, ranging from networks for all forms of communication to systems designed for monitoring the nation's critical infrastructure to devices for tracking transportation systems, such as airplanes, trains, buses and even private cars. While some systems have been hardened against attack, in many areas, especially systems that control critical infrastructures, the potential remains for attackers to corrupt or commandeer such systems. The systemic vulnerabilities are due to many factors, including: errors in software or in configuration, ill-informed policies that do not account for all hazards, economic restrictions that inhibit the development of appropriate defenses against attacks and misuse, and sheer technical problems that have so far resisted resolution.

Many problems stem from factors of software engineering and attempts to retrofit security measures onto systems. In the extreme, legacy systems must be re-engineered to protect them against security attacks that were not envisaged when those systems were initially designed. Even in modern development regimens, the time and cost required for security certification and performance evaluations is prohibitively high. In the realm of security policies, many issues at the enterprise-wide level are not well understood. The fact that security components are notoriously non-compositional means that policies must be crafted at the overall system level, rather than built up or reasoned about incrementally. Hence, in a complicated, multi-tiered system, security policies must be devised for each level, and the overall system then checked to ensure that lower level policies integrate properly with those at higher levels.

Privacy, anonymity, and accountability in cyberspace are often debated on both technical and policy grounds. The objectives of privacy, anonymity and accountability often conflict with each other and need to be adapted in changing environments. Information has tangible value and real costs. That value depends in part upon the exercise of control and ownership over information and the perceived importance of that information. Its costs depend at least upon storage, bandwidth and processing. Information can also be erroneous, hidden, misused, misrepresented, partial, unverified, conflicting, and certainly personal. Many problems arise from differences in assumptions, expectations, feasibility, and actual use by different stakeholders. Whatever policies on information in cyberspace prevail will have significant impact upon society, commerce, defense, and the individual.

Over the next few decades, computing will be dramatically reshaped. Early trends suggest a greater convergence of software-enabled technologies with a wider diversity and presence of applications that build upon a large number of sensors, embedded devices and physical systems integrated through the Internet. In addition to advances in classical computing, functioning quantum devices capable of algorithm processing are expected to be common. Service-oriented architectures may gain a prominent place in the delivery and distribution of differentiated, yet composable, software services. Social networks and information content will be more important to the public and the research community. Critical infrastructures will be bound more closely via our information infrastructure. Unfortunately, convergence and closer integration often introduce new security vulnerabilities. Furthermore, security needs will be different and solutions will have to keep pace with technological advances, mitigating vulnerabilities and weaknesses before they manifest.

The challenges alluded to above promote a need for innovative research ideas driven by newly emerging technologies, new applications that impose new security and privacy requirements, and the ever increasing demand for more people knowledgeable about security.

Cyber Trust Program Vision

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 and communication systems to perform all functions but especially critical functions correctly, safely, and securely despite disruptions of any types;
- Information that is secure, protected, and properly managed everywhere at all times; and
- A diverse, well-trained workforce in cybersecurity and a general public educated in the ethical and secure use of computer technology.

II. PROGRAM DESCRIPTION

Trustworthiness is a system property. Many factors influence how trustworthy systems are designed, implemented, and used. Accordingly, CT covers all aspects of trust in computing and communication, including the social, legal, organizational, and economic factors. To make progress towards the CT vision requires:

- **New fundamental advances in knowledge and technology**. Of particular interest are projects that seek to explore new and innovative approaches, beyond existing ones, to address the growing complexity of security challenges. Focus on security evaluation and privacy is encouraged.

- **Trustworthiness at all levels of system design, implementation, and use**. Of particular interest are projects which take a holistic approach to security, focusing on new and innovative activities that provide for analysis, attribution, measurement and assurance at scale.
- **Security shaped by economic, ethical, legal, organizational, social, technical and usability factors.** Of particular interest are projects that address security and its usability within a technical, economic, ethical and legal framework. Projects which consider legacy systems in the approach to the solution are encouraged.
- **A well-trained and educated workforce and an informed public on information security**. Of particular interest are projects that capitalize upon the unique interests of academia, industry, and government - including accreditation and certificate granting institutions, community libraries, and the media - in the development of an informed, trained and educated cybersecurity workforce and citizenry. Activities that reach a broad community are encouraged.

Research Areas

Research supported will address: all security-related aspects of computer and network systems, including system evolution over time; development of security and privacy policies; definition of requirements; methodologies, models, and architectures that support security and privacy; construction, evaluation and verification of components and systems; operation, monitoring, maintenance, and recovery and reconstitution after failures or incidents; survivability and early discovery of large scale attacks; and forensics, sanitization, and disposal in the aftermath of an incident. Research that spans technical areas promoting effective integration of information technologies is strongly encouraged since many technologies are hampered by being "stand-alone". Accordingly, research focused on the integration of promising technologies into one or more evaluatable architectures is encouraged. CT is also interested in projects that 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 since 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 of the technical implications as well as the role of social, economic and other factors in developing trustworthy computer systems.

The following paragraphs elaborate upon some research challenges in CT areas of interest. ***They should be considered representative, not exhaustive.*** Research that is highly innovative and promises to set new directions for the security field, particularly reflecting future and skilled adversaries, is strongly encouraged.

Security for Software- and Data-Intensive Applications

Software-intensive applications are pervasive. Furthermore, recent developments in multi-core technology, coupled with the proliferation of web services, are ushering in new data-intensive services and applications. Increasingly society depends on these applications to interoperate correctly and securely in increasingly hostile environments. The desired level of security and trustworthiness must be weighed against the risks and costs of compromise, disruption, and performance impact. The CT program seeks new insights and understandings that ensure applications are trustworthy and that they interoperate in cyberspace. Research areas of interest include, but are not limited to:

- Security, trust and privacy in high interest applications (e.g., critical national infrastructures, healthcare, databases, mobile and sensor applications, data mining, web services, digital libraries, finance and banking, transportation, e-government, and e-commerce);
- Security and privacy for data-intensive applications, such as geospatial systems, and others, where the data itself impose unique security requirements and introduce trade-offs between security and performance;
- Security across federated or distributed systems;
- Knowledge integration and management within applications, especially for security;
- Authentication, access control, privacy control, and information flow management;
- Security policy specification, discovery, and implementation;
- Reasoning about and automatic abstraction and explanation of security policies;
- Transparency of trust, security, and privacy in and across applications;
- Cyber forensics for auditability, recovery and accountability in critical applications;
- Autonomous adaptation of applications to changes in threats and environments; and
- Survivability against massive attacks and wide spread disruptions.

Security for Computer Systems

Computer systems are controlled by (operating) systems software that governs behavior and provides basic services to computer resources on which applications are built. Large high performance servers and sensor networks alike are vulnerable to disruption and compromise. Many factors, including cost, time to market, complexity, power, and response-time

often inhibit the development of controls that might prevent system misuse and abuse. The purpose and use of a system, whether it is large or small, affects the type and extent of its security controls. New fundamental insights and approaches to trust and security are required for future generations of hardware processors, systems software and overall architectures. Research areas of interest include, but are not limited to:

- Trustworthy operating system architectures, including re-visiting separation kernels, hypervisors, and other operating structures that localize security-critical functionality;
- Trade-offs between generic systems that address many applications and systems specialized for an application (the concept of a family of secure operating systems that is subsettable to address particular needs can be considered);
- Virtualization mechanisms to support separation of processes with an emphasis on the evaluation of such mechanisms;
- Middleware for trustworthy systems in support of transaction processing, wireless and sensor systems, fault-tolerant systems, real-time systems and others;
- Access control for specialized operating systems such as those that support real-time and sensor -based systems;
- Special-purpose hardware modules for trustworthiness, accountability, and attestation (e.g., TPM security devices);
- Devices for authentication (e.g., biometric systems);
- Security co-processors to support critical security functions such as anti-tamper, tamper-resistance, intrusion detection, and the encryption of data;
- Security solutions that do not impact performance;
- Storage devices to support forensics and recoverability from attacks;
- Secure hierarchical control and trustworthy transaction processing for infrastructure systems; and
- Secure long-lived data archiving mechanisms.

Security for Networks

Research is needed to improve not only the security of the current Internet, but also to inform the design of future networks, including the future Internet, in which security and robustness are embedded from the ground up. Of particular interest are new protocols and network architectures that promise substantial security improvements. Research areas of interest include, but are not limited to:

- Building secure networks from insecure components (including novel designs for usable Byzantine security);
- Developing network security mechanisms to lead to networks (of all kinds, including infrastructure, wireless and sensor) that are resilient to denial of service attacks;
- Ensuring anonymity and accountability in networks, e.g., balancing attribute key-based pseudonymity with social requirements (revocable anonymity can be considered);
- Improving deployability and usability of network-based and network-disseminated security solutions;
- Enhancing network support for end-system security;
- Preserving security in federated systems especially after compromise and during recovery and repair;
- Developing new approaches to existing technologies that are secure (e.g. secure tunneling, secure plug-ins);
- Advancing the design of secure services and protocols involving middle boxes and proxies;
- Creating secure approaches to network functions such as addressing, routing, forwarding, naming, etc.;
- Evaluating the security of those networks which are too large to be faithfully represented on currently available, size-constrained testbeds (e.g. DETER/EMIST, WAIL, ORBIT);
- Designing mechanisms that enable trade-offs in security, privacy, need-to-know and need-to-share*;*
- Ensuring robust and secure network management and network substrates; and
- Development of security mechanisms for the security management of all network layers.

Security Foundations, Including Cryptography, Metrics and New Models

The CT program also supports research whose goal is to establish a sound scientific foundation and technological basis for reasoning about computing and communications in a world that includes malicious actors. Research results can be expected to have broad application, and are not limited to a particular platform or operating system. Research areas of interest include, but are not limited to:

- Cryptography, especially (1) cryptographic systems that are designed to be usable, (2) investigations towards stronger cryptographic systems, (3) proofs of cryptographic systems, including distributed protocols and of techniques that combine provable security with standard verification methods;
- Methods for specifying, reasoning about, and developing trustworthy components and systems, including novel hardware and firmware designs (of particular interest are lightweight methods to verification - such as static analysis - of program code and configuration files);
- Formal verification where different approaches (e.g., lightweight and theorem proving-based) operate synergistically;
- Maintaining trustworthiness as systems change and adapt;
- New mechanisms that provide quantifiable guarantees of trust (it might be necessary to initially address small and stand-alone components and protocols, building larger quantifiable systems from these);
- Metrics to enable the quantification of the security of a system or of 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;
- Methods to assure the trustworthiness of security features themselves;
- Methods to achieve trustworthiness in the presence of attacks more complex and disruptive than those currently observed;
- Synergistic combinations of static and dynamic evaluation methods;
- 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;
- Compositional security methods;
- Automatic generation of security configurations from policy specifications;
- Methods to assure that information flow in complex systems comply with security and privacy policies; and
- New models for security, such as control theory or models of social networks that offer the potential of providing new research directions.

Security for Complex Systems, Including New Security Architectures and Achieving Usable Security

For complex systems, attention must be given to all components that are subject to attack or that provide defenses and allow the management of attacks. Efficient security solutions for complex systems may require humans-in-the-loop. It is not possible to attain security by focusing attention, for example, on a single layer in a complex system organization. Research areas of interest include, but are not limited to:

- Aggregation of alerts across layers to enable accurate discrimination of attacks versus anomalous but not malicious activity, and also to enable effective cross-layer responses to attacks;
- Design principles for secure complex systems with human-in-the-loop, including providing humans with automatically derived explanations of security events and addressing other approaches towards security measures that are human-friendly;
- Prediction of the possible paths of a complex attack in progress and determination of possible remediation actions against such attacks;
- Efficient management of security mechanisms across a complex system, for example to derive configurations from a security policy;
- Security mechanisms that promote usability appropriate to the needs and skill level of each class of user, e.g., operator, administrator, forensic expert, "home" user;
- Dynamic dispatching of security-enhancement actions; and
- Security architectures that integrate security technologies that are currently largely stand-alone.

Privacy, Confidentiality, and Identity in Cyber Trust

Communication in cyberspace requires that some degree of identity be established, possibly revealing personal information. As sensor networks and web services become more pervasive, collection and inference of personal information becomes easier, bringing about new challenges to privacy preservation. The challenge then becomes to balance security issues against privacy concerns. Research areas of interest include, but are not limited to:

- Naming schemes;
- Information hiding, anonymity and accountability;
- Trust-modulated transparency;
- Group identity and individual identity;
- Privacy-enabling/disabling technologies;
- Privacy policy monitoring;
- Privacy and privacy-related metrics;
- Integrated flexible security solutions combining both trust and privacy;
- Formal logics languages, models and methods for specifying and reasoning about privacy; and
- Transformation of sensitive data, for example to prevent its association with particular individuals, without loss of the utility of the data for research purposes. Transformation methods that are generic but also application-dependent are of interest, as are methods to reason about the ability of the transformation methods to preserve utility but prevent the disclosure of sensitive data.

Long-Range Research in Cyber Trust Driven by Newly Emerging Technology and New Environments

Over the next 20 years computing will change dramatically. New technology that will support – or thwart -- security and privacy must be anticipated. New applications which will impose new and more challenging security requirements must be envisioned.

Pervasive computing will be the norm. Views of privacy, anonymity, accountability, and personal data will change as society and the individual adapt to life in cyberspace. Mobility, location-aware, RFID, and ad hoc networking will change how people respond to and recover from natural disasters. The Internet itself may fragment into a collection of distinct Internets with different protocols and constituencies. Software-enabled technologies will continue to make inroads into the medical device

field, which will change medical practices. Increased trust in computing, communications, and security will be essential for the success and adoption of pervasive computing.

All of these point to a need for reinventing the foundations of security and trustworthiness to accommodate the expected changes over the next 20 years. In the case of quantum information sciences, a new theory of computing that combines classical and quantum computing in a new paradigm would enable reasoning about each in a common framework and about interoperations between classical and quantum computing systems. For the Internet, a new theory of the "Internet as a computational device" could be advanced that allows reasoning about how computations on the Internet evolve. The mathematics and logics that have served well as models of sequential and concurrent computation will have to be augmented with new theories that support reasoning about computations where threads spontaneously evolve in response to other, spontaneous computations, and in which control is diffuse. These few examples among many raise challenging issues about security, trustworthy computing, and about the most basic notion of "What is a computation?"

- A common framework for reasoning about security in quantum and classical computing
- Control of computational interactions in dynamically evolving networks
- Extension of sequential and concurrent computational models to new computing paradigms
- Scalable provable security of cooperating systems
- Trust implications of convergence of information technology with biological systems

Research Prototyping, Experimental Deployment, and Measurement

Research proposals enhancing the usability of testbeds for cybersecurity experimentation and measurement are encouraged. Topics include, but are not limited to:

- Data set acquisition, collection, anonymization and associated tools;
- Parameterized data sets enabling dynamic and adaptive use and replay;
- Testing methodologies;
- The synergism among simulation, emulation and analytical methods, particularly as related to the accurate analysis of complex systems in a resource-limited testbed; and
- Experimentation and measurement tools and techniques

Proposals in all topic areas may choose to address prototype development or experimental deployment phases in their research agenda. In addressing a prototype phase, proposals should describe development plans, anticipated capabilities, and schedule. Software prototypes are encouraged to be open source. Developers should use the open source definition by the Open Source Initiative.

In addressing experimental deployment, proposals are expected to target either a testbed or a production environment whose capabilities and characteristics are relevant and appropriate. A test and evaluation plan must be provided. Production networking environments with the potential to support an experimental deployment include Internet2 and the National LambdaRail (NLR), as well as international network connections and facilities supported in NSF's International Research Network Connections (IRNC) program.

Information on Current Research Infrastructure – Testbeds and Repositories

Proposals in all research areas may leverage existing cybersecurity and network research infrastructures as part of their proposed activities. This partial list of testbeds below as well as others may be considered for use in experimentation:

- **DETER**, the cyber defense technology experimental research network, testbed facility. See http://www.isi.deterlab.net/ for more information.
- **Emulab**, a network testbed, providing a wide range of environments in which to develop, debug, and evaluate systems. See http://www.emulab.net/ for more information.
- **ORBIT**, a research testbed for wireless networks, providing emulation and field trial capabilities. See http://www.orbit-lab.org/ for more information.
- **PlanetLab**, a global research network supporting the development of new network services with 817 nodes at close to 405 sites. See http://www.planet-lab.org/ for more information.
- **WAIL**, a network testbed at the University of Wisconsin, supporting in-situ and laboratory based network research and testing on a collection of commercial systems. See http://wail.cs.wisc.edu/ for more information.
- **PREDICT**, a protected data repository to assist in research for cyber defense technologies, products, models and strategies, which is to open soon. See https://www.predict.org/ for more information.
- **HPWREN**, a wireless research and education network. See http://hpwren.ucsd.edu for more information.

There are also numerous testbeds in industry today, supporting cybersecurity research. Industry partners, in some circumstances, may make such resources available to researchers.

International Collaborations

Proposals are welcome that request supplemental funding to support collaboration with principal investigators affiliated with foreign research universities or research institutions and funded by foreign government research organizations. Such proposals should request only funds to support travel of U.S. affiliated personnel to work with their foreign collaborators.

Additional Considerations for Proposers

- **Building Workforce Capacity**

  All CT projects must include educational components that develop, maintain, and enhance the cybersecurity educational infrastructure. These components should be natural extensions of the research activity, and fully engage CT investigators. Collaboration between researchers and educators is strongly encouraged. Educational innovation with a clear vision and linkage to the current state of CT research are essential. Particularly encouraged are innovative classes or activities that transition research into educational material that is made available to a broad education community and which has the potential to interest new students in security and privacy.

- **Proposal Preparation Guidance**

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

III. AWARD INFORMATION

Four types of awards will be supported:

- Exploratory Research awards will last up to 2 years, with budgets not to exceed $200,000 total. In FY 2008, CISE expects to select for award up to 10 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 2008, CISE expects to select for award up to 60 projects in this category.
- Medium awards may last up to 3 years, with budgets not to exceed $1,500,000 total. In FY 2008, CISE expects to select for award up to 15 projects in this category.
- Large awards will last up to 3 years, with budgets not to exceed $3,000,000. In FY2008, CISE expects to select for award up to 2 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:

None Specified

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. An individual may appear as PI, co-PI, Senior Personnel or

Consultant on **no more than three proposals** submitted in total to the following NSF programs in each fiscal year: Cyber Trust (CT), Computer Systems Research (CSR), and Networking Technology and Systems (NeTS).

Additional Eligibility Info:

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 Medium proposal = CT-M
- Cyber Trust Large proposal = CT-L

For example, a Cyber Trust Medium proposal might have a title such as "CT-M: 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.

Medium Proposals

Proposals in this size class must describe substantial and ambitious research and education projects to focus a team of researchers and educators on either a particularly challenging technical area or to address important multidisciplinary challenges that contribute to realization of the CT vision.

Medium 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 a Medium-scale effort is required.

Large Proposals

Large projects promote synergy among academic, industrial and other partners. Proposals must address the combined needs for in-depth or multidisciplinary research investigations, education and workforce development, and incorporation of research results into deployed products and systems that lead to the realization of the Cyber Trust vision. Project descriptions for Large projects are limited to 18 pages, including: up to 15 pages total for the Research Plan, Education and Outreach Plan, and the Effective Partnership and Technology Transfer elements; and up to three pages total for the Management and Evaluation Plan elements.

The project description for a Large proposal must incorporate five main elements:

- Research Plan: Describe the research objectives of the project, objectives that bring diverse scientific, engineering, and other disciplines together to address fundamental research issues crucial to achieving the Cyber Trust vision. Provide a detailed research plan with a timeline for the activities proposed.
- Education and Outreach: Describe activities designed to (1) create a culture in which graduate and undergraduate students of diverse backgrounds work in cross-disciplinary teams, in close collaboration with external partners; (2) integrate education and research and expose students to the integrative aspects of Cyber Trust-related systems and industrial practice to build competence for their future careers; (3) develop curriculum innovations derived from the activity's goals; and/or (4) produce graduates with the depth and breadth of education needed to sustain leadership throughout their careers. Large projects will include one or more community-extending concepts such as creative undergraduate education activities; programs to address the under-representation of women and minorities in the Cyber Trust workforce; links to institutions with strong traditions of teaching, mentoring, and workforce development; or participation by institutions in EPSCoR states.
- Effective Partnership and Technology Transfer: Describe activities designed to develop and sustain strong partnerships between academic and other partners. Activities may involve collaboration with partners in industry, including service industries, public agencies, or government laboratories. Partners may be involved through integral activities such as participation in strategic planning, joint research, mentoring students, and supporting proof-of-concept testbeds—-all modes that strengthen the partnership and speed technology transfer. Describe the intellectual foundation for partners to collaborate with faculty and students to address both long-range and shorter-term challenges, producing the knowledge needed to ensure steady advances in technology and to speed their transition to the marketplace, while training graduates who are more effective in their subsequent careers.
- Management Plan: Describe the management and coordination of the proposed activities. The plan must identify the Project Director responsible for leading the activity and administering the award in accordance with the terms and conditions of the Award Letter issued by the NSF in the event of an award. In addition, it should address the following needs:
    - A central point of communication with NSF,
    - Management of project activities,
    - Coordination of technology transfer activities,
    - Fulfillment of educational and workforce development responsibilities, and
    - An Advisory Board of outside experts to advise the Director.
- Evaluation Plan: Specify evaluation methods that will support assessment of both research results and the effectiveness of education and workforce development activities.

B. Budgetary Information

Cost Sharing: Cost sharing is not required under this solicitation.

C. Due Dates

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

  March 24, 2008

  December 09, 2009

  Second Wednesday in December, 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, original, or potentially transformative 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?

Examples illustrating activities likely to demonstrate broader impacts are available electronically on the NSF website at: http://www.nsf.gov/pubs/gpg/broaderimpacts.pdf.

NSF staff will give careful consideration to the following in making funding decisions:

Integration of Research and Education
One of the principal strategies in support of NSF's goals is to foster integration of research and education through the programs, projects, and activities it supports at academic and research institutions. These institutions provide abundant opportunities where individuals may concurrently assume responsibilities as researchers, educators, and students and where all can engage in joint efforts that infuse education with the excitement of discovery and enrich research through the diversity of learning perspectives.

Integrating Diversity into NSF Programs, Projects, and Activities
Broadening opportunities and enabling the participation of all citizens -- women and men, underrepresented minorities, and persons with disabilities -- is essential to the health and vitality of science and engineering. NSF is committed to this principle of diversity and deems it central to the programs, projects, and activities it considers and supports.

Additional Review Criteria:

For Cyber Trust Large proposals only, reviewers will be asked to provide specific comments on the following areas:

- Research: Comment on the extent to which the project brings diverse scientific, engineering, and other disciplines together to address fundamental research issues crucial to achieving the Cyber Trust vision;
- Education and Outreach: Comment on the degree to which the proposed education and outreach activities meet the objectives described in the solicitation;
- Partnership and Technology Transfer: Comment on the quality and potential impact of the partnership and technology transfer activities;
- Management and Evaluation Plans: Comment on the quality and likely effectiveness of the proposed Management and Evaluation Plans.

B. Review and Selection Process

Proposals submitted in response to this program solicitation will be reviewed by Ad hoc Review and/or Panel Review.

Reviewers will be asked to 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 *Award & Administration Guide* (AAG) Chapter II, available electronically on the NSF Website at http://www.nsf.gov/publications/pub_summ.jsp?ods_key=aag.

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.

Site visits for Cyber Trust Medium and Large awards may be conducted at NSF's discretion.

VIII. AGENCY CONTACTS

General inquiries regarding this program should be made to:

- Karl Levitt, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: klevitt@nsf.gov
- David Du, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: ddu@nsf.gov
- Jim French, Program Director, Division of Information and Intelligent Systems, 1125S, telephone: (703) 292-8930, fax: (703) 292-9073, email: jfrench@nsf.gov
- Richard Beigel, Program Director, Division of Computing and Communication Foundations, 1115N, telephone: 703-292-8910, fax: (703) 292-9010, email: rbeigel@nsf.gov
- Kevin Thompson, Program Director, Office of Cyberinfrastructure, 1160N, telephone: 703-292-8962, fax: (703) 292-9010, email: kthompso@nsf.gov
- Ralph Wachter, Program Director, Division of Computer and Network Systems, 1175N, telephone: (703) 292-8950, fax: (703) 292-9010, email: rwachter@nsf.gov

For questions related to the use of FastLane, contact:

- FastLane Help Desk, telephone: 1-800-673-6188; e-mail: fastlane@nsf.gov.
- Termia M. Millard, telephone: (703) 292-8950, email: tmillard@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
- Division of Information and Intelligent Systems: Advancing Human-Centered Computing, Information Integration and Informatics, and Robust Intelligence (Proposals that address these issues towards advancing security and privacy should be submitted to Cyber Trust.)
- Division of Computing and Communication Foundations: fundamental research in algorithms, computer architecture, programming languages and software engineering (Proposals that address security issues related to these areas can be submitted to Cyber Trust.)

A PI preparing a security-related proposal but unsure of what program to submit to should contact a program manager affiliated with Cyber Trust and/or a program manager affiliated with other CISE or NSF programs with interest in computer security and privacy.

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