

Secure and Trustworthy Cyberspace (SaTC) Program

December 2, 2011 webinar



National Priorities

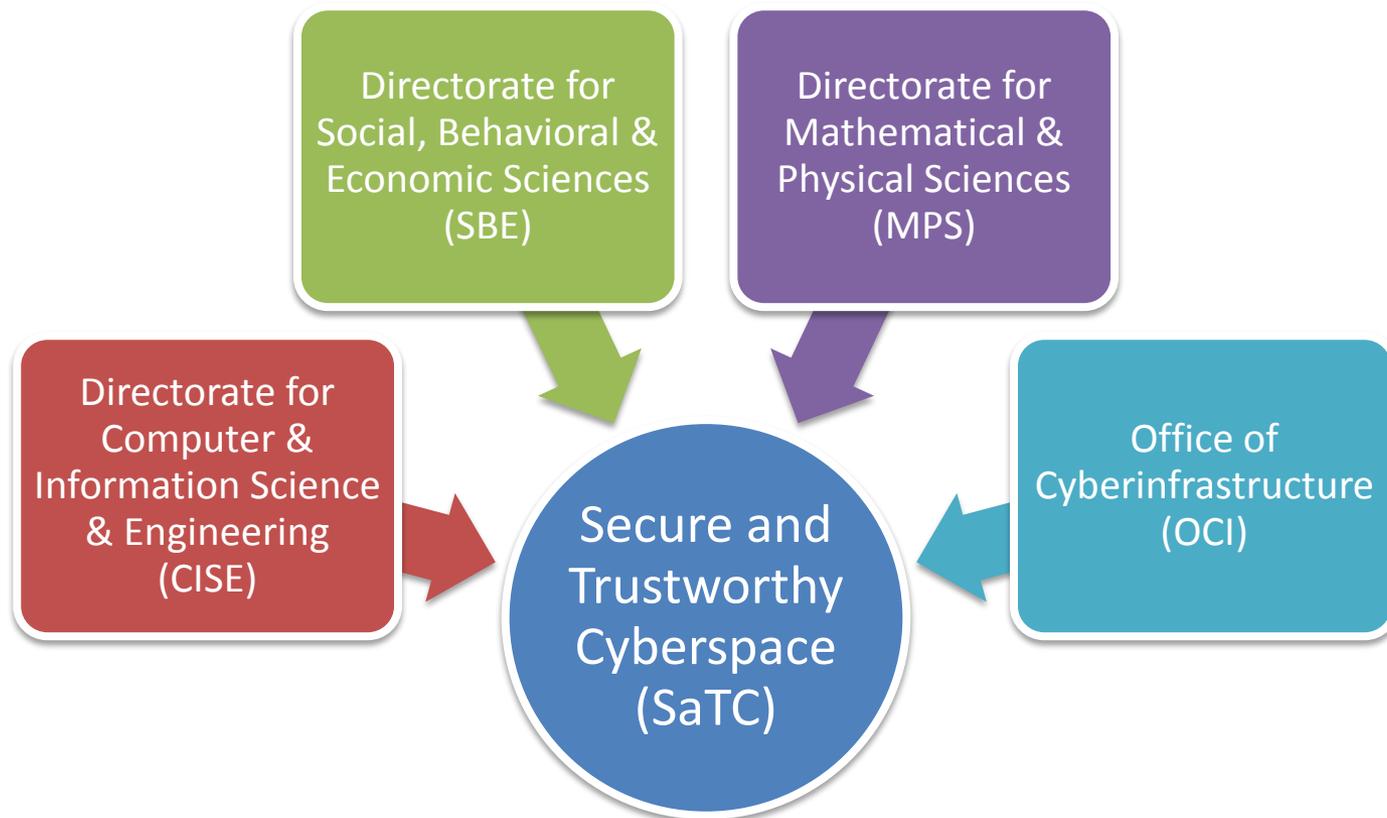
“America’s economic prosperity in the 21st century will depend on cybersecurity.”

President Obama, May 2009

- This pronouncement has ignited a national-level focus on cybersecurity and the need to maximize the impact of R&D on our cybersecurity posture.



Secure and Trustworthy Cyberspace Program (SaTC)



Agenda

1. Overview
2. SaTC Perspectives and Phases
 - a. Trustworthy Computing Systems
 - b. Social, Behavioral and Economics
 - c. Transitions To Practice
3. Program Procedures
4. Frontier awards
5. Other SaTC clarifications
6. Questions from the audience



SaTC Goals and Principles

To protect cyber-systems (including host machines, the internet and other cyber-infrastructure) from *malicious behaviour*, while preserving privacy and promoting usability

We recognize that cybersecurity is a *multi-dimensional problem*, involving both the strength of security technologies and variability of human behavior.

- We need the expertise and resources from a wide range of disciplines: e.g., computer scientists, engineers, economists, mathematicians, behavioural scientists



NSF Cybersecurity Activities Over Time



SaTC: Program Scope and Principles

Cast a wide net and let the best ideas surface, rather than pursuing a prescriptive research agenda

Engage the research community in developing new fundamental ideas and concepts

Promote a healthy connection between academia and a broad spectrum of public and private stakeholders to enable transition of innovative and transformative results



SaTC Perspective Goals

- Cybersecurity cannot be fully addressed by only technical approaches
- SaTC emphasizes different approaches and research communities by introducing *perspectives*
 - **Trustworthy Computing Systems (TC-S)**
 - **Social, Behavioral & Economic (SBE)**
 - **Transition to Practice (TtoP)**
- Each proposal must address at least one perspective



SaTC Perspectives

Programmatic Goals

- We encourage both single perspective and multi-perspective proposals:
 - We will not abandon the foundational research directions that have been fostered by Trustworthy Computing.
 - We instead wish to broaden the base.
- A successful multi-perspective proposal will most likely require a strong multi-disciplinary team.



Trustworthy Computing Systems Perspective

- Roughly corresponds to former Trustworthy Computing Program
 - Supports designing, building or operating cyber-infrastructure that resists malicious attackers
 - Includes security, privacy and accountability concerns
 - Supports approaches from theoretical to experimental to human-centric
 - Theories, models, algorithms, methods, architectures, languages, tools, systems and evaluation frameworks
 - Studies of tradeoffs among security, privacy, usability
 - Methods to assess, reason about and predict system trustworthiness
 - Methods to increase attacker cost, enable tailored security environments
- Other perspectives provide collaboration opportunities
- TC-S contacts: see list of CISE PDs on last slide, choose PD closest to topic



SBE Perspective

- The Social, Behavioral and Economic science (SBE) perspective concerns proposals that:
 - Have the potential to promote a safe and trustworthy cyberspace
 - Must *contribute* to, not merely *apply*, basic SBE science
 - Proposals that apply SBE science may fit as part of the Trustworthy Computing Systems (TC-S) perspective



SBE Perspective

- What counts as a “contribution”?
 - Develops new theories or methods that advance our understanding of the SBE sciences in the cybersecurity domain and that are generalizable to other domains as well
 - Any level of analysis (individual, group, organization, market, society, ...)
 - Any SBE methodology (theoretical, experimental, observational, statistical, survey, simulation, ethnographic,...)



SBE Perspective

- What counts as a “contribution”?
 - Given the fledgling state of the field, we are especially interested in proposals for workshops and intellectual engagements
 - Authors should clarify the possible, preferably broad, expected substantive SBE science contribution
 - Research conducted outside the U.S. is within scope
 - SBE Contact: Peter Muhlberger, pmuhlber@nsf.gov



Transition to Practice (TtoP) Perspective

- Supports later stage activities in the research and development lifecycle such as prototyping and experimental deployment
- Emphasis on activities that lead to potential impact on science and education environments – NSF cyberinfrastructure
- Review Criteria
 - Impact on deployed environment
 - Value in terms of needed capability and potential impact across the broad NSF community
 - Feasibility, utility, and interoperability in operation
 - Project plan including goals, milestones, demonstration and evaluation
 - Tangible metrics to evaluate effectiveness of capabilities developed



Transitions Phase

- Transition phase is an optional supplemental part to small and medium proposals going into other Perspectives only
- Similar in theme and types of activities to Transitions to Practice perspective
- TtoP Contact: Kevin Thompson,
kthompso@nsf.gov



Small

- up to \$500,000, up to 3 years duration
- Deadline: Jan 11, 2012

Medium

- up to \$1,200,000, up to 4 years duration
- Deadline: Jan 25, 2012

Frontier

- up to \$10,000,000, up to 5 years duration
- Deadline: Feb 22, 2012

Limit of 2 proposals per PI per year



Frontier Projects

- Previously CISE programs funded “Center-Scale” projects, such as:
 - Cybertrust Center for Internet Epidemiology and Defenses (CCIED)
 - Large-scale internet-based pathogens
 - Passive monitor for > 1% of routable Internet routable address space
 - Investigating economics of spam, how malware is monetized
 - ACCURATE
 - Ways in which technology can be used to improve voting systems and the voting process
 - Science that will help inform the election community and the public about the tradeoffs among various voting technologies and procedures
 - Resource to the elections community, politicians, vendors and the public about issues related to public policy, technology, and law with respect to voting
 - Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)
 - Architecture for end-to-end resilient, trustworthy and real-time power grid cyber-infrastructure
 - Included test bed combining power grid hardware and software with sophisticated simulation and analysis tools
 - Now transitioned to Department of Energy and Department of Homeland Security
- These efforts are now ending/transitioning



Frontier Project Goals

- Up to \$10 million/5 year projects
 - Cohesive effort that cannot be funded by collection of smaller awards
- Long-term vision
- In-depth or multidisciplinary research investigations
- Include education and workforce development and incorporate research results into deployed products and systems

- Restrictions:
 - Cannot be submitted solely to SBE perspective, but can be multi-perspective *including* SBE
 - Cannot have Transition Phase

- Strongly advise consulting with Program Director before submitting



SaTC: Mathematical and Statistical Challenges

Engage the Mathematical Sciences research community in developing new fundamental ideas and concepts that can assist in exposing vulnerabilities, detecting attacks and finding new secure methods that are, for example, quantum resistant.



Relationship with Core Programs

- SaTC is multi-disciplinary and overlaps with many CISE/SBE/OCI core programs
- Decide where to submit based upon
 - Research area that proposed work will impact, not on motivation or application
- Example: secure networking proposal
 - If will primarily advance networking -> NeTS
 - If will primarily advance security/privacy -> SaTC
- NSF program officers share/transfer proposals between programs to ensure best merit review, but advisable to carefully choose target program



SaTC Proposal Advice

- Make problem statement clear and relevant to SaTC
 - SaTC aim: “to protect cyber-systems”
 - State clearly what proposed work will protect *against*
 - Goals and abilities of “attacker”
 - Technical term: “threat model”



International Cooperation

- Ideas cross borders
- Attackers do not respect international borders
- Many centers of expertise isolated geographically, hindering research
- NSF and SaTC support international collaboration
 - Individual: supplements, support for collaboration: travel, visitors, workshops
 - If project needs co-funding with non-US agency, talk to Program Officer as soon as possible
 - General rule: NSF funds US participants, other agency funds non-US participants



SaTC Contacts

Computer & Information Science and Engineering	Networks and Systems	Sam Weber	sweber@nsf.gov
		Ralph Wachter	rwachter@nsf.gov
	Theory and Foundations	Sol Greenspan	sgreensp@nsf.gov
		Nina Amla	namla@nsf.gov
	Human-Centric and Artificial Intelligence	Vijay Atluri	vatluri@nsf.gov
Social, Behavioral & Economic Sciences		Peter Muhlberger	pmuhlber@nsf.gov
CyberInfrastructure		Kevin Thompson	kthomps@nsf.gov
Mathematical Sciences		Andrew Pollington	adpollin@nsf.gov

To sign up for the SaTC email list, send an email to listserv@listserv.nsf.gov with the text of the message being:

subscribe SaTC-Announce <your name>

For example: subscribe SaTC-Announce Jane Doe

