

Secure and Trustworthy Cyberspace (SaTC) Program

*Presentation to
DHS Software Assurance Forum*

Jeremy Epstein
Program Director
National Science Foundation

September 20, 2012





National Priorities

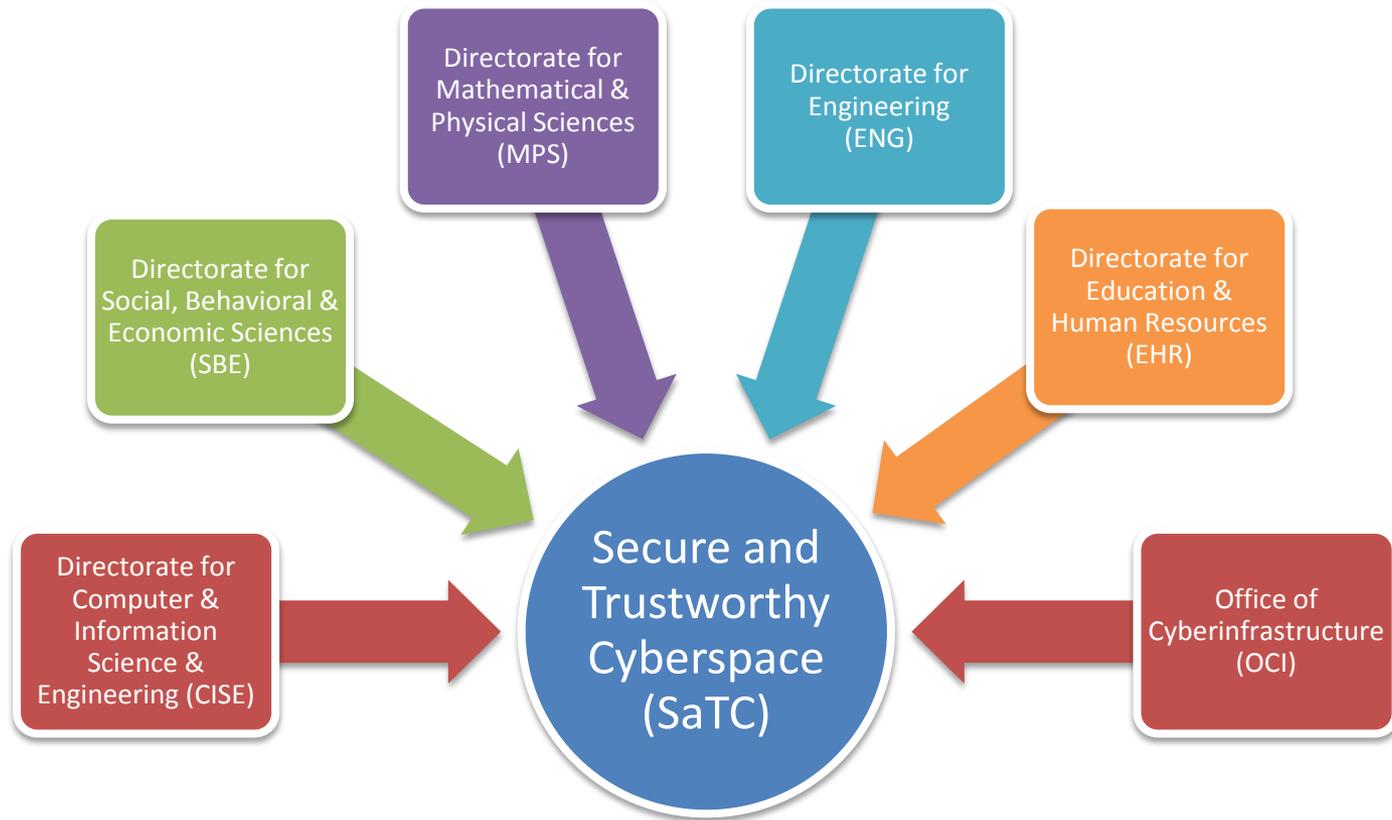
“America’s economic prosperity in the 21st century will depend on cybersecurity.”

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)



***Total budget about \$55M (FY12 actual),
\$75M (FY13 President's request to Congress)***





SaTC Goals and Principles

To protect cyber-systems (including host machines, the internet and other cyber-infrastructure) from *malicious behavior*, 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)**
 - **Cybersecurity Education**
- 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.



National Strategy Areas

3. Federal Cybersecurity Research and Development Program Thrusts .

1

3.1 Inducing Change

Designed-in Security

Tailored Trustworthy Spaces

Moving Target

Cyber Economic Incentives

3.2 Developing Scientific Foundations

3.3 Maximizing Research Impact

Supporting National Priorities

Engaging the Cybersecurity Research Community

3.4 Accelerating Transition to Practice

Technology Discovery

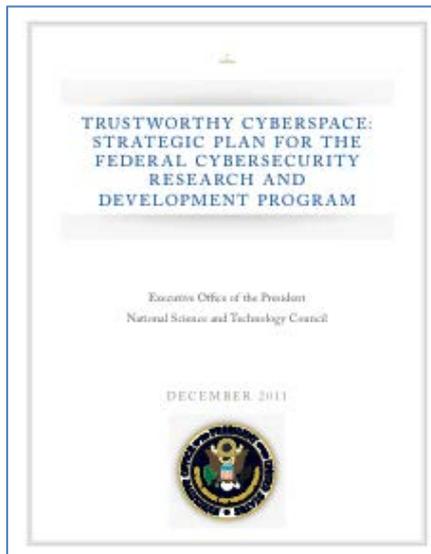
Test and Evaluation

Transition, Adoption, and Commercialization.



National Strategic Priorities in Cyber Security

- December 2011
- **“Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program”**



Cybersecurity R&D Themes Inducing Change	Designed-in Security	Tailored Trustworthy Spaces
	Moving Target	Cyber Economic Incentives

FY12 & FY13 Solicitation Language

Secure and Trustworthy Cyberspace (SaTC)

PROGRAM SOLICITATION NSF 12-596

REPLACES DOCUMENT(S): NSF 12-503



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

Directorate for Social, Behavioral & Economic Sciences
Division of Social and Economic Sciences

Directorate for Mathematical & Physical Sciences
Division of Mathematical Sciences

Office of Cyberinfrastructure

Directorate for Education & Human Resources
Division of Undergraduate Education

Directorate for Engineering
Division of Electrical, Communications

Submission Window Date(s) (due by 5 p.m. propose)

November 15, 2012 - November 30, 2012

MEDIUM Projects

December 01, 2012 - December 14, 2012

SMALL Projects

December 01, 2012 - December 14, 2012

CYBERSECURITY EDUCATION Projects

January 16, 2013 - January 30, 2013

FRONTIER Projects

“...research addressing how better to design into components and systems desired security and privacy properties...”

Trustworthy Computing Systems Perspective

Proposals addressing Cybersecurity with a Trustworthy Computing Systems perspective aim to provide the basis for designing, building, and operating a cyberinfrastructure with improved resistance and improved resilience to attack that can be tailored to meet a wide range of technical and policy requirements, including both privacy and accountability. Within its scope, the program supports all research approaches from theoretical to experimental, including participation by human subjects. Theories, models, cryptography, algorithms, methods, architectures, languages, software, tools, systems and evaluation frameworks are all of interest.

Of particular interest is research addressing how better to design into components and systems desired security and privacy properties. Methods for raising attacker costs by incorporating diversity and change into systems, while preserving system manageability, are also relevant.

Research that studies the tradeoffs among trustworthy computing properties, e.g., security and usability, or accountability and privacy, as well as work that examines the tension between security and human values such as openness and transparency is also welcomed. Also, methods to assess, reason about, and predict system trustworthiness, including observable metrics, analytical methods, simulation, experimental deployment and, where possible, deployment on live testbeds for experimentation at scale are considered. Statistical, mathematical and computational methods in the area of cryptographic methods, new algorithms, risk assessments and statistical methods in cybersecurity are also welcome.



How NSF Selects Grants

“NSF's task of identifying and funding work at the frontiers of science and engineering is not a "top-down" process. **NSF operates from the "bottom up,"** keeping close track of research around the United States and the world, maintaining constant contact with the research community to identify ever-moving horizons of inquiry, monitoring which areas are most likely to result in spectacular progress and choosing the most promising people to conduct the research.”

<http://www.nsf.gov/about/how.jsp>

- NSF issues very broad solicitations for
 - U.S. academic institutions, non-profit organizations, companies
- NSF enables the growth of scientific communities in areas of national importance



How Much for Designed-In Security?

Fiscal Year 2010

- 40% of awards (by cost)
- \$22.3M total

Fiscal Year 2011

- 46% of awards (by cost)
- \$24.0M total



FY11 Designed-In Related Grants

Principal Investigator	University	Proposal Title
Foster/Walker	Cornell/Princeton	TC: Large: High-Level Language Support for Trustworthy Networks
Zhong Shao	Yale	TC: Medium: Making OS Kernels Crash-Proof by Design and Certification
Clark Barrett	New York University	TC: EAGER: Collaborative Research: Parallel Automated Reasoning
Daniel Bernstein	University of Illinois Chicago	TC: SMALL: Higher-Speed Cryptography
David Brumley	Carnegie-Mellon University	CAREER: Towards Identifying and Eliminating Exploitable Software Bugs
Hao Chen	UC at Davis	TC: SMALL: Designing New Authentication Mechanisms using Hardware...
Yevgeniy Dodis	New York University	TC: SMALL: The Design of Secure Hash Functions and Block Ciphers
Virgil Gligor	Carnegie-Mellon	CNS: EAGER: All Trust is Local: User-Oriented Trust Establishment
Wenke Lee	Georgia Tech	TC: SMALL: A Foundational & Practical Platform for Host Security Applications
Darrell Long	UC at Santa Cruz	TC: SMALL: LockBox: Enabling Users to Keep Data Safe
Jason Nieh	Columbia	TC: SMALL: Improving System Security through Virtual Layered File Systems
Patrick Traynor	Georgia Tech	CAREER: Protecting User Data on Lost, Stolen & Damaged Mobile Phones
Aviel Rubin	Johns Hopkins	TC: LARGE: Self Protecting Electronic Medical Records
Andrew Myers	Cornell	TC: MEDIUM: Higher-level Abstractions for Trustworthy Federated Systems
Patrick Schaumont	Virginia Tech	TC: MEDIUM: Foundations for Future On-chip Fingerprints
Scott Shenker	ICSI UC Berkeley	TC: SMALL: Practical Data Confinement
Roberto Tamassia	Brown	TC: LARGE: Collaborative: Towards Trustworthy Interactions in the Cloud
Jaideep Vaidya	Rutgers	TC: SMALL: Collaborative: Formal Analysis of Access Control Models & Extensions
Moshe Vardi	Rice	CNS: EAGER: Automated Synthesis for System Design





Small

- up to \$500,000, up to 3 years duration, 1-3 of TWC, SBE, TTP
- Deadline: Dec 14 2012

Medium

- up to \$1,200,000, up to 4 years duration, 1-3 of TWC, SBE, TTP
- Deadline: Nov 30 2012

Frontier

- up to \$10,000,000, up to 5 years duration, 1-3 of TWC, SBE, TTP
- Deadline: Jan 30 2013

Education

- up to \$300,000, up to 2 years duration, EDU *only*
- Deadline: Dec 14 2012

Limit of 3 proposals per PI per year,
2 from Small/Med/Frontier; 1 from EDU



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”

Who Can Apply?

- Mostly targeted at colleges/universities, including community colleges
- Non-profits also eligible
- Small businesses in some cases
- Large businesses can be subcontractors
- *See the NSF Grant Proposal Guide (GPG) for more details*



SaTC Contacts

Computer & Information Science and Engineering	Networks and Systems	Jeremy Epstein	jepstein@nsf.gov
		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	kthompso@nsf.gov
Mathematical Sciences		Andrew Pollington	adpollin@nsf.gov
Education and Human Resources		Victor Piotrowski	vp Piotrow@nsf.gov
Engineering		Zhi (Gerry Tian)	ztian@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**

