National Science Foundation
Directorate for
Computer & Information Science & Engineering (CISE)

Secure and Trustworthy Cyberspace (SaTC) Program Overview

Presented by Jeremy Epstein, Program Officer

The SaTC Team

Program Officers

- Nina Amla
- Chris Clifton
- Jeremy Epstein
- Sol Greenspan
- Anita Nikolich
- Victor Piotrowski
- Andrew Pollington
- Deborah Shands (Sep 8)
- Gerry Tian
- Ralph Wachter
- Heng Xu

Admin Staff

- Carl Anderson
- Cassandra Queen
- Richard Sheehey

SaTC Goals and Perspectives

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

- SaTC is interdisciplinary, encompassing 5 NSF directorates:
  - **CISE: Computer and Information Science & Engineering**
  - **SBE: Social, Behavioral and Economic Sciences**
  - **EHR: Education and Human Resources**
  - **MPS: Mathematical and Physical Sciences**
  - **ENG: Engineering**

- **Participation of the five directorates reflects multi-faceted/multi-disciplinary nature of cybersecurity R&D**

NSF

SaTC
Secure and
Trustworthy
Cyberspace

SaTC includes many pieces

- Base solicitation (old 13-578, new 14-599)
- NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy (CPS-Security) (14-571)
- Dear Colleague Letters
  - SaTC EAGERs Enabling New Collaborations Between Computer and Social Scientists (14-016) [deadline passed]
  - Research on Privacy in Today's Networked World (14-021)
  - Cybersecurity Education EAGERs - Pushing the Dimensions of the Domain (14-075) [deadline passed]
  - Special Guidelines for Submitting Collaborative Proposals under the US NSF/CISE/SaTC – US-Israel BSF International Opportunity (14-TBD) – new for FY15
- SaTC participates in
  - CAREER
  - CISE Research Initiation Initiative (CRII)
- Others still to come!

SaTC
Secure and Trustworthy Cyberspace

SaTC Base Solicitation

NSF

SaTC
Secure and
Trustworthy
Cyberspace

Overview

- Trustworthy Computing Systems (TWC)
  - Traditional computer science
- Social, Behavioral, and Economic (SBE)
  - Psychological, economic, behavioral, social, and political aspects of cybersecurity
- Cybersecurity Education (EDU)
  - Building workforce capacity

SaTC Base Solicitation – Major changes for FY15

- Replace Frontier (max $10M, 5 years) with Large (max $3M, 5 years)
  - Expect about 6
- Merger of STARSS solicitation into base (STARSS = Secure and Trustworthy Cyberspace: Secure, Trustworthy, Assured and Resilient Semiconductors and Systems)
- Submission windows:
  - Small: Jan 02 - Jan 14, 2015
  - Medium: Oct 27 - Nov 10, 2014
  - Large: Nov 12 - Nov 20, 2014
  - Education: Dec 04 - Dec 19, 2014
- http://www.nsf.gov/pubs/2014/nsf14599/nsf14599.htm?org=NSF

SaTC
Secure and Trustworthy Cyberspace

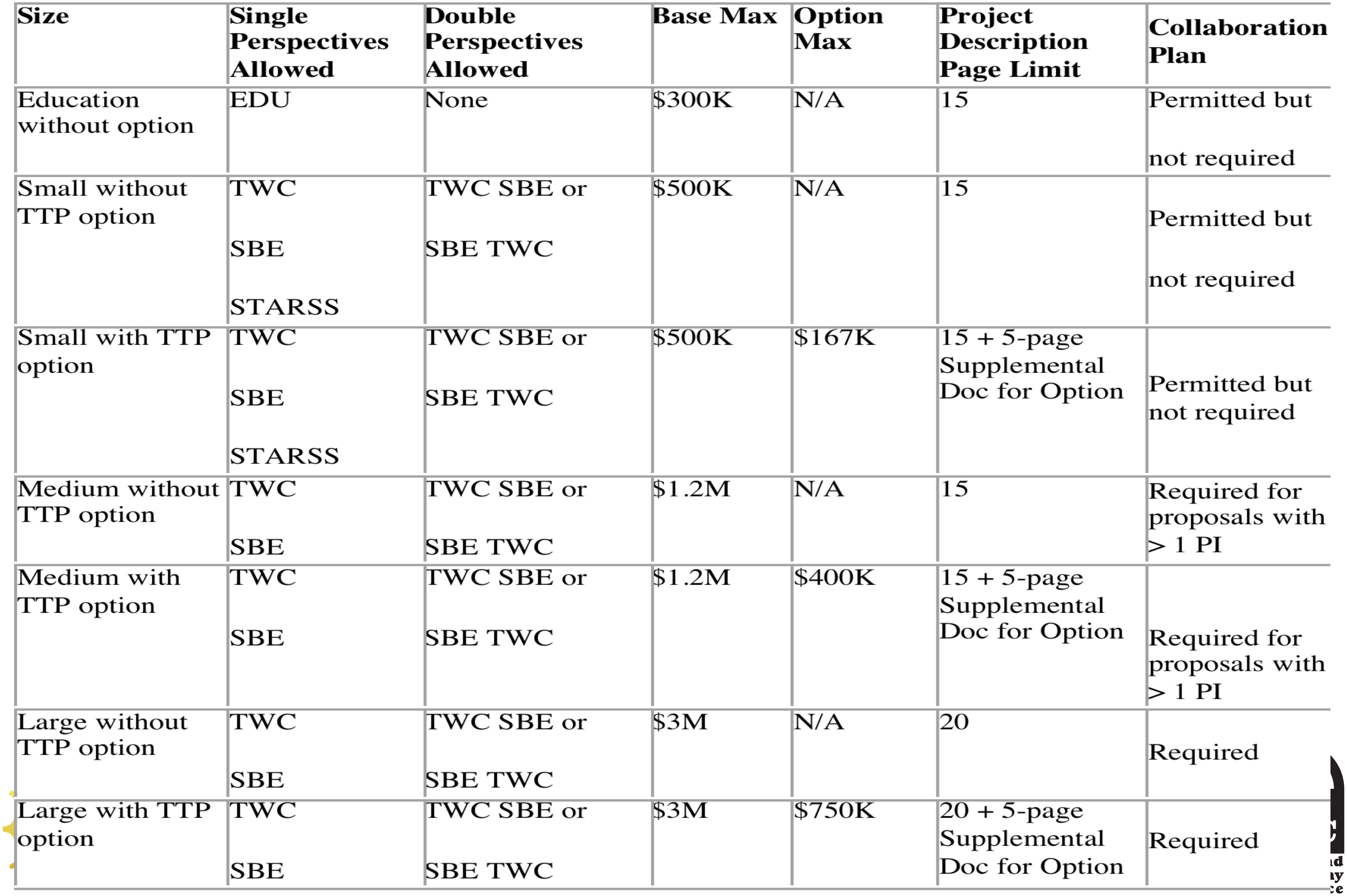
Sizes & Schedule

	Amount & duration	**Transition Option Permitted?**	**Submission window**	**# FY14 funded**
Small	Up to $500k, 3 years	Yes	Jan 02 2015 – Jan 14 2015	65 proposals/ 52 projects
Medium	Up to $1.2M, 4 years	Yes	Oct 27 2014 – Nov 10 2014	40 proposals/ 20 projects
Large	Up to $3M, 5 years	Yes	Nov 12 2014 – Nov 20 2014	(New)
Cybersecurity Education	Up to $300K, 2 years	No	Dec 04 2014 – Dec 19 2014	10 proposals/ 8 projects

NSF

SaTC
Secure and
Trustworthy
Cyberspace

SaTC Combinations



Size	Single Perspectives Allowed	Double Perspectives Allowed	Base Max	Option Max	Project Description Page Limit	Collaboration Plan
Education without option	EDU	None	$300K	N/A	15	Permitted but not required
Small without TTP option	TWC SBE STARSS	TWC SBE or SBE TWC	$500K	N/A	15	Permitted but not required
Small with TTP option	TWC SBE STARSS	TWC SBE or SBE TWC	$500K	$167K	15 + 5-page Supplemental Doc for Option	Permitted but not required
Medium without TTP option	TWC SBE	TWC SBE or SBE TWC	$1.2M	N/A	15	Required for proposals with > 1 PI
Medium with TTP option	TWC SBE	TWC SBE or SBE TWC	$1.2M	$400K	15 + 5-page Supplemental Doc for Option	Required for proposals with > 1 PI
Large without TTP option	TWC SBE	TWC SBE or SBE TWC	$3M	N/A	20	Required
Large with TTP option	TWC SBE	TWC SBE or SBE TWC	$3M	$750K	20 + 5-page Supplemental Doc for Option	Required

Trustworthy Computing Systems Perspective

Secure and Trustworthy Cyberspace

Trustworthy Computing Systems Perspective

- The “technical” part of cybersecurity (i.e., computer science research)
- 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

Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) Perspective

NSF

SaTC

Secure and
Trustworthy
Cyberspace

What is STARSS?

- Hardware security, with focus on *Design for Assurance*
- Joint effort of NSF and the Semiconductor Research Corporation (SRC)
  - Awards are co-funded between NSF & SRC
  - Proposals must include authorization to share with SRC
- See last year's STARSS webinar for lots more details
  - http://www.nsf.gov/events/event_summ.jsp?cntn_id=129985&org=CISE
- For Small proposals ONLY!

Social, Behavioral, and Economic Sciences Perspective

Wait for Heng’s turn

Cybersecurity Education Perspective

Wait for Victor’s turn

SaTC
Secure and
Trustworthy
Cyberspace

Transitions to Practice Option

Secure and Trustworthy Cyberspace

What is Transition to Practice?

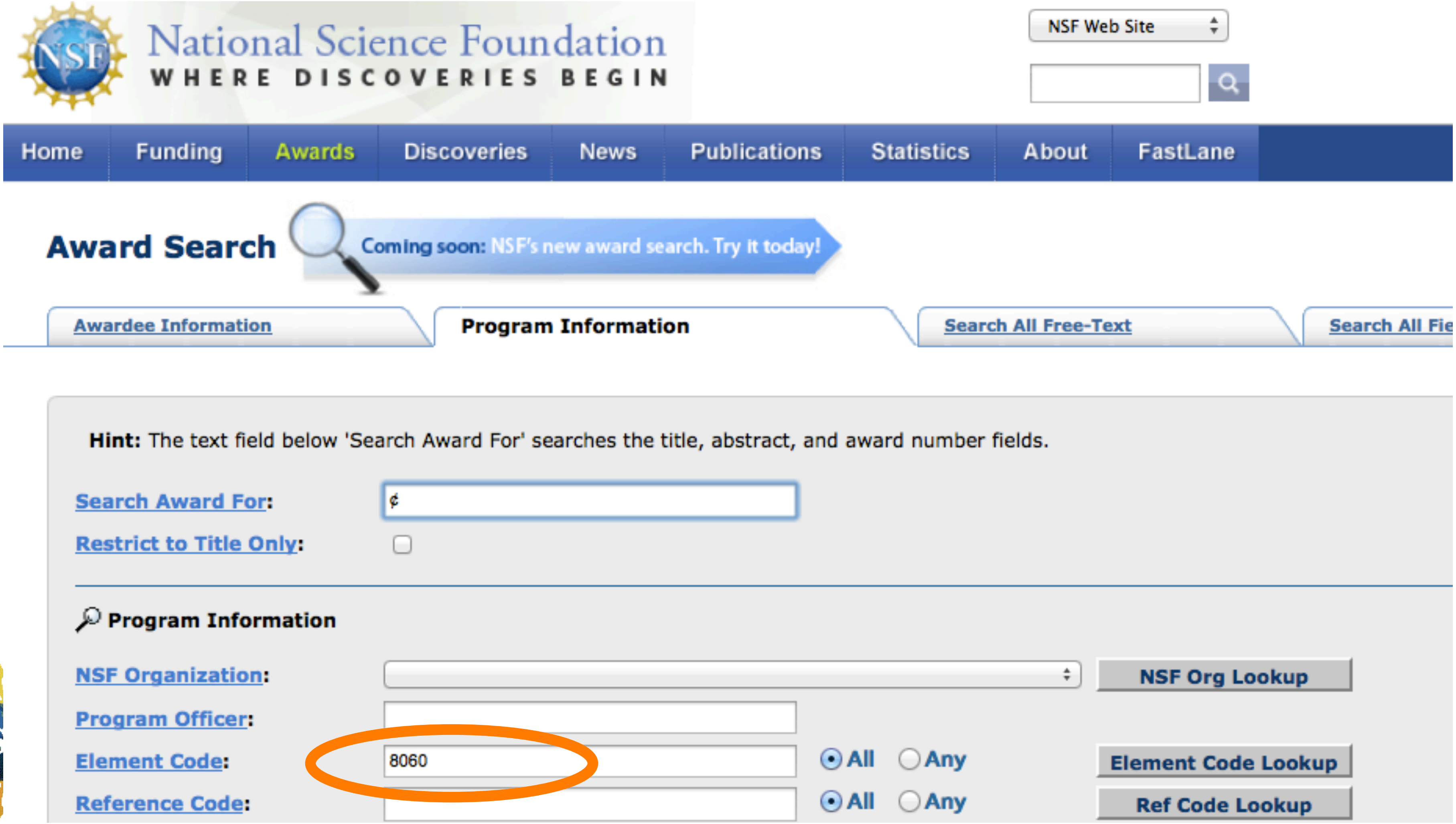
- Supports later stage activities in the research and development lifecycle such as prototyping and experimental deployment
- Emphasis on activities that lead to potential impact on science and education environments – NSF cyberinfrastructure
- Supplemental funding:
  - Small: up to $167,000
  - Medium: up to $400,000
  - Large: Up to $750,000
- Software developed must be released under an open source license
- Other opportunities for TTPs – During FY14, Department of Homeland Security (DHS) provided additional TTP funding in partnership with NSF

How do I get Transition to Practice?

- OPTION on the original proposal (Include **TTP Option:** in title)
  - Up to five page supplementary document
  - DO NOT discuss in the main body of the proposal
- Budget for option not included in regular budget
  - Discuss budget and how additional funds will be used in five page TTP option supplement
- Review Criteria:
  - Impact on deployed environment (experimental or operational)
  - 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
- *TTP option considered independently!*
  - TTP supplement not considered in ranking the research proposal

Does my research fit?

- Look on www.nsf.gov/awardsearch for what we've funded already!



Hint: The text field below 'Search Award For' searches the title, abstract, and award number fields.

Search Award For: ¢

Restrict to Title Only: □

Program Information

NSF Organization:

Program Officer:

Element Code: 8060 ● All ○ Any

Reference Code: ● All ○ Any

SaTC Actual FY14 Funding Areas (128 new research projects)

Access control
Anti-malware
Anticensorship
Applied cryptography
Authentication
Cellphone network security
Citizen science
Cloud security
Cognitive psychology
Competitions
Cryptographic theory
Cyber physical systems
Cybereconomics
Cyberwar
Digital currencies
Education
Forensics
Formal methods
Governance
Hardware security
Healthcare security
Insider threat
Intrusion detection
Mobile security
Network security
Operating systems
Personalization
Privacy
Provenance
Security usability
Situational awareness
Smart Grid
Social networks
Sociology of security
Software security
Vehicle security
Verifiable computation
Voting systems security
Web security

National Strategy Areas Where We'd Like To See More Proposals

- Underrepresented
  - Moving Target
  - Tailored Trustworthy Spaces
  - Science of Security
  - SBE beyond cybereconomics
  - Forensics

NSF

SaTC
Secure and
Trustworthy
Cyberspace

NSF/Intel Partnership on Cyber-Physical Systems Security and Privacy (CPS-Security) (14-571)

Secure and Trustworthy Cyberspace

Synopsis

- "Ideas lab" to develop concepts & teams held in DC area Aug 12-16 (by invitation)
- Full proposals due Oct 28 2014 (Ideas Lab participation NOT required)
- Two sizes:
  - Synergy (up to $3M/3 yrs, jointly funded by Intel & NSF)
  - Breakthrough (up to $500K/3 yrs, NSF only)
- Webinar June 30 @ 2pm-3pm Eastern (recorded) http://www.nsf.gov/events/event_summ.jsp?cntn_id=131795&org=CISE
- Solicitation at http://www.nsf.gov/pubs/2014/nsf14571/nsf14571.htm
- Total $8M funding

SaTC
Secure and Trustworthy Cyberspace

SaTC EAGERs Enabling New Collaborations Between Computer and Social Scientists (14-016)

SaTC

Secure and Trustworthy Cyberspace

New CISE/SBE Collaborations

- Goal: Start collaboration between computer scientists and social scientists <u>who have not previously worked together</u>
- Two phase process:
  - Submit white paper
  - If accepted, submit EAGER proposal (8 pages, up to $300K)
- 10 funded in FY13; 16 funded in FY14
- Stay tuned for future opportunities in this space; we'll post any updates to the SaTC-announce list

FY13 Awards

1343141	Zhu, Ye	Cleveland State U	EAGER: The Game Changer: A New Model for Password Security
1343258	Beyah, Raheem A.	Georgia Tech Res Corp	EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime
1343237	Wingfield, Adia Harvey	Georgia State U	EAGER: Collaborative: Winning the Internet Lottery: Growing Income Inequality, Social Class, and Susceptibility to Cybercrime
1343430	Aliari Zonouz, Saman	U of Miami	EAGER: Cybercrime Susceptibility in the Sociotechnical System: Exploration of Integrated Micro- and Macro-Level Sociotechnical Models of Cybersecurity
1343433	Egelman, Serge M.	International Computer Science Institute	EAGER: Designing Individualized Privacy and Security Systems
1343451	Peer, Eyal	CMU	EAGER: Designing Individualized Privacy and Security Systems
1343453	Chellappan, Sriram	Missouri U S&T	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343482	Holt, Thomas J.	Michigan State U	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343245	Bossler, Adam	Georgia Southern U	EAGER: Collaborative: A Multi-Disciplinary Framework for Modeling Spatial, Temporal and Social Dynamics of Cyber Criminals
1343766	Khan, Mohammad	U of Connecticut	EAGER: The Role of Emotion in Risk Communication and Warning: Application to Risks of Failures to Update Software
1347075	Milward, H. Brinton	U of Arizona	EAGER: Human-centric Predictive Analytics of Cyber-threats: a Temporal Dynamics Approach
1347113	Ho, Shuyuan M.	Florida State U	EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication
1347120	Hancock, Jeffrey T.	Cornell U	EAGER: Collaborative: Language-Action Causal Graphs for Trustworthiness Attribution in Computer-Mediated Communication
1347151	Garg, Vaibhav	Drexel U	EAGER: Cybercrime Science
1347186	Hong, Jason	CMU	EAGER: Social Cybersecurity: Applying Social Psychology to Improve Cybersecurity

SaTC

Secure and Trustworthy Cyberspace

FY14 Awards

1358723	Richard, Golden G.	U of New Orleans	EAGER: Integrating Cognitive and Computer Science to Improve Cyber Security: Selective Attention and Personality Traits for the Detection and Prevention of Risk
1359542	Yue, Chuan	U of Colorado Colorado Springs	EAGER: Investigating Elderly Computer Users' Susceptibility to Phishing
1359601	Nov, Oded	Polytechnic U of New York	EAGER: Exploring spear-phishing: a socio-technical experimental framework
1359632	Telang, Rahul	CMU	EAGER: Consumer Response to Security Incidences and Data Breach Notification: An Empirical Analysis
1444633	Coming soon!		
1444827	Coming soon!		
1444823	Coming soon!		
1444840	O'Brien, James F.	UC Berkeley	EAGER: Collaborative: Understanding How Manipulated Images Influence People
1444861	Shen, Cuihua	UC Davis	EAGER: Collaborative: Understanding How Manipulated Images Influence People
1444863	Coming soon!		
1444871	Coming soon!		
1444500	Coming soon!		
1445079	Coming soon!		
1450193	Howard, Philip N.	U of Washington	EAGER: Computational Propaganda and The Production/Detection of Bots
1450500	Coming soon!		
1450600	Coming soon!		
1450619	Coming soon!		
1450624	Coming soon!		
1450625	Coming soon!		

Research on Privacy in Today's Networked World (14-021)

Wait for Heng’s turn

Cybersecurity Education EAGERs - Pushing the Dimensions of the Domain (14-075)

Synopsis

- Goal: Encourage advances in cybersecurity education through collaborations between CS education researchers and cybersecurity researchers
- Up to $300K / 2 years
- Two phase process:
  - Submit white paper
  - If accepted, submit EAGER proposal (8 pages, up to $300K)
- New for FY15
- Submission deadline for first phase: Aug 1 2014
- Selections: Sep 1 2014
- Full proposals: Sep 30 2014
- Deadline passed for white papers
- Stay tuned for future opportunities in this space; we'll post any updates to the SaTC-announce list
- Details at http://nsf.gov/pubs/2014/nsf14075/nsf14075.jsp?org=NSF
- See also EDU perspective in base solicitation

Special Guidelines for Submitting Collaborative Proposals under the US NSF/CISE/SaTC – US-Israel BSF International Opportunity (14-TBD)

Secure and Trustworthy Cyberspace

Want to be a panelist on an NSF panel?

- *Good reasons to be a panelist*: Learn what makes a good proposal; serve the community with your expertise!
- *Bad reasons to be a panelist*: Money! (a few hundred $ + airfare for reviewing 8-10 proposals and spending 1-2 days in Arlington VA)
- Eligibility: faculty, industry, government, postdocs
- Non-US people can attend in person or by phone; expenses are paid but no honoraria
- Send a list of topic areas you're interested/qualified to review to jepstein@nsf.gov
- Can't review for the same program/size as you submit (e.g., if submit a SaTC Medium, can review SaTC Small but not SaTC Medium)
- No guarantee that you'll get selected, but we are always seeking qualified panelists

Jeremy Epstein

Secure and Trustworthy Cyberspace (SaTC) Program

Computer & Network Systems Division

jepstein@nsf.gov

+1 703-292-8338