
Re: Secure and Trustworthy Cyberspace (SaTC)

From : Rose Smyrski <smyrskir@uwplatt.edu> Fri, Aug 17, 2012 01:51 PM
Subject : Re: Secure and Trustworthy Cyberspace (SaTC)
To : William Hudson <hudsonw@uwplatt.edu>
Cc : Lisa A Riedle <riedle@uwplatt.edu>, Joseph Clifton <clifton@uwplatt.edu>, Philip Sealy <sealy@uwplatt.edu>, Robert W Roberts <robertsro@uwplatt.edu>, Sabina Burton <burtons@uwplatt.edu>, Center for New Ventures <newventures@uwplatt.edu>, cooleyde@uwplatt.edu, Jennifer M deCoste <decostej@uwplatt.edu>

Bill,
I started to respond right away to your email and it was tabled as I prepared for the Cabinet Retreat.

When this came across my desk, that was my thought exactly and the reason I included Sabina Burton in the initial email list, which by the way she too expressed interest in exploring this further.

Please let me know if I can help in any way, even if it is as simple as helping to coordinate the plenary meeting.

Rose

Rose Smyrski
Legislative Liaison
University of Wisconsin-Platteville
smyrskir@uwplatt.edu
(608) 342-1282

----- Original Message -----
From: "William Hudson" <hudsonw@uwplatt.edu>
To: "Joseph Clifton" <clifton@uwplatt.edu>, "Philip Sealy" <sealy@uwplatt.edu>, "Robert W Roberts" <robertsro@uwplatt.edu>
Cc: "Lisa A Riedle" <riedle@uwplatt.edu>, "Rose Smyrski" <smyrskir@uwplatt.edu>
Sent: Sunday, August 12, 2012 7:56:14 PM
Subject: Fwd: Secure and Trustworthy Cyberspace (SaTC)

I have to wonder if we could find opportunities in the investigation of cyber crimes??

----- Original Message -----
From: "Rose Smyrski" <smyrskir@uwplatt.edu>

To: "William Hudson" <hudsonw@uwplatt.edu>, "Kenneth M Wiegman" <wiegmake@uwplatt.edu>, "Michael S Sherer" <sherer@uwplatt.edu>, "Sabina Burton" <burtions@uwplatt.edu>
Sent: Friday, August 10, 2012 4:25:06 PM
Subject: Fwd: Secure and Trustworthy Cyberspace (SaTC)

Good afternoon,

I wanted to share with you the information from NSF with the thought you would review it and pass the information on to those that might be interested.

If I can be of assistance, please don't hesitate to ask.

Rose Smyrski

Rose Smyrski
Legislative Liaison
University of Wisconsin-Platteville
smyrskir@uwplatt.edu
(608) 342-1282

----- Forwarded Message -----

From: "National Science Foundation" <nsf-update@nsf.gov>
To: smyrskir@uwplatt.edu
Sent: Friday, August 10, 2012 2:49:32 PM
Subject: Secure and Trustworthy Cyberspace (SaTC)

NSF Program Announcements and Information for National Science Foundation Update. This information has recently been updated, and is now available.

Secure and Trustworthy Cyberspace (SaTC)

Available Formats:

HTML: http://www.nsf.gov/pubs/2012/nsf12596/nsf12596.htm?WT.mc_id=USNSF_25&WT.mc_ev=click

PDF: http://www.nsf.gov/pubs/2012/nsf12596/nsf12596.pdf?WT.mc_id=USNSF_25&WT.mc_ev=click

TXT: http://www.nsf.gov/pubs/2012/nsf12596/nsf12596.txt?WT.mc_id=USNSF_25&WT.mc_ev=click

Document Number: nsf12596

This is an NSF Program Announcements and Information item.

I. INTRODUCTION

Cyberspace - a global "virtual" village enabled by hyper-connected digital infrastructures - has transformed the daily lives of people for the better. Families and friends regardless of distance and location can see and talk

with one another as if in the same room. Cyber economies create new opportunities. Every sector of the society, every discipline, has been transformed by cyberspace. Today it is no surprise that cyberspace is critical to our national priorities in commerce, education, energy, financial services, healthcare, manufacturing, and defense.

The rush to adopt cyberspace, however, has exposed its fragility. The risks of hyper-connectedness have become painfully obvious to all. The privacy of personally identifiable information is often violated on a massive scale by persons unknown. Our competitive advantage is eroded by the exfiltration of significant intellectual property. Law enforcement is hobbled by the difficulty of attribution, national boundaries, and uncertain legal and ethical frameworks. All these concerns now affect the public's trust of cyberspace and the ability of institutions to fulfill their mission.

The National Science and Technology Council with the cooperation of NSF has put forth a 2011 report, (NSTC) Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program. The plan identifies a broad, coordinated research agenda to make cyberspace secure and trustworthy. Research in cybersecurity must "change the game," check the misuses of cyber technology, bolster education and training in cybersecurity, establish a science of cybersecurity, and transition promising cybersecurity research into practice. The goal is to make cyberspace worthy of the public's trust.

This solicitation is supportive of the NSTC strategic plan for a trustworthy cyberspace. It recognizes that cyberspace will continue to grow and evolve, and that advances in the sciences and technologies will create new "leap-ahead" opportunities expanding cyberspace. It recognizes that cybersecurity must also grow and co-evolve, and that a secure and trustworthy cyberspace will ensure continued economic growth and future technological innovation.

II. PROGRAM DESCRIPTION

Cybersecurity is arguably the most important challenge confronting society in the information age. No one - whether governments, businesses or individuals - is exempt from the ravages of malicious cyber acts upon imperfect technologies. Posing cyber conflict solely in terms of classic attackers and defenders shortchanges the diversity and subtlety of the motivations, incentives, ethics, asymmetries, and strategies of the constituent actors and players in cyberspace. The intelligent adversary, whether human or software, learns, evolves, and co-evolves to exploit, disrupt, and overpower with cyberspace. Addressing this challenge requires a coordinated multi-disciplinary approach, contributing to the body of knowledge on cybersecurity in the respective disciplines, and leading to practical usable deployable technologies.

This program welcomes proposals that address Cybersecurity from a Trustworthy Computing Systems perspective (TWC); a Social, Behavioral and Economic Sciences perspective (SBE); and a Transition to Practice perspective (TPP) (see below). In addition, we welcome proposals that integrate research addressing two or more of these perspectives as well as proposals focusing entirely on Cybersecurity Education (see below). Proposals may be submitted in one of the following three categories:

Small projects: up to \$500,000 in total budget, with durations of up to three years

Medium projects: \$500,001 to \$1,200,000 in total budget, with durations of up to four years

Frontier projects: \$1,200,001 to \$10,000,000 in total budget, with durations of up to five years

Projects with Trustworthy Computing Systems and/or Social, Behavioral and Economic Sciences perspectives may include a Transitions option, described in a supplemental document of no more than five pages. This document should describe how successful research results are to be further developed, matured, and experimentally deployed in organizations or industries, including in networks and end systems used by members of the NSF science and engineering communities. Proposals with a Transitions option may exceed the above-stated maximums up to \$167,000 for Small projects, \$400,000 for Medium projects and \$750,000 for Frontier projects.

In addition, the SaTC program seeks proposals addressing Cybersecurity Education with total budgets limited to \$300,000 and durations of up to two years. The announcement for a NSF I am forwarding this information to you
