NSF Secure and Trustworthy Cyberspace (SaTC) PI Meeting

National Harbor, MD
November 27-29, 2012

Good morning. On behalf of my colleagues at the National Science Foundation, I am pleased to welcome you to the first Secure and Trustworthy Cyberspace, or SaTC, Principal Investigators' meeting.

This meeting brings together more than 400 researchers, practitioners and thought leaders from academia, industry and the government sector. On a personal note, it is great to see so many colleagues, friends and collaborators at the event.

I'd like to take a few minutes to share with some thoughts on the SaTC program and our investments in this area.

This audience, of course, recognizes the significance of this area of exploration and its importance as not just a national priority, but also a global priority.

As automation and information technology pervade new platforms, cyber-enabled systems have become ubiquitous in our everyday lives and grow increasingly complex each year. The Nation's critical infrastructure, and, more generally, the Internet, play a vital role in tightly integrating the economic, political, and social fabric of society. These interdependencies leave the Nation vulnerable to a wide range of threats that challenge the security, reliability, availability, and overall trustworthiness of all information technology resources.

Technology adoption patterns will lead to a dramatic shift in the size, complexity and diversity of cyber attacks.

- Consider pervasive deployment of wireless networks, mobile devices, and social media platforms.
- Consider the barriers to adoption of cloud infrastructure.
- Consider automation and potential vulnerability of critical infrastructure, medical devices, SCADA system, automotive systems.
- Or, consider the proliferation of attacks spurred by financial gains or political motive.

Overcoming these challenges calls for long-term investments in a spectrum of scientific and technical areas in computer science, mathematics, economics, social and behavioral sciences, and education – and as a national priority, it requires participation from multiple Federal agencies.

Within this framework, the National Science Foundation has a long history of supporting fundamental research in cybersecurity. Over the last decade, through the:

- Trusted Computing,
- Cyber Trust, and
- Trustworthy Computing programs,

the CISE Directorate at NSF has funded key advances in this area.

Today, the SaTC program is seeking to build upon this success by enabling an interdisciplinary approach to cybersecurity.

Here's what is truly exciting about the program:

Last year, NSF's Directorates for Social, Behavioral, and Economic Sciences (SBE) and Mathematical and Physical Sciences (MPS), together with the Office of Cyberinfrastructure (OCI), partnered with CISE to expand the scope of the program. And with this year's solicitation, the Directorates for Engineering (ENG) and Education and Human Resources (EHR) have joined the SaTC program.

Working together, we are pursuing four underlying principles:

1. Uncover and address underlying cybersecurity research gaps, whereby it is important to focus on the root causes rather than just treating the symptoms.
2. Approach cybersecurity as a multi-dimensional problem, involving both the strength of security technologies and variability in human and institutional motivation and behavior.
3. Develop enduring cybersecurity principles that will allow us to stay secure despite changes in technology and evolution of threat environment: *a science of security.*
4. Ensure the "Right Science at the Right Scale" by casting a wide net to encourage more speculative research, and multiple perspectives including transition to practice.

As the scope of the SaTC program has expanded, so has the range of those involved. Let me share a couple of data points:

- There are approximately 600 active awards from SaTC and its legacy programs. For this last fiscal year alone (FY 2012), we have invested $65M in the SaTC program including over 90 new SaTC awards (35 small, 54 medium, and 2 frontier awards)*.

Furthermore, the EHR directorate will invest more than $45M in the scholarship for service program – directly aimed at booting the number skilled professionals in this area.

When you add up all the cybersecurity investments in various programs across NSF, we estimate a total investment of more $150M in 2013 FY.

Let me share a few thoughts on the agenda for the next two days:

The agenda for this week's meeting features keynote addresses that will help us understand the myriad perspectives and interests engaged in cybersecurity R&D. For example, in just a little while, you will hear from Google's Vice President for Security Engineering, Eric Grosse, about private sector's efforts in this space. Later this morning, University College London's Angela Sasse, a leading cybersecurity scholar in England, will provide an international perspective. And on Thursday, Stuart Firestein of Columbia University will inspire us with his vision of how the unknown is the true engine of science.

There will of course be various opportunities to discuss recent advances and brainstorm the many challenges that lie ahead including:

- panel discussions,
- poster sessions, and
- Birds of a Feather engagements.

I want to call your attention to one session in particular. This afternoon, senior representatives from several Federal agencies (including DHS, NIST, DoD, DNI and NSF) will discuss the Federal Cybersecurity R&D Strategic Plan. My colleagues will describe the plan in some detail – and also explore what comes next as part of an interactive dialogue – including emerging areas in cybersecurity research that may warrant further focus.

Just a few years ago, I sat as a PI as many of you today. Now as the head of the CISE directorate, I am excited by the advances from the wide range of cutting-edge interdisciplinary cybersecurity research and education activities over the years; the work that has been done has had tremendous impact on our society today. I am inspired by the new directions of the SaTC program, and I look forward to the expanding possibilities ahead as we build a cyber-secure society.

There are a number of people to thank for this excellent program. Let me first thank *you* for taking time out of your busy schedules to join us here over the next few days. I want to thank all of the organizers - in particular, Lance Hoffman and Carl Landwehr of George Washington University for putting together the program, and Frankie King and Katie Dey of Vanderbilt University for organizing all the logistics. I also want to thank all the NSF staff, especially Jeremy Epstein, for their tremendous efforts.

Now, it is my pleasure to introduce the Director of the National Science Foundation, Dr. Subra Suresh. Subra, a member of both that National Academy of Sciences and National Academy of Engineering, was nominated by President Barack Obama and confirmed by the U.S. Senate as the 13th director of NSF in September 2010. Prior to assuming his current role, Subra served as the dean of the School of Engineering and the Vannevar Bush Professor of Engineering at MIT. Under his leadership, NSF has launched a number of cross-Foundational initiatives, and Subra has played a leading global role to enhance international collaboration in science. I should add that Subra has been a huge advocate for the research led by our community – with his support, we have made SaTC a cross-foundation activity at NSF. Please join me in welcoming Dr. Subra Suresh to the stage.