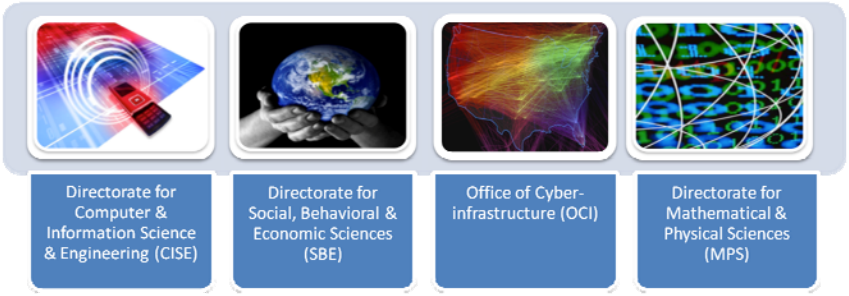
Secure and Trustworthy Cyberspace (SaTC)

Keith Marzullo
Division Director, Computer and Network Systems
CISE Directorate
National Science Foundation

Secure and Trustworthy Cyberspace Program (SaTC)

A* cross-directorate program *to address cybersecurity from one or more of three perspectives:
–Trustworthy Computing Systems
–Social, Behavioral and Economics
–Transition to Practice



SaTC Perspectives
Research Opportunities

Trustworthy Computing Systems	• Perspective aims to provide scientific basis for designing, building and operating cyber-infrastructure with improved resilience and resistance • Support for both theoretical and experimental approaches • Investigation of tradeoff among trustworthy properties
Social, Behavioral & Economic	• Perspective includes research at individual, group, organizational, market and societal levels, identifying risks and exploring solution feasibility • Understanding attack or defense behaviors to develop more effective strategies and solutions • Cyber economic incentives including metrics and models
Transition to Practice	• Perspective addresses the challenge of moving from research to practice • Focus on later stages of R&D activities including evaluation and experimental deployment • Software required to be released under open software license

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 pubic and private stakeholders to enable transition of innovative and transformative results

SaTC Programmatic Goals

Frontier Projects

- Earlier CISE programs had funded four center-scale awards with the goal of promoting synergy among academic, industrial and other partners:
  ACCURATE, CCIED, TCIP, SAFE
- In subsequent years, we created a large category to fund smaller in-depth/multidisciplinary efforts.
- Now that the original center-scale efforts are ending/transitioning, we wish to fund new efforts

SaTC: Research Principles
Where are the gaps?

1. We need to aim at understanding *underlying cybersecurity deficiencies:*
   - It is important to focus on *root causes* rather than just treating the symptoms
   - Identifying these fundamental causes may require an iterative approach, taking theory and prototypes to practice (e.g., cybersecurity in cyber-physical systems)
   - Can also be the basis of curiosity driven research (e.g., return oriented programming)

SaTC: Research Principles

2. 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: computer scientists, engineers, economists, mathematicians, behavioral scientists, ...
   - This will take work: collaboration across mature fields requires effort (e.g., "*trust*" from a social science perspective versus "*trustworthy*" from a computer science perspective)

SaTC: Research Principles

3. We need *enduring cybersecurity principles* that will allow us to stay secure despite changes in technology and threat environment: a *science of security*
   - Organize disparate areas of knowledge
   - Enable discovery of universal laws
   - Apply the rigors of the scientific method
   - Enhance capabilities to design, develop and evolve high assurance software and systems

SaTC: Research Principles

4. "Right Science at the Right Scale"
   - Cast a wide net to encourage more speculative research
   - Portfolio mix: small, medium and frontier projects
   - Multiple perspectives, including transition to practice