OneNSF INVESTMENTS
SECURE AND TRUSTWORTHY CYBERSPACE (SaTC)

OVERVIEW

The Secure and Trustworthy Cyberspace (SaTC) investment is aimed at building a cybersecure society and providing a strong competitive edge in the Nation's ability to produce high-quality digital systems and a well-trained workforce. Achieving a cybersecure society is a critical challenge in today's world, as corporations, agencies, national infrastructure, and individuals have been victims of cyber-attacks. These attacks exploit weaknesses in technical infrastructures and human behavior. Understanding the motivations and incentives of individuals and institutions, both as attackers and defenders, can aid in creating a more secure and trustworthy cyberspace. Addressing this problem requires multi-disciplinary expertise in statistical, mathematical, computational, economic, and computer sciences, and ultimately the transition of new concepts and technologies to practice.

Fundamental research in algorithms, models, probability theory, reliability, statistical theory and analysis, cryptanalysis, system structures, and secure computing is needed to stay ahead of new threats enabled by new technologies. The increasing power of computers implies that in the next era of computing many existing algorithms used to secure transmissions will no longer be robust or adequate. Research is needed in market mechanisms that can align incentives, hedge risks, and reduce the frequency and severity of attacks and that provides a deeper understanding of the social and behavioral factors that affect cybersecurity. Development and deployment of innovative cybersecurity models and practices throughout scientific environments, including research and education communities, to embed innovative curricula within these models and practice is also required. This research and development requires a well-trained professional workforce with new skills and knowledge, necessitating creative and innovative approaches to the education and preparation of tomorrow's cybersecurity researchers.

The 2010 President's Council of Advisors on Science and Technology (PCAST) report on Networking and Information Technology R&D (NITRD) and several National Academy of Sciences reports[1] have argued strongly for the need to increase U.S. cybersecurity research and development. The NITRD *Strategic Plan for the Federal Cybersecurity Research and Development Program* (released in December 2011) details four thrusts that together cover a set of interrelated priorities for the federal agencies that conduct or sponsor research and development in cybersecurity. These four thrusts are: (1) inducing change, which provides four game-changing research themes to direct efforts towards understanding the root causes of current threats, namely designed-in security, moving target defense, tailored trustworthy space, and cyber economic and behavioral incentives; (2) developing scientific foundations, which calls for the development of an organized, cohesive scientific foundation for the body of knowledge that informs the field of cybersecurity; (3) maximizing research impact, which aims to catalyze integration across the research themes, to increase cooperation between governmental and private-sector communities, to increase collaboration across international borders, and to protect critical infrastructure, such as Health IT and Smart Grid; and (4) accelerating transition to practice, which calls for focusing efforts on ensuring adoption and implementation of the new technologies that emerge from the research themes and scientific foundations, so as to create measureable improvements in the cybersecurity landscape.

Specific objectives of NSF's SaTC program, and how they relate to the four thrusts of the Federal Cybersecurity Strategic Plan, include:

[1] Reports available from http://sites.nationalacademies.org/CSTB/CSTB_059144

Inducing Change

- Focus the direction of research on four game-changing research topics – designed-in security, moving target defense, tailored trustworthy space, and cyber economic and behavioral incentives – to better understand the motivations, incentives, and behaviors of users, attackers, and defenders. For example, study how information flows within and between these groups, how organizations or policies can be developed to align individual and societal incentives, or how targets are selected and defended.
- Provide the foundations and tools for privacy, confidentiality, accountability, and anonymity, as well as extraction of knowledge from massive datasets without compromising societal values.
- Advance the design and implementation of software that exhibits resiliency in the face of an attack; the design and composition of software components into large-scale systems with known security properties; the design, including attention to behavior and human factors, of reliable systems that can function dependably even if some subset of components do not function as intended; and support transition of novel software into shared cyberinfrastructure.

Developing Scientific Foundations

- Develop the scientific foundations for digital systems that can resist attacks, including a range of cryptographic algorithms and statistical tools that can withstand attacks from novel computing engines, such as quantum computers, and that support operation in environments with restricted computational resources.
- Develop the mathematical and statistical theory and methodologies required to model and predict the behavior of large-scale, complex systems; assure that the large-scale computations in many fields of research are not vulnerable to manipulation or compromise; and develop and implement improved cybersecurity defenses for scientific environments and cyberinfrastructure.
- Develop the scientific foundations to understand how individuals, groups, organizations, and other actors make decisions in the realm of cybersecurity; develop market-based approaches to align incentives for investments, efficiently share risks, and internalize externalities.

Maximizing Research Impact

- Ensure that the Nation’s populace understands the security and privacy characteristics and limitations of the digital systems on which they rely daily.
- Coordinate with the NSF Cyber-enabled Materials, Manufacturing, and Smart Systems (CEMMSS) investment to support foundational research in cybersecurity issues arising in advanced manufacturing, robotics, and critical infrastructure such as Smart Grids.
- Investigate opportunities and challenges in organizational alliances around cybersecurity; examine alternative governance mechanisms, for example, private-public partnerships and international agreements.

Accelerating Transition to Practice

- Provide insight and incentives into the process for innovation diffusion and adoption at the organizational, group, and individual levels.
- Drive innovation through applied research, development, and experimental deployment. Transition successful basic research results and commercial innovations into early adoption and use tailored for NSF communities and learning environments. Enable NSF cyberinfrastructure as a premier proving ground and state-of-the-art environment for advancing cybersecurity solutions and moving them into technical and organizational practice.

In addition, SaTC will address the pivotal issues in the education and preparation of tomorrow’s cybersecurity researchers. Specific objectives are:

- Promote innovation and development of new curricula and learning opportunities to create and sustain an unrivaled cybersecurity workforce capable of developing sound and secure cyberinfrastructure components and systems.
- Study new approaches to training and education in cybersecurity to understand their impact and provide a basis for continual refinement and improvement.

Goals

The long-term goal of the SaTC program is to build the knowledge base in cybersecurity that enables discovery, learning, and innovation in this critical area, and ultimately leads to a more secure and trustworthy cyberspace. The program aligns with the President's *Strategic Plan for the Federal Cybersecurity Research and Development Program* (released in December 2011), which details four subgoals that together cover a set of interrelated priorities for the federal agencies that conduct or sponsor research and development in cybersecurity. These four goals are: (1) inducing change, (2) developing scientific foundations, (3) maximizing research impact, and (4) accelerating transition to practice. In order to achieve these goals, a coordinated, interdisciplinary program is needed.

Approach

The Directorates for Computer and Information Science and Engineering (CISE); Education and Human Resources (EHR); Engineering (ENG); Mathematical and Physical Sciences (MPS); Social, Behavioral, and Economic Sciences (SBE); and the Office of Cyberinfrastructure (OCI) will participate in this program. Each of these organizations supports a research community whose abilities are needed to build the envisioned cybersecure and trustworthy environment and to prepare the scientists and supporting workforce needed to sustain and improve that environment. The SaTC program is managed by a Working Group (WG) made up of program directors from the participating directorates and offices.

Under the OneNSF umbrella, the SaTC working group will coordinate with the EHR Scholarship for Service (SFS) program to help align opportunities for cybersecurity education and workforce development. SFS, which focuses on cybersecurity education and workforce development, has funded more than 1,500 students. Over 1,100 of these students have been successfully placed in internships and full-time positions in more than 120 federal agencies and departments. Furthermore, SFS capacity building grants have increased the capacity of the higher education enterprise in cybersecurity education and research.

NSF is uniquely positioned to support the broad, open, long-term, foundational research and education needed to establish a sound basis for progress in this critical area. There are currently about 500 active projects in the CISE cybersecurity programs that pre-date the FY 2012 SaTC program. This research portfolio includes projects addressing security from the microscopic level (e.g., detecting whether a silicon chip may contain a malicious circuit) to the macroscopic level (e.g., determining strategies for securing the next generation electrical power grid). The portfolio also ranges from mathematical algorithms and statistical tools – cryptography, cryptographic protocol analysis, formal specification and verification techniques, reliability, probabilistic modeling, risk analysis, data and text-mining, static and dynamic program analysis, and security testing methods – to human-centric systems that include web applications, smart phones, medical devices, and automotive systems. Through the interagency NITRD program, NSF plays a number of key roles in cross-agency coordination of the federal government's cybersecurity research investments. NSF is active in the NITRD Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), which has a leadership role in executing and coordinating the *Strategic Plan for the Federal Cybersecurity Research and Development Program* across the thirteen member agencies. In addition with its co-chair role on the Senior Steering Group (SSG) for

Cybersecurity R&D, NSF helps define, coordinate, and recommend strategic federal R&D objectives in cybersecurity, and to communicate research needs and proposed budget priorities to policy makers and budget officials, including recommendations to OSTP, OMB, and the Joint Inter-Agency Cyber Task Force (JIACTF).

INVESTMENT FRAMEWORK

FY 2012

In FY 2012, CISE, MPS, SBE, and OCI issued a joint solicitation for the new Secure and Trustworthy Cyberspace (SaTC) program that called for proposals that build teams across these different research communities. To help develop this community, the directorates are planning community-building workshops and a PI meeting with interagency representation that will be held in 2012.

SFS will continue its focus on increasing the number of qualified students entering the fields of information assurance and cybersecurity and enhancing the capacity of the United States higher education enterprise to continue to produce professionals in these fields to meet the needs of our increasingly technological society.

FY 2013 Request

The following activities are planned for FY 2013:

- Expand the number of large, multi-institution projects that provide high-level visibility to grand challenge research areas.
- Expand the research portfolio to include more cross-disciplinary projects and broaden the portfolio to both cover a broader set of research topics and to increase transition to practice.
- Coordinate SaTC efforts with Cyber-enabled Materials, Manufacturing, and Smart Systems, which supports foundational research in cybersecurity issues arising in advanced manufacturing, critical infrastructure, and robotics.
- Continue to facilitate the development of a National Virtual Lab for Cybersecurity Education to promote collaboration and resource sharing.
- Hold a PI meeting that brings together SaTC funded PIs with interested parties from industry and government agencies in support of the NITRD *Strategic Plan for the Federal Cybersecurity Research and Development Program* thrust of accelerating transition to practice.
- Support efforts to define a cybersecurity body of knowledge and to establish curricula recommendations for new courses, degree programs, and educational pathways.
- Through SFS, continue to support efforts to define the knowledge base in cybersecurity education and work with the community to develop recommendations for new courses, degree programs, and educational pathways based on evidence of effective practice. SFS supports innovative and creative projects, which lead to an increase in the ability of the United States higher education enterprise to produce information assurance and cybersecurity professionals.

FY 2014 – FY 2016

Building on the knowledge base developed during the previous years, SaTC will continue to focus on game-changing research and education; the development of digital systems that are resistant to attacks; coordination with the CEMMSS WG to secure advanced manufacturing systems, robotics, and critical infrastructure; and transition to practice of the research results ready for experimental deployment, early adoption, commercial innovation, or implementation in cyberinfrastructure. To more effectively achieve its long-term goals, SaTC will develop partnerships with other agencies, industry, and international organizations. The cybersecurity research community is also expected to grow to include more researchers who cross the boundaries between computer science, engineering, economics, social and behavioral sciences, statistics, and mathematics, creating a flourishing cybersecurity research and development ecosystem.

SaTC Funding

(Dollars in Millions)

Directorate/Office	FY 2012 Estimate	FY 2013 Request
CISE	55.00	69.00
ENG	3.25	4.25
MPS	0.50	2.00
SBE	4.00	4.00
OCI	4.00	6.00
EHR	45.00	25.00
Total, NSF	**$111.75**	**$110.25**

Totals may not add due to rounding.

EVALUATION FRAMEWORK

Using information collected by the SaTC WG and the recommendations in the recent national strategic plan on cybersecurity, the WG will conduct gap and portfolio analysis to develop a shared understanding of program goals, milestones, and outcomes over the next four years. Each year, the program will conduct an annual review based on those assessments and report its results to NSF senior management as well as to the NITRD CSIA Senior Steering Group for feedback and recommendations.

Based on the four subgoals of SaTC, the outcomes will include: for inducing change – discovery of the root causes of threats and attacks and continuous investment in transformational approaches that improve the security of cyberspace; for developing scientific foundations – development of a systematic scientific approach to cybersecurity, including discovery of laws and principles; for maximizing research impact – partnerships with other agencies, industry, and international collaborators as well as linkages to national priorities, such as health IT or Smart Grid; and for accelerating transition to practice – new patents, products, services, companies, and research that can be transitioned into cyberinfrastructure.

The SaTC program will convene biennial PI meetings to monitor progress in this area of research. In addition, a trend analysis based on the annual reviews will be presented to the CISE Committee of Visitors, which is held every three years.

The SFS program will be evaluated by the Office of Personnel Management's Human Resources Solution (HRS) group with input from the NSF SFS program directors and the OPM SFS Program Office. An evaluation plan and design that links SFS program objectives with measures, data sources, and expected and unexpected outcomes will be submitted and agreed upon in January/February of 2012. The mixed method evaluation is designed to provide information to the program for purposes of program improvement, accountability, and learning, and builds on the previous evaluation that was released in January 2008 by the Assessment Services Branch of the Division for Human Resources Products and Services, U.S. Office of Personnel Management (OPM). As the current evaluation proceeds, HRS will continue to consult with NSF in the design and execution of the evaluation of the SFS program. The evaluation is expected to be completed in FY 2013.