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 computational, statistical, mathematical, 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 and ubiquity 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 research that provides a deeper understanding of the social and behavioral factors affecting cybersecurity. The development and deployment of innovative cybersecurity models and practices throughout scientific environments 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.

Total Funding for SaTC

(Dollars in Millions)

FY 2012 Actual	FY 2012 Enacted/ Annualized FY 2013 CR	FY 2014 Request
$113.37	**$111.75**	**$110.25**

Goal

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 *Trustworthy Cyberspace: 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); and Social, Behavioral, and Economic Sciences (SBE) participate in this program. Each of these organizations supports a research community whose abilities are needed to collectively 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.

EHR invests in the CyberCorps: Scholarship for Service (SFS) program, which supports cybersecurity education and workforce development. SFS has funded more than 1,700 students and provides capacity building grants to promote cybersecurity education and research at higher education institutions. 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 secure the Nation's cyberinfrastructure.

The following paragraphs describe the specific objectives of NSF's SaTC program, and how they relate to the four thrusts of the Federal Cybersecurity Strategic Plan:

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 of reliable systems including attention to behavior and human factors that can function dependably even if some subset of components do not function as intended, and support the 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.

Investment Framework

SaTC Funding by Directorate

(Dollars in Millions)

Directorate/Office	FY 2012 Actual	FY 2012 Enacted/ Annualized FY 2013 CR	FY 2014 Request
Computer and Information Science and Engineering	$58.89	$59.00	$75.00
Education and Human Resources	44.98	45.00	25.00
Engineering	5.00	3.25	4.25
Mathematical and Physical Sciences	0.50	0.50	2.00
Social, Behavioral, and Economic Sciences	4.00	4.00	4.00
Total	**$113.37**	**$111.75**	**$110.25**

Totals may not add due to rounding.

FY 2012 – FY 2013

In FY 2012, 61 SaTC proposals were funded from a solicitation jointly issued by CISE (including the Division of Advanced Cyberinfrastructure, formerly the Office of Cyberinfrastructure), MPS, and SBE. These proposals support the four thrust areas of the Federal Cybersecurity Strategic Plan: inducing change, developing scientific foundations, maximizing research impact, and accelerating transition to practice. In addition, six CAREER awards associated with SaTC were funded in FY 2012. In FY 2013, a SaTC solicitation was jointly issued by CISE, EHR, ENG, MPS, and SBE to elicit research proposals to expand research and development of secure and trustworthy cyberspace using the approach outlined above in the Federal Cybersecurity Strategic Plan.

To develop the SaTC community, in FY 2012, the directorates held community-building workshops and Principal Investigator (PI) meetings. In 2013, meetings will be held to facilitate the exchange of ideas on the SaTC program and related research and development. Interdisciplinary workshops that focus on specific problems (e.g., metrics, fundamental results, evidence-based research) in the scientific foundations of cybersecurity are planned, as well as meetings to educate SaTC program directors about other NSF programs that focus on transitions to practice, such as NSF Innovation Corps and the Accelerating Innovation Research activity in the Partnerships for Innovation program. NSF held a workshop in partnership with the Computing Community Consortium and the Semiconductor Research Corporation on fundamental cybersecurity issues of interest to both industry and academic researchers.

NSF has collaborated with, and will continue to collaborate with, other federal partners on cybersecurity: NSF co-chairs the NITRD Cyber Security and Information Assurance Senior Steering Group, which provides leadership across the government in cybersecurity R&D and provides a forum for information sharing. In addition, NSF and the Department of Education co-lead the Formal Education Component of the National Initiative for Cybersecurity Education. In FY 2012, NSF and the National Security Agency (NSA) jointly held a Principal Investigator (PI) workshop, as well as jointly funded the Cyber-Physical Systems Virtual Organization at Vanderbilt University to encourage it to extend its scope into cybersecurity and to better understand how it relates to smart systems.

In FY 2012, the SFS program continued 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. SFS funded 43 projects in FY 2012. In FY 2013, NSF will continue funding SFS capacity building proposals focusing on broadening participation of women, veterans, and underrepresented minority groups. At least two university pilots on cybersecurity education and secure programming, jointly supported by CISE and EHR, will be launched in FY 2013. NSF will hold a workshop to help create a community of researchers and students interested in cross CISE-SBE-EHR related issues. These efforts will include the development of a National Virtual Lab for Cybersecurity Education to promote collaboration and resource sharing.

In FY 2013, a fourth perspective on cybersecurity education has been added to the SaTC solicitation with the aim to promote innovation, development, and assessment of new learning opportunities and to create and sustain an unrivaled cybersecurity workforce capable of developing secure cyberinfrastructure components and systems, as well as to raise the awareness of cybersecurity challenges to a more general population.

FY 2014 Request

The following activities are planned:

- Expand the research portfolio to include more cross-disciplinary projects to cover a broader set of research topics and to increase transition to practice.
- Fund up to two large, multi-institutional projects that provide high-level visibility to grand challenge research areas.
- Develop a mechanism for supporting foundational research that has industrial impact, such as Grant Opportunities for Academic Liaison with Industry (GOALI) supplements or co-funding with an industrial consortium.
- Expand cybersecurity outreach and collaboration efforts by establishing a partnership with at least one other agency (e.g., the Department of Homeland Security, National Institute of Standards and Technology, NSA) for co-funding or transition of projects, and hold a workshop with the European Union to determine mutual interests.
- Hold a SaTC PI meeting to help build a broad community that crosses disciplinary interests.

- Expand the education and preparation of cybersecurity researchers by funding projects on curriculum development and evaluation in cybersecurity. Support efforts to define a cybersecurity body of knowledge and to establish curricula recommendations for new courses, degree programs, and educational pathways.

FY 2015 – Beyond

Building on the knowledge base developed during the previous years, SaTC will continue to focus on game-changing research and education and the development of digital systems that are resistant to attacks. In coordination with the CEMMSS WG, the focus will be to secure advanced manufacturing systems, robotics, and critical infrastructure; and transition to practice 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, thereby creating a flourishing cybersecurity research and development ecosystem.

NSF will continue to promote the development of new curricula and learning opportunities to augment the cybersecurity workforce with focused efforts to recruit and retain underrepresented minorities, women, first-generation/low-income students, and/or veterans.

Evaluation Framework

NSF has engaged the Science Technology Policy Institute (STPI) to conduct a program evaluation feasibility study for the SaTC program. This evaluation feasibility study will examine the baseline portfolio of SaTC investments and identify metrics to measure progress of goals as part of an impact assessment.

This feasibility study will be conducted to develop a plan for an impact assessment of the SaTC investment. The approach outlined below will be followed:

- Meetings will be held with the SaTC WG and SaTC management to examine the past and current portfolio of awards, including an assessment of the components of the portfolio by technical and scientific content. In addition, various recommendations from federal advisory boards and stakeholder communities on how to structure future cybersecurity investments will be synthesized.
- A roadmap will be refined to help NSF track progress toward its major scientific objectives (e.g., discovery of the root causes of threats and attacks and continuous investment in transformational approaches that improve the security of cyberspace; development of a systematic scientific approach to cybersecurity, including discovery of laws and principles). This effort may entail workshops with the stakeholder community to define the major research questions and research goals for SaTC.

Based on the results of the workshops and related activities (stated above), a third party contractor and NSF will develop the appropriate plan for assessing progress across NSF's SaTC activities.

The initial contract for the evaluation feasibility study was put into place and a kick-off meeting was held during the fourth quarter of FY 2012. Work is ongoing to establish an evaluation framework, which will be in place by the end of FY 2013.

Additionally, in FY 2012, NSF and the Organizational Assessment Group of the U.S. Office of Personnel Management (OPM) worked together to assess the extent to which the SFS program achieved its major goals. The OPM evaluation team conducted focus groups, administered surveys to the different stakeholders of the SFS program (e.g., students, graduates, PIs, faculty, agency supervisors, hiring officials and recruiters), and also conducted a workforce analysis to project the federal hiring demands

for computer professionals. The evaluation is expected to be completed in October 2013. In FY 2013, NSF and OPM plan to look for ways to increase the marketing of the SFS program to agencies and expand the internship opportunities for students. A competency gap analysis of competencies needed once on the job is underway.