SECURE AND TRUSTWORTHY CYBERSPACE (SaTC) $124,250,000
+$1,500,000 / 1.2%

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 trustworthy cyberspace is a critical challenge as corporations, agencies, national infrastructure, and individuals have been victims of cyberattacks, which exploit weaknesses in technical infrastructures as well as in human behavior. Through long-term foundational research in algorithms, models, probability theory, reliability, statistical theory and analysis, cryptanalysis, system structures, and secure computing, SaTC promises to develop the scientific foundations for cybersecurity and privacy research for years to come. SaTC funding broadens the cybersecurity research portfolio through support for multi-disciplinary projects with expertise in computer, computational, statistical, mathematical, social, behavioral, and economic sciences. Such projects, for example, investigate the motivations and incentives of individuals and institutions, both as attackers and defenders, and lead to a more cybersecure society. Additionally, SaTC supports new, innovative approaches to educate and prepare tomorrow's cybersecurity researchers and professionals with the skills and knowledge necessary to build a secure and trustworthy cyberspace.

Total Funding for SaTC

(Dollars in Millions)

FY 2014 Actual	FY 2015 Estimate	FY 2016 Request
$126.00	**$122.75**	**$124.25**

Goal

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

Approach

The Computer and Information Science and Engineering (CISE) directorate leads this NSF-wide effort, and is joined by the Education and Human Resources (EHR), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral, and Economic Sciences (SBE) directorates. Each of these organizations supports a research community whose abilities are needed collectively to build the envisioned secure and trustworthy cyber 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) comprised 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 2,100 students and provides capacity-building grants to promote cybersecurity education and research at higher education institutions. SFS will

[1] www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

continue its focus on increasing the number of qualified students entering the fields of information assurance and cybersecurity, which enhances the capacity of the U.S. higher education enterprise to continue to produce professionals in these fields to secure the Nation's cyberinfrastructure.

NSF also collaborates with other federal partners on cybersecurity. For example, NSF co-chairs the Networking and Information Technology Research and Development Program (NITRD) Cyber Security and Information Assurance (CSIA) Senior Steering Group (SSG), which provides leadership across the government in cybersecurity R&D by serving as a forum for information sharing and cross-agency agenda setting. SaTC activities are also coordinated with other agencies through NSF's participation in the CSIA Interagency Working Group (IWG) and the Special Cyber Operations Research and Engineering (SCORE) Interagency Working Group. In addition, NSF and the Department of Education (ED) co-lead the Formal Education Component of the National Initiative for Cybersecurity Education (NICE).

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.
- 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, and the design of reliable systems including attention to behavior and human factors.

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.
- 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 as well as 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; and 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 societal, organizational, group, and individual levels.
- Drive innovation through applied research, development, and experimental deployment and implementation, resulting in fielded capabilities and innovations of direct benefit to campus networks, systems and environments supporting NSF science and engineering research and education environments.
- Transition successful basic research results and commercial innovations into early adoption and use, allowing NSF cyberinfrastructure to serve 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 addresses important issues in the education and preparation of tomorrow's cybersecurity researchers. Specific objectives are to:

- Promote innovation, development, and testing and evidence-gathering 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 innovative approaches in cybersecurity training and education 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 2014 Actual	FY 2015 Estimate	FY 2016 Request
Computer and Information Science and Engineering	$71.18	$70.00	$70.50
Education and Human Resources	44.87	45.00	45.00
Engineering	3.75	3.25	3.25
Mathematical and Physical Sciences	2.00	0.50	1.50
Social, Behavioral, and Economic Sciences	4.20	4.00	4.00
Total	**$126.00**	**$122.75**	**$124.25**

Totals may not add due to rounding.

FY 2014 – FY 2015

In FY 2014, CISE, EHR, ENG, MPS, and SBE jointly issued the SaTC solicitation to continue to elicit proposals that expand the research and development of a secure and trustworthy cyberspace. In FY 2015, the SaTC solicitation was reissued, and a new size category was created for projects – "Large" (up to $3.0 million in total budget and up to five years in duration). This new category aims to provide portfolio balance through investments in a diverse set of collaborations focused on large-scale Trustworthy Computing (TwC) research, large-scale Social, Behavioral, or Economic Sciences (SBE) research, or integrated TwC/SBE efforts.

To foster additional multidisciplinary research in privacy, NSF issued a Dear Colleague Letter (DCL) in FY 2014 encouraging the submission of proposals that specifically addressed the need to develop new and deeper fundamental understandings of privacy in today's networked world. In FY 2015, SaTC is continuing to fund projects on fundamental research in privacy.

Education and training continued to be a major component of SaTC in FY 2014 and FY 2015. EHR

continued to fund SFS capacity-building awards, which focus on recruiting and retaining underrepresented minorities, women, first-generation undergraduate students, low-income students, and/or veterans, as well as applications by and partnerships with minority-serving institutions and two-year colleges. Additionally, NSF sponsored a workshop in FY 2014 that brought together computer science educators and cybersecurity researchers to discuss more innovative approaches to advance cybersecurity education. On the basis of this workshop, in FY 2015 SaTC is focusing on new ways to promote innovation, development, and assessment of new learning opportunities in order to create and sustain an unrivaled cybersecurity workforce. NSF also supported, and is continuing to support, large-scale cybersecurity competitions through collaborations with California State Polytechnic University Pomona's National Cybersecurity Sports Federation, which provides a shared pathway for students to learn cyber competitions the way athletes learn a sport.

Broadening the SaTC research community is critical to facilitating advances in cybersecurity research. Building on the successes of a workshop in FY 2013, a second workshop for aspiring SaTC principal investigators (PIs) was held in FY 2014. The goal was to educate potential SaTC researchers on the priorities of the program and components of successful research projects. NSF will continue to use this approach to bring new researchers with a broad set of talents and interests into the SaTC PI community.

Several workshops focused on cybersecurity research were held in FY 2014, including a Science of Cybersecurity workshop that considered specific foundational problems (e.g., metrics, fundamental results, evidence-based research, and protection of critical infrastructure); a "Cybersecurity 2025" workshop that sought to catalyze a community-wide discussion to review SaTC progress relative to the federal strategic plan and to envision long-term research agendas for the field; and two workshops at the NSF-funded Institute for Computational and Experimental Research in Mathematics (ICERM) to explore mathematical developments needed in cybersecurity research. Building on the results of the Science of Cybersecurity workshop, SaTC will fund projects that focus on the scientific foundations of cybersecurity in FY 2015. NSF is also holding a cross-agency workshop in FY 2015 to review progress made in developing a science of cybersecurity, and to propose ways in which needs and results can be communicated more effectively to stakeholders from academe, industry, and government.

In order to facilitate translation of research to practice, a session at the FY 2015 SaTC principal investigator (PI) meeting was dedicated to educating SaTC PIs about other NSF programs that focus on transition to practice, such as NSF Innovation Corps (I-Corps™) and the Accelerating Innovation Research (AIR) activity in the Partnerships for Innovation (PFI) program. Over 400 cybersecurity researchers and educators from academe, industry, and government attended the SaTC PI meeting.

In FY 2014, NSF announced two new partnerships with industry in the domain of cybersecurity. NSF issued a new solicitation in partnership with Intel in the area of cyber-physical systems security and privacy (CPS-Security). The goal of this partnership between NSF and Intel is to foster novel, transformative, multidisciplinary approaches that ensure the security of current and emerging cyber-physical systems. Projects are being awarded in FY 2015. NSF also issued a solicitation with the Semiconductor Research Corporation (SRC) in FY 2014 for Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS). The STARSS solicitation resulted in nine projects jointly funded by NSF and SRC focused on strategies, techniques, and tools that avoid and mitigate vulnerabilities and lead to semiconductors and systems that are resistant and resilient to attack or tampering. In FY 2015, SaTC is continuing this partnership with SRC through a STARSS perspective in the SaTC solicitation.

In FY 2015, NSF partnered with the US-Israel Binational Science Foundation (BSF) to support collaborations between U.S. and Israeli researchers focused on foundational research in all areas of

cybersecurity. It is expected that this partnership will yield international teams that will enhance the security and trustworthiness of cyberspace in the long term.

FY 2016 Request

The following activities are planned:

- Continue to fund innovative projects in the science of cybersecurity, the science of privacy, cybersecurity for cloud computing, and cybersecurity for cyber-physical systems. Fund at least two projects on big data analytics for cybersecurity, and at least two projects on software engineering for cybersecurity.
- Issue a new solicitation based on community feedback and the results of a portfolio analysis, with a specific call for research into privacy, security of cyber-physical systems, and low-cost and/or low-effort approaches for securing systems such as web services and the Internet of Things (IoT).
- Hold a series of workshops with key stakeholders to identify research areas based on the recommendations in the NITRD National Privacy Research Strategy that is expected to be published in late FY 2015/early FY 2016. One of these workshops will be a cross-agency workshop that reviews progress toward developing a science of privacy, and that proposes ways that research needs and results can be better communicated across government, academe, and industry.
- Hold the next in a series of biennial PI meetings with representation from academe, industry, and government, including other federal agencies. This PI meeting will feature sessions on emerging frontiers in cybersecurity, including a session focused on the science of privacy. The PI meeting will also showcase successful Transition to Practice/I-Corps™/AIR activities resulting from SaTC investments. It will also serve as an opportunity for the CPS-Security performers to review progress and identify critical unaddressed problems and directions.
- Leverage the ongoing SaTC portfolio analysis to identify and develop new directions for FY 2016 and beyond.
- Support projects through a new Transition to Education (TtE) mechanism. Through TtE, research results in software engineering, science of cybersecurity, and designed in security will be moved into relevant course curriculum that will be implemented, assessed, and improved in a variety of settings. Such efforts will be supported using TtE supplements and options. TtE is analogous to the Transition to Practice (TTP) component of SaTC whereby research results that show promise beyond furthering basic research are transitioned into practical applications.
- Support research and development in cybersecurity education to encourage and test innovative approaches to the preparation of cybersecurity professionals in formal and informal learning settings. As part of this, support the development and assessment of learning modules and approaches for cybersecurity education that can be incorporated into computer science instruction, quantitative and scientific literacy curricula, and science and engineering programs for undergraduate and graduate students who will need basic understandings of cybersecurity relevant to their domains. Foundational research to examine the basic concepts and instructional approaches for cybersecurity also will be supported. These efforts will be included in such programs as the EHR Core Research (ECR) program, CyberCorps®: Scholarship for Service (SFS), Cyberlearning and Future Learning Technologies (Cyberlearning), and the NSF-wide Improving Undergraduate STEM Education (IUSE) program.

FY 2017 and 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 NSF-wide CEMMSS investment, SaTC will include a focus on secure advanced manufacturing systems, robotics, and critical infrastructure. SaTC will also focus on transitioning to practice research results ready for experimental deployment, early adoption, commercial innovation, or implementation in cyberinfrastructure. In addition, SaTC will build upon existing, and

develop new, partnerships with other federal agencies, industry, and international organizations to effectively achieve its long-term goals. 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. A PI meeting will be held with interagency representation, focusing on the science of cybersecurity and novel interdisciplinary areas of research.

NSF will continue to promote the development of and related research about 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 and Technology Policy Institute (STPI) to conduct a program evaluation feasibility study for the SaTC program. This evaluation feasibility study is examining the baseline portfolio of SaTC investments and identifying metrics to measure progress towards goals as part of an impact assessment. The evaluation feasibility study was initiated in the fourth quarter of FY 2012, and a final report is anticipated in FY 2015.

This feasibility study has developed a plan for an impact assessment of the SaTC investment. The approach outlined below has been followed:

- Meetings have been held with the SaTC working group 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, as part of this portfolio analysis, various recommendations from federal advisory boards and stakeholder communities on how to structure future cybersecurity investments have been synthesized.
- A logic model has been developed 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; and development of a systematic scientific approach to cybersecurity, including discovery of laws and principles).

Based on the results, NSF and a third-party contractor will develop the appropriate plan for assessing progress across NSF's SaTC activities, following the framework STPI is developing.

In addition, staff from the Office of the Director for National Intelligence (ODNI) were charged with monitoring the Comprehensive National Cybersecurity Initiative (CNCI) investments across agencies engaged in categorizing projects using the four game-changing research themes outlined in the national cybersecurity research and development strategy. The results of this activity will be reported to the CSIA SSG in FY 2015.

Research that has been transitioned into practice will be highlighted at the biennial PI meetings (e.g., new products, patents, start-ups, and commercialization of new approaches and techniques).

The Office of Personnel Management's Human Resources Solutions (HRS) conducted an evaluation of the SFS program, primarily focusing on the program's scholarship and capacity building tracks. HRS and NSF are finalizing a report on the 2012-2013 Summative Evaluation, and it is expected to be ready for public distribution by the end of FY 2015. Going forward, program monitoring and evaluation activities for the SFS program will be coordinated to reduce the burden on principal investigators, scholarship recipients, and program administrators. HRS will consult with NSF on the program evaluation in ways that maintain the integrity and independence of the evaluation while ensuring that the evaluation is sensitive to the program's objectives, goals, mission, vision, and any pending legislation or executive level initiatives. The intent of the SFS program monitoring system is to provide a description of the implementation and selected desired outcomes of the program over time and to address the issues raised

by the GAO report, *Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination* (GAO-12-8; November 2011).[2]

[2] www.gao.gov/new.items/d128.pdf