## SECURE AND TRUSTWORTHY CYBERSPACE (SaTC) $149,750,000 +$20,000,000 / 15.4%

### Overview

Achieving a secure and trustworthy cyberspace is a challenge of national importance. Organizations, infrastructure, and individuals are increasingly victims of cyber attacks, which result from weaknesses in the technical infrastructure coupled with human behaviors that play to the advantage of attackers. The outcomes are worsened by inadequate knowledge about how to respond to and mitigate these adverse events. As we move to ubiquitous cyber-physical systems and a future Internet of Things (e.g., in transportation systems, smart grids, medical devices, and advanced manufacturing, etc.), this challenge will become even more acute. The trustworthiness of cyberspace is challenged in complex ways, including misinformation, cyber identity verification issues, and the increasing sophistication and co-evolution of attacks and responses. Addressing these problems requires multi-disciplinary expertise in computer science; statistics; mathematics; and social, behavioral, and economic sciences, along with the transition of new concepts and technologies into practice. The NSF-wide Secure and Trustworthy Cyberspace (SaTC) investment supports long-term foundational research and education in cybersecurity and privacy leading to 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.

**Total Funding for SaTC**

(Dollars in Millions)

| FY 2015<br>Actual | FY 2016<br>Estimate | FY 2017<br>Request |
|---|---|---|
| **$124.71** | **$129.75** | **$149.75** |

### Goal

The long-term goal of the SaTC investment is to build the knowledge base in cybersecurity that enables discovery, learning, and innovation; leading to a more secure and trustworthy cyberspace. SaTC aims to develop the scientific foundations for cybersecurity and privacy research for years to come through a focus on long-term, foundational research in cybersecurity. More specifically, SaTC looks to broaden the cybersecurity research portfolio to include more cross-disciplinary projects with expertise in computer, computational, statistical, mathematical, social, behavioral, and economic sciences; increase opportunities for implementing new technologies that emerge from the research; expand the number of large, multi-institutional projects that provide high-level visibility to cybersecurity grand challenges; and establish curricular recommendations for new courses, degree programs, and educational pathways that foster innovative approaches to educate and prepare tomorrow's cybersecurity researchers and professionals. The investment aligns with recent federal cybersecurity strategies, including *Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program*;[1] the government-wide Comprehensive National Cybersecurity Initiative (CNCI); and the recent Cybersecurity Enhancement Act of 2014 (P.L. 113-274).

### Approach

The Directorate for Computer and Information Science and Engineering (CISE) 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

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

workforce necessary to sustain and improve that environment. The SaTC investment is managed by a Working Group (WG) comprising program directors from the participating directorates.

EHR invests in the CyberCorps®: Scholarship for Service (SFS) program, which supports cybersecurity education and workforce development. Since 2002, SFS has funded more than 2,300 students, and more than 1,700 have graduated and been placed in federal agencies and departments. SFS scholarships are currently available at over 50 institutions of higher education. Furthermore, over 200 SFS capacity-building grants are increasing the ability of the higher education enterprise to produce cybersecurity professionals.

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) IWG. In addition, NSF and the Department of Education (ED) co-lead the Formal Cybersecurity Education component of the National Initiative for Cybersecurity Education (NICE).

The SaTC investment has the following objectives:

<u>Inducing Change</u>
SaTC investments induce change by investing in research that:

- Leads to a better understanding of the motivations, incentives, and behaviors of users, attackers, and defenders;
- Provides the foundations and tools for privacy, confidentiality, accountability, and anonymity, as well as extraction of knowledge from massive datasets without compromising societal values;
- Provides the foundations and tools for privacy, confidentiality, accountability, and anonymity, as well as extraction of knowledge from massive datasets without compromising societal values; and
- Advances 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.

<u>Developing Scientific Foundations</u>
SaTC investments develop the scientific foundations of cybersecurity by supporting research on:

- 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;
- The mathematical and statistical theory and methodologies required to model and predict the behavior of large-scale, complex systems; assuring 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; and
- The scientific foundations necessary to understand how individuals, groups, organizations, and others make decisions in the realm of cybersecurity as well as market-based approaches to align incentives for investments, efficiently share risks, and internalize externalities.

<u>Maximizing Research Impact</u>
The SaTC investment maximizes research impact by:

- Ensuring that the Nation's populace understands the security and privacy characteristics and limitations of the digital systems on which they rely daily;

- Coordinating with NSF's 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;
- Investigating opportunities and challenges in organizational alliances around cybersecurity;
- Examining alternative governance mechanisms, for example, private-public partnerships and international agreements.

Accelerating Transition to Practice

SaTC investments are transitioning successful basic research results and commercial innovations into early adoption and use by:

- 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;
- Providing insight and incentives into the process for innovation diffusion and adoption at the societal, organizational, group, and individual levels; and
- Driving innovation 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.

Cybersecurity Education:

SaTC activities address important issues in the education and preparation of tomorrow's cybersecurity workforce by:

- Promoting innovation, development, and testing and evidence-gathering of new curricula and learning opportunities;
- Increasing the number of qualified students entering the fields of information assurance and cybersecurity and information assurance; and
- Enhancing the capability of the U.S. higher education enterprise to produce professionals in these fields to meet the needs of our increasingly technological society.

**Investment Framework**

**SaTC Funding by Directorate**

(Dollars in Millions)

| Directorate/Office | FY 2015<br>Actual | FY 2016<br>Estimate | FY 2017<br>Request |
|---|---|---|---|
| Computer and Information Science and Engineering | $70.56 | $70.50 | $70.50 |
| Education and Human Resources | 45.04 | 50.00 | 70.00 |
| Engineering | 3.25 | 3.25 | 3.25 |
| Mathematical and Physical Sciences | 1.86 | 2.00 | 2.00 |
| Social, Behavioral, and Economic Sciences | 4.00 | 4.00 | 4.00 |
| **Total** | **$124.71** | **$129.75** | **$149.75** |

**FY 2015 – FY 2016**

In FY 2015, CISE, EHR, ENG, MPS, and SBE jointly issued a revised SaTC solicitation to continue to seek proposals that expand the research and development frontiers for a secure and trustworthy cyberspace. The revised SaTC solicitation offered a new size category for projects: "Large" (up to $3.0 million per award 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, SBE research, or integrated TwC/SBE efforts. In summer 2015, NSF issued the FY 2016 SaTC program solicitation for Small, Medium, and Large proposals.

Building on the results of a Science of Cybersecurity workshop held in FY 2014, SaTC funded projects in FY 2015 focused on the scientific foundations of cybersecurity. NSF also held 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 FY 2016, SaTC is funding innovative projects in the science of cybersecurity, the science of privacy, cybersecurity for cloud computing, and cybersecurity for cyber-physical systems. These projects include foci on big data analytics for cybersecurity and software engineering for cybersecurity.

SaTC also continued funding community-building workshops with interagency representation. For example, in FY 2015 SaTC jointly funded a workshop with the Department of Homeland Security (DHS) to identify ways to transition NSF- and DHS-funded cybersecurity research into practice.[2] In addition, a SaTC workshop titled, *Privacy in the Era of Big Data*, brought together experts in the domains of big data and privacy to develop a research agenda for better understanding and promoting privacy in an era of big data.[3] In FY 2016, SaTC will sponsor additional community workshops to explore mathematical research necessary for advancing cybersecurity. NSF will also hold a series of workshops with key stakeholders to identify research areas based on the recommendations contained in the National Privacy Research Strategy that is expected to be published in FY 2016. One of these workshops will be held in collaboration with other federal agencies, and will seek to review progress toward developing a science of privacy and to propose ways that research needs and results can be better communicated across government, academe, and industry.

Education and training continued to be a major component of SaTC. EHR continued funding SFS capacity-building awards, which focus on recruiting and retaining underrepresented minorities, women, first-generation undergraduate students, low-income students, and/or veterans. EHR also continued funding SFS awards to and partnerships with minority-serving institutions and two-year colleges. In FY 2015, SFS continued to work with community colleges designated as Centers of Academic Excellence in Information Assurance 2-Year (CAE2Y) by providing funds for two Advanced Technological Education (ATE) centers for cybersecurity education. SFS plans to launch two related efforts in FY 2016, one to increase the number of community colleges holding the CAE2Y designation, and one to create and disseminate a cybersecurity-themed version of the Advanced Placement® Computer Science Principles course for use in community colleges. In FY 2016, SFS will support research and development in cybersecurity education to encourage and test innovative approaches for the preparation of cybersecurity professionals in formal and informal settings. This effort will include support for 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. NSF will also support foundational educational research to examine basic concepts and instructional approaches for cybersecurity.

[2] http://soc.southalabama.edu/TTP/images/TTPWorkshopExecutiveSummary.pdf

[3] http://www.fox.temple.edu/cms/wp-content/uploads/2014/11/White-Paper-for-Privacy-in-an-Era-of-Big-Data-Workshop.pdf

In FY 2015, SaTC focused 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 in FY 2015 and FY 2016 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.

Following a FY 2014 Cybersecurity Education workshop[4] that brought together computer science educators and cybersecurity researchers, NSF funded high-risk/high-reward collaborative projects to develop innovative approaches to advance cybersecurity education.

Broadening the SaTC research community is critical to facilitating advances in cybersecurity research. Building on the successes of workshops held in FY 2013 and FY 2014, a third workshop for aspiring SaTC principal investigators (PIs) was held in FY 2015. The goal was to educate potential SaTC researchers on the priorities of the program and components of successful research projects. In FY 2016, NSF will continue to use this approach to bring new researchers with a broad set of talents and interests into the SaTC PI community.

NSF convened its second biennial principal investigators' (PI) meeting, bringing together over 400 NSF-funded cybersecurity researchers and educators along with representatives from industry, and government, including other federal agencies. The PI meeting served as an opportunity for assessing progress through previous and active cybersecurity research and education investments, and to identify emerging directions including novel interdisciplinary areas. In addition, in order to facilitate transition of research to practice, a session at this PI meeting was dedicated to educating SaTC PIs about other NSF programs that focus on transition to practice, such as the Accelerating Innovation Research (AIR) activity within NSF's Partnerships for Innovation (PFI) program and NSF Innovation Corps (I-Corps™).

In FY 2015 and FY 2016, NSF continued its partnerships with industry in the domain of cybersecurity. In FY 2015, NSF and Intel Corporation jointly funded two large-sized projects with the goal to foster novel, transformative, multidisciplinary approaches that ensure the security of current and emerging cyber-physical systems. NSF also partnered with the Semiconductor Research Corporation (SRC) in FY 2015 and FY 2016 through the Secure, Trustworthy, Assured and Resilient Semiconductors and Systems (STARSS) perspective within the SaTC solicitation. NSF and SRC are jointly funding projects 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 and FY 2016, 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. This partnership is yielding international teams that are seeking to enhance the security and trustworthiness of cyberspace in the long term.

### <u>FY 2017 Request</u>

The following activities are planned:

- The SFS program will be expanded and will lay groundwork for SFS alumni to be available over the course of their careers to serve the federal government to help rapidly respond to cybersecurity challenges.
- SaTC will continue to fund innovative projects in the science of security and privacy, security for cloud computing, as well as big data analytics for cybersecurity, improved cryptographic algorithms, and software engineering for cybersecurity.

[4] https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf

- SaTC will also support research on the security of cyber-physical systems, as well as low-cost and/or low-effort approaches for securing systems such as web services and the emerging Internet of Things (IoT)
- SaTC will coordinate with the NSF-wide CEMMSS investment and will include a focus on secure advanced manufacturing (including cyber-manufacturing) systems, robotics, and critical infrastructure such as smart grids.
- NSF will build upon existing, and develop new, partnerships with other federal agencies, industry, and international organizations to effectively achieve long-term goals related to SaTC.
- NSF will continue growing the cybersecurity research community to include more researchers who cross the boundaries between computer science, engineering, social, behavioral, and economic sciences, statistics, and mathematics.
- SaTC also will continue to focus on transitioning to practice research results ready for experimental deployment, early adoption, commercial innovation, or implementation in cyberinfrastructure through support of TTP projects. NSF will also support at least one experimental testbed to enable cybersecurity researchers to experiment in realistic environments.
- As part of SaTC's goal to enhance the capacity of the U.S. higher education enterprise to produce cyber professionals to meet societal needs, the investment will support initiatives by diverse groups of computing professionals representing academic institutions and professional societies to develop curriculum guidelines and a case for accreditation for a baccalaureate in "Cyber Science." It is expected that the Accreditation Board for Engineering and Technology, Inc. (ABET) will introduce this new accreditation in FY 2018, and that it will become a parent domain for the cybersecurity field.
- Additionally, SaTC 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.
- SaTC will also support education and professional development through a new Transition to Education (TtE) mechanism. Through TtE, research results in the science of cybersecurity and designed-in security will be incorporated into relevant course curricula that will be implemented, assessed, and improved in a variety of settings. Such efforts will be supported using TtE supplements and options. TtE will be analogous to the Transition to Practice component of SaTC.
- SaTC will continue to build the cybersecurity research community by holding the next in a series of biennial PI meetings with representation from academe, industry, and government, including other federal agencies, focusing on the science of cybersecurity and novel interdisciplinary areas of research. The PI meeting will continue to showcase successful TTP/AIR/I-Corps™ projects resulting from SaTC investments. NSF also will hold a PI meeting with cybersecurity for cyber-physical systems awardees to review progress and identify critical unaddressed problems and directions.

### FY 2018 and Beyond

Building on the knowledge base developed during the previous years, NSF plans to continue to focus on game-changing research and education, and the development of digital systems that are resistant to attacks through the SaTC program. In coordination with the NSF-wide CEMMSS investment and its successor activities, SaTC will include a focus on secure advanced manufacturing systems, robotics, and critical infrastructure such as smart grids. 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 achieve its long-term goals effectively. The cybersecurity research community is expected to continue growing to include more researchers who cross the boundaries between computer science, engineering, economics, social and behavioral sciences, statistics, and mathematics.

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 NSF expects to receive a final report in FY 2016.

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

- STPI held meetings with the SaTC working group and SaTC management to examine the past and current award portfolios, including an assessment of the components of the portfolio by technical and scientific content. In addition, as part of this portfolio analysis, STPI synthesized various recommendations from federal advisory boards and stakeholder communities on how to structure future cybersecurity investments.
- STPI developed a logic model 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 fundamental principles).

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

The Office of Personnel Management's Human Resources Solution (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 this evaluation.

Going forward, program monitoring and evaluation activities will be coordinated to reduce the burden on principal investigators, scholarships 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.[5]

[5] www.gao.gov/assets/590/586494.pdf