## 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 trustworthy cyberspace is a critical challenge as corporations, agencies, national infrastructure, and individuals have been victims of cyber-attacks, 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 research for years to come. It will also broaden the research portfolio through multi-disciplinary projects with expertise in computer, computational, statistical, mathematical, social, behavioral, and economic sciences to better understand, for example, the motivations and incentives of individuals and institutions, both as attackers and defenders, in creating a more cybersecure society. New innovative approaches are needed to educate and prepare tomorrow's cybersecurity researchers and professionals with the skills and knowledge necessary to continue to build the knowledge base and to secure a trustworthy cyberspace.

**Total Funding for SaTC**

(Dollars in Millions)

| FY 2013<br>Actual | FY 2014<br>Estimate | FY 2015<br>Request |
|---|---|---|
| **$108.01** | **$124.75** | **$99.75** |

**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 *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 Directorate for Computer and Information Science and Engineering (CISE) leads this cross-agency effort; other participating directorates include Education and Human Resources (EHR), Engineering (ENG), Mathematical and Physical Sciences (MPS), and Social, Behavioral, and Economic Sciences (SBE). 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) comprising 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 2,000 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, which enhances the capacity of the United States 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 and provides a forum for information sharing and cross-agency agenda setting. In addition, NSF and the Department of Education 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; 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 will address the pivotal issues in the education and preparation of tomorrow's cybersecurity researchers. Specific objectives are:
- 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 2013<br>Actual | FY 2014<br>Estimate | FY 2015<br>Request |
|---|---|---|---|
| Computer and Information Science and Engineering | $59.00 | $70.00 | $67.00 |
| Education and Human Resources | 41.26 | 45.00 | 25.00 |
| Engineering | 3.25 | 3.75 | 3.25 |
| Mathematical and Physical Sciences | 0.50 | 2.00 | 0.50 |
| Social, Behavioral, and Economic Sciences | 4.00 | 4.00 | 4.00 |
| **Total** | **$108.01** | **$124.75** | **$99.75** |

Totals may not add due to rounding.

### FY 2013 – FY 2014

In FY 2013, ENG and EHR joined CISE, MPS, and SBE in the revised SaTC solicitation, which included a third perspective on cybersecurity education (in addition to the existing trustworthy computing (TwC) and SBE perspectives). SaTC funded 34 small projects, 13 medium projects, three Frontier projects, 13 CAREER projects, and five workshops in FY 2013. Of these awards, 40 focused on the development of the scientific and engineering foundations for digital systems that can resist attacks; approximately another 15 focused on developing the scientific foundations to understand how individuals, groups, organizations, and other actors make decisions in the realm of cybersecurity; 19 were SFS projects; and 11 were SaTC Education Perspective projects with the aim to promote innovation, development, and assessment of new learning opportunities and to create and sustain an unrivaled cybersecurity workforce.

In FY 2014, CISE, EHR, ENG, MPS, and SBE again jointly issued the SaTC solicitation to continue to elicit research and education proposals that will expand the research and development of secure and trustworthy cyberspace. NSF will also continue 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.

In an effort to further collaborations between the CISE and SBE research communities, a cyber café-style workshop was held in FY 2013 that brought together economists, social scientists, and computer scientists to discuss cyber-economic and behavioral incentives research problems. NSF funded ten Early-concept Grants for Exploratory Research (EAGER) awards as a result of this workshop. Additional investments are anticipated in FY 2014. To encourage more multidisciplinary research in privacy, NSF issued a Dear Colleague Letter in FY 2014 encouraging the submission of proposals that specifically address the need to develop new and deeper fundamental understandings of privacy in today's networked world.

In FY 2013, NSF developed a National Virtual Lab for Cybersecurity Education to promote collaboration and resource sharing. The lab consists of a main hub at West Point and five additional hubs in Colorado, Hawaii, California, Virginia, and Mississippi. In FY 2014, NSF will expand the National Virtual Lab and add a cyber-operations function. In FY 2014, CISE and EHR have jointly sponsored a workshop that brings together computer science educators and cybersecurity researchers to discuss more innovative approaches to advance cybersecurity education. NSF will also support large-scale cybersecurity competitions through collaborations with California State Polytechnic University Pomona’s National Cybersecurity Sports Federation.

Several workshops focused on cybersecurity research are planned for FY 2014. NSF will hold a Science of Cybersecurity workshop that focuses on specific problems (e.g., metrics, fundamental results, evidence-based research, and protection of critical infrastructure) in the scientific foundations of cybersecurity. In FY 2014, NSF will also hold a “Cybersecurity 2025” workshop for the research community to develop long-term research agendas, as well as to review how SaTC has addressed the federal strategic plan.

A novel workshop for “Aspiring SaTC Principal Investigators (PIs)” was held in FY 2013 and will be repeated in FY 2014. The goal is to educate potential SaTC researchers on the priorities of the program and components of successful research projects. NSF will continue to bring new researchers with a broad set of talents and interests into the SaTC PI community.

**FY 2015 Request**

The following activities are planned:

- Create a new size category of projects – “Large” (up to $3.0 million in total budget and up to five years in duration), which would provide portfolio balance and allow for investments in a diverse set of collaborations focused on large-scale TwC, or large-scale SBE, or integrated TwC/SBE projects to emerge.
- Building on results of the FY 2014 Science of Cybersecurity workshop, fund projects that focus on the scientific foundations of cybersecurity.
- Hold a cross-agency workshop that reviews progress made in developing a science of cybersecurity, and that proposes ways that needs and results can be better communicated across the agencies, academics, and industry.
- Coordinate with the Cyber-physical Systems (CPS) program in funding projects for the protection of critical infrastructure.
- Fund community infrastructure and/or testbed projects for cybersecurity to accelerate innovation.
- Continue to fund projects on fundamental research in privacy.
- Develop a long-term roadmap and start to implement new programs and activities to achieve those goals, which are based on recommendations resulting from the “Cybersecurity 2025” workshop.
- Hold a workshop, open to the SaTC PI community, focused on transitions to practice; highlighting successful transitions and developing innovative ways to accelerate transitions in the future.
- Continue the strong focus in the SFS solicitation 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. In addition to the $25.0 million requested for SFS, $20.0 million is included in the Opportunity, Growth, and Security Initiative (OGSI).
- Hold a PI meeting with interagency representation, focusing on the science of cybersecurity and novel interdisciplinary areas of research.
- In collaboration with EHR, focus on new ways to promote innovation, development, and assessment of new learning opportunities in order to create and sustain an unrivaled cybersecurity workforce.

**FY 2016 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 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. SaTC will develop partnerships with other 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 among 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. During FY 2013, a portfolio characterization was completed and an initial logic model was developed. An evaluation framework is being established and is expected to be in place by the first quarter of FY 2015. Based on the results, NSF and a third-party contractor will develop the appropriate plan for assessing progress across NSF's SaTC activities.

The Office of Personnel Management (OPM), Human Resources Strategy & Evaluation Solutions (HRS) has completed the evaluation of the SFS program with a final report due in 2014. Focusing on the program's scholarship and capacity building tracks, the two year study links SFS program goals and objectives with inputs, activities, data sources, measures, outputs, and desired outcomes and has been underway since December 2011. The current study builds on a previous evaluation that was released in January 2008 by OPM's Assessment Services Branch. The current quantitative and qualitative mixed method study draws on the NICE framework and includes a gap analysis, focus groups interviews, stakeholder surveys, workforce analysis, and contextual information. The current program evaluation response rates for program graduates (62 percent) and current students (66 percent) will inform the development of strategies to increase response rates of (1) recipients who are beginning and completing their program of study, (2) recipients as they graduate, and (3) recipients as they complete their service obligation. The program's goal is to obtain a response rate of 100 percent for each of the three recipient groups.

To further enhance program monitoring and to address the issues raised by the GAO report (Cybersecurity Human Capital: Initiatives Need Better Planning and Coordination, GAO-12-8, November

2011), NSF has acquired the services of OPM HRS to develop and administer a web-based annual survey requesting information from SFS program scholarship recipients. This effort supports the infrastructure necessary for annual data collection. The SFS program now requires recipients to submit information at specific programmatic milestones: initial scholarship/fellowship award; completion of internship/graduation; completion of service obligation; and every year for ten years after completion of the service obligation. The data collection will start in Spring 2014 for new recipients and in Fall 2014 for recipients with ongoing support and former recipients. To document retention in the public sector, information will be collected and linked by individual and securely held and archived by the Organizational Assessment Section of OPM.