## SECURE AND TRUSTWORTHY CYBERSPACE (SaTC) $128,340,000

**-$5,990,000 / -4.5%**

**SaTC Funding**
(Dollars in Millions)

| | FY 2018<br>Actual | FY 2019<br>(TBD) | FY 2020<br>Request |
|---|---|---|---|
| CISE | $70.50 | - | $65.00 |
| EHR | 55.09 | - | 55.09 |
| ENG | 3.25 | - | 3.25 |
| MPS | 1.49 | - | 1.00 |
| SBE | 4.00 | - | 4.00 |
| **Total** | **$134.33** | **-** | **$128.34** |

### Overview

In today's increasingly networked, distributed, and asynchronous world, cybersecurity involves hardware, software, networks, data, people, and integration with the physical world. Seemingly overnight, society has become deeply reliant on the smooth functioning of its digital infrastructure. Unfortunately, attacks on corporations, agencies, national infrastructure, and individuals have exposed the fragility and vulnerability of this complex cyberspace. Achieving a truly secure cyberspace requires addressing not only challenging scientific and engineering problems involving many components of a system, but also vulnerabilities that arise from human behaviors and choices. Examining the fundamentals of security and privacy as a multidisciplinary subject is the most promising approach to develop better ways to design, build, and operate cyber systems; to protect existing and future infrastructure; and to motivate and educate individuals about cybersecurity. Achieving these goals not only requires expertise in computer science, engineering, statistics, mathematics, social, behavioral, and economic sciences, and education research, but also the translation of new concepts and technologies into practice.

SaTC is a multi-year investment area that began in FY 2012 and must evolve continuously to address new threats. Outcomes from SaTC include an organized scientific body of knowledge that informs the theory and practice of cybersecurity and privacy, and an improved understanding of the causes of and mitigations for current threats. SaTC contributes to the development of foundational countermeasure techniques leveraging sound mathematical and scientific foundations, principled design methodologies, and socio-technical approaches that consider human, social, organizational, economic, and technical factors, as well as design metrics for evaluating success or failure of these approaches. In the space of training and education, SaTC makes recommendations for new instructional materials, degree programs, and educational pathways. Foundational research in SaTC leads to a research community pursuing a broad and deep multidisciplinary research portfolio spanning cybersecurity and privacy, whose results underlie methods for securing critical infrastructure. Ultimately, through SaTC, NSF expects to produce an innovation ecosystem that ensures (a) new and existing technologies are secure from attacks and (b) users' information is protected from violations of privacy despite new attack surfaces that these technologies may present. Similarly, the creation of an American workforce and citizenry with an understanding of cybersecurity and privacy issues is one of the benefits of NSF's support for activities related to the education and training of cybersecurity researchers and professionals. As the goals of SaTC contribute to national security, NSF plans to continue investments in this area for the forseeable future.

**Goals**

1. Foundational Research: Develop the scientific theory, methodologies, and tools necessary for the development of trustworthy and usably secure systems and appropriate privacy safeguards.
2. Accelerating Transition to Practice: Transition successful fundamental research results and innovations into early adoption and use, and allow 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.
3. Education and Preparation of Cybersecurity Researchers and Professionals: Increase the number of qualified American students who pursue degrees in cybersecurity and privacy and enhance the capacity of institutions of higher education to produce professionals in these fields to meet the needs of our increasingly technological society. This goal also includes NSF's investment in the CyberCorps®: Scholarship for Service (SFS) program, which supports cybersecurity education and workforce development.

**FY 2020 Investments**

Goal 1: Foundational Research

- NSF will issue a revised SaTC solicitation for FY 2020. SaTC will continue to fund innovative projects that advance the science of cybersecurity and privacy, with emphases on: sociotechnical aspects; "blue sky" approaches to security and privacy; artificial intelligence (AI) as a tool for cybersecurity; security of AI and machine learning (ML) systems, including adversarial ML; implications of quantum computing for security, including post-quantum cryptography; and architectures and technologies for protecting cyberspace from the ever-growing smart-and-connected commodity devices.
- NSF will issue a separate solicitation under the SaTC umbrella in FY 2020 for center-scale efforts that address "grand challenge" research areas in cybersecurity and privacy.
- NSF will build upon existing and develop new partnerships with other federal agencies, industry, and international organizations to more effectively achieve the SaTC program's long-term goals. Towards this end, NSF will support a Research Coordination Network (RCN) that focuses on fostering international collaborations between US-based researchers and their counterparts in other countries.
- NSF will pursue additional efforts to grow the cybersecurity research community to include more researchers who cross the boundaries between computer and information science and engineering, engineering, the social, behavioral, and economic sciences, mathematics, statistics, and education research. For example, NSF may issue a Dear Colleague Letter that will focus on bringing together computer and information scientists and engineers with social, behavioral, and economic scientists to enable early-stage, socio-technical advances in cybersecurity and privacy. In addition, NSF will hold workshops on a range of cutting-edge topics, including novel applications of blockchain, as well as security and privacy challenges in smart infrastructure, autonomous, and AI-based systems.

Goal 2: Accelerating Transition to Practice (TTP)

- SaTC will continue its focus on TTP research results ready for experimental deployment, early adoption, commercial innovation, and/or implementation in cyberinfrastructure through support of TTP-designated projects.
- In FY 2020, SaTC plans to fund an industry-academic RCN to foster stronger collaboration between academic researchers and industry.

Goal 3: Education and Preparation of Cybersecurity Researchers and Professionals

- SaTC will continue the focus on cybersecurity education in FY 2020, with the aim of creating and sustaining an unrivaled American cybersecurity workforce capable of developing secure cyberinfrastructure components and systems and raising the awareness of cybersecurity challenges across the entire American population.

- SFS will increase outreach to the K-12 community, supporting efforts such as summer camps and a cybersecurity element within NSF's K-12 computer science education portfolio.
- NSF will encourage and incentivize SFS institutions to participate in task forces on the cybersecurity workforce at the state level and explore possible private-public partnerships. SFS will include community colleges in the types of institutions eligible for awards.
- SFS will continue to support the GenCyber project on SFS campuses.