SECURE AND TRUSTWORTHY CYBERSPACE (SaTC)

SaTC Funding
(Dollars in Millions)

	FY 2019 Actual	FY 2020 (TBD)	FY 2021 Request
CISE	$70.22	-	$65.00
EHR	55.33	-	52.13
ENG	3.25	-	3.03
MPS	1.70	-	0.95
SBE	4.00	-	3.80
Total	**$134.50**	**-**	**$124.91**

Overview

In today's increasingly networked, distributed, and asynchronous world, society is deeply reliant on the smooth functioning of its digital infrastructure—and the security of that infrastructure (also known as cybersecurity) involves hardware, software, networks, data, people, and integration with the physical world. Recent events have exposed the dual nature of cyberspace: while it is an unprecedented source of innovation, efficiency, and growth, it also brings the potential for attacks on enterprises, loss of privacy, and even erosion of trust in democratic institutions. Indeed, key components of the digital infrastructure were not designed to operate in a hostile environment with intentional adversaries. Achieving a truly secure and trustworthy cyberspace therefore requires addressing not only challenging scientific and engineering problems involving many components of a complex system, but also issues that arise from human behaviors and choices. Examining the fundamental principles of security and privacy as a multidisciplinary subject constitutes a 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 continuously evolves to address new threats. SaTC is aligned with the 2019 *Federal Cybersecurity Research and Development Strategic Plan*,[1] which was developed pursuant to the Cybersecurity Enhancement Act of 2014 (P.L. 113-274), and the Presidential Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[2] 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. Ultimately, through SaTC, NSF funds a broad and deep multidisciplinary research and education portfolio spanning cybersecurity and privacy, whose results underlie methods for securing critical infrastructure. Further, NSF expects to produce an innovation ecosystem that ensures (a) new and existing technologies are secure from both current threats and potential future threats as technologies evolve, and (b) users' information is protected from violations of privacy despite new attack surfaces that

[1] www.nitrd.gov/cybersecurity/index.aspx - FedCyberR&DStratPlan2019
[2] www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

these technologies may present. Similarly, the development of an American workforce and citizenry with an understanding of cybersecurity and privacy issues is a key benefit of NSF's support in this area. As the goals of SaTC contribute to national security, NSF plans to continue investments in this area for the foreseeable future.

Importantly, SaTC also supports cybersecurity and privacy for the Industries of the Future (IoTF) through research investments, for example, in threats and countermeasures in the context of advanced wireless networks; artificial intelligence (AI) as a tool for cybersecurity; security of AI and machine learning (ML) systems, including adversarial ML; and the implications of quantum computing for security, including post-quantum cryptography.

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 that account for the role of human behavior and decision-making.
2. *Accelerating Transition to Practice (TTP)*: 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 digital society. This goal also includes NSF's investment in the CyberCorps®: Scholarship for Service (SFS) program.

FY 2021 Investments

Goal 1: Foundational Research

- NSF will issue a revised SaTC solicitation for FY 2021 that is aligned with the 2019 *Federal Cybersecurity Research and Development Strategic Plan*. Through this revised solicitation, NSF will continue to fund innovative projects that advance the science of cybersecurity and privacy, with emphases on: architectures and technologies for protecting cyberspace from increasingly sophisticated connected devices; security and privacy aspects of smart infrastructure including the Internet of Things, and security and privacy for IoTF as described above.
- NSF will continue its efforts to grow the cybersecurity research community to include more researchers who cross the boundaries between computer and information science, engineering, the social, behavioral, and economic sciences, mathematics, statistics, and education research. In support of this specific aim, NSF will hold a range of workshops on cutting-edge topics. For example, NSF plans to develop a series of workshops and summer schools that will explore the role of security in the quantum computing era.
- In FY 2021, NSF plans to fund a SaTC Research Coordination Network (RCN) on propagation of information in cyberspace and methods of reliably detecting "deep fakes" and inferring provenance of such misinformation, especially in the context of images, audio, and video.

Goal 2: Accelerating Transition to Practice

- NSF will continue its focus on transitioning to practice research results that are ready for experimental deployment, early adoption, commercial innovation, and/or implementation in cyberinfrastructure. NSF will also continue to support research infrastructure in security and privacy in conjunction with the CISE Community Research Infrastructure program.

- In FY 2021, NSF plans to develop an industry-academia RCN, separate from the one described above, to foster stronger collaboration between academic researchers and industry.

Goal 3: Education and Preparation of Cybersecurity Researchers and Professionals

- In alignment with the Presidential Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, NSF will continue the focus on cybersecurity education in FY 2021, with the aims of building and sustaining an American cybersecurity workforce that is unrivaled in its ability to develop secure cyberinfrastructure components and systems, and raising the awareness of cybersecurity challenges across the entire American population.
- CyberCorps®: SFS will prioritize investments in K-12 education with the aim of growing interest in cybersecurity careers, promoting foundational cybersecurity principles and safe online behavior, improving teaching methods for delivering cybersecurity topics within computer science curricula, and promoting teacher recruitment in the field of cybersecurity. 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 support innovative approaches to workforce re-skilling, apprenticeships, cooperative learning opportunities, and practice-oriented models for training.
- In support of the 2019 *Federal Cybersecurity Research and Development Strategic Plan* and the Presidential Executive Order on *America's Cybersecurity Workforce*,[3] SFS will address a critical shortage of cybersecurity educators and researchers including in priority areas such as the cybersecurity aspects of AI, quantum information science, and advanced wireless networks.

[3] www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/