SECURE AND TRUSTWORTHY COMPUTING (SaTC)

SaTC Funding[1]
(Dollars in Millions)

	FY 2020 Actual	FY 2021 Estimate	FY 2022 Request
CISE	$70.94	$69.50	$74.50
EHR	55.00	60.00	70.00
ENG	3.25	3.25	3.25
MPS	1.18	1.25	1.25
SBE	4.00	4.00	4.00
Total	**$134.37**	**$138.00**	**$153.00**

[1] Funding displayed may have overlap with other topics and programs.

Overview

In today's increasingly networked, distributed, and asynchronous world, society is deeply reliant on 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 and information science; engineering; mathematics; statistics; the social, behavioral, and economic sciences; and education research, but also the transition 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 cybersecurity threats. SaTC is aligned with the 2019 *Federal Cybersecurity Research and Development Strategic Plan*, which was developed pursuant to the Cybersecurity Enhancement Act of 2014 (P.L. 113-274). 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 these technologies may present. Similarly, NSF's support in this area will lead to the development of an American workforce and citizenry with an understanding of cybersecurity and privacy issues. As the goals of SaTC contribute to national security, NSF plans to continue investments in this area for the foreseeable 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 that account for the role of human behavior and decision making.
2. *Accelerating Transition to Practice (TTP)*: Transition promising 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 includes NSF's investment in the CyberCorps®: Scholarship for Service (SFS) program.

FY 2022 Investments

Foundational Research

- NSF will issue a revised SaTC solicitation in FY 2022 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 and engineering of cybersecurity and privacy, with emphases on: security and privacy aspects of pandemic-related technologies including new threats in the virtual setting; security and reliability of 5G and Beyond wireless networks; methods of reliably detecting "deep fakes" and inferring provenance of such misinformation, especially in the context of images, audio, and video; radio-frequency (RF)/analog hardware electronics and supply chain security; implications of quantum computing for security, including post-quantum cryptography; developing new architectures, systems, and technologies for protecting cyberspace from new and increasingly sophisticated attacks including adversarial machine learning; and security of smart infrastructure including the Internet of Things (IoT) and advanced manufacturing.
- 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; mathematics; statistics; the social, behavioral, and economic sciences; 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 and privacy in the healthcare information technology infrastructure as well as the next generation of wireless networks beyond 5G. Additionally, NSF anticipates one or more workshops examining security and privacy needs associated with sharing government data with researchers.
- In FY 2022, NSF will continue to explore the role of cybersecurity and privacy research in future pandemics through a virtual organization established in FY 2020 that engages researchers, industry, government, and other stakeholders. This organization will hold a series of workshops to encourage research collaborations with the aim of generating a community-driven research roadmap that identifies key research challenges and directions.
- NSF will invest in research to analyze the flow of information and to mitigate the impacts of false or misleading information in online and other computer-mediated systems. Topics will include detecting, mitigating, and countering threats to accurate information, and understanding the interactions of people with information systems. This research includes analyzing factors that influence trust in communications, and understanding the motivations and behaviors of actors creating and transmitting misinformation and disinformation. NSF will promote multi-disciplinary research collaborations that will enable enhancements to the integrity of U.S. information systems, for example, by helping to

counter foreign and extremist influence on social media and to enhance the flow of accurate information to support public health and a thriving economy.

Accelerating TTP

- 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 through support of TTP-designated projects. NSF will also continue to support research infrastructure in security and privacy in conjunction with the CISE Community Research Infrastructure program.

Education and Preparation of Cybersecurity Researchers and Professionals

- In support of the 2019 *Federal Cybersecurity Research and Development Strategic Plan*, NSF will continue its focus on cybersecurity education in FY 2022, with the aims of (i) building and sustaining an unrivaled cybersecurity workforce; (ii) promoting the development and maintenance of inclusive learning settings to improve diversity in cybersecurity; and (iii) raising cybersecurity awareness across the general population.
- CyberCorps®: SFS will address a critical shortage of cybersecurity educators and researchers by preparing up to 80 SFS scholars to fulfil their service obligation as cybersecurity faculty members; continuing support of collaborative efforts among the AI, cybersecurity, and education research communities to foster a robust workforce with integrated AI and cybersecurity competencies; and exploring new collaborations at the intersection of cybersecurity and other priority areas such as quantum information science and engineering as well as next-generation wireless networks.
- CyberCorps®: SFS will accelerate 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 to help K-12 teachers integrate cybersecurity into formal and informal learning settings; and promoting teacher recruitment in the field of cybersecurity.
- NSF will address cybersecurity education and workforce development challenges emerging as a result of the COVID-19 pandemic, including the security, reliability, and privacy of a teleworking and online learning society; cloud services, digitization, and contact-free processes; cyber awareness against opportunistic cybercrime; innovation in incident handling; cyber-enterprise risk management; and societal resilience to misinformation and related activities.