SECURE AND TRUSTWORTHY CYBERSPACE (SaTC)

SaTC Funding[1]
(Dollars in Millions)

	FY 2021 Actual	FY 2022 (TBD)	FY 2023 Request
CISE	$70.81	-	$75.81
EDU[2]	59.99	-	75.00
ENG	3.25	-	3.25
MPS	1.26	-	1.25
SBE	4.00	-	4.00
Total	**$139.31**	**-**	**$159.31**

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

[2] Formerly known as Directorate for Education and Human Resources (EHR).

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 an interdisciplinary 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,*[1] 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 and mitigations of 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 supports education research that leads to

[1] www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf

the development of new instructional materials, degree programs, and educational pathways, for example from the undergraduate sector into the cybersecurity workforce. Ultimately, through SaTC, NSF funds a broad and deep interdisciplinary 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. *Fundamental 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 and privacy solutions and moving them into operational environments.
3. *Education and Preparation of Cybersecurity and Privacy 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 2023 Investments

Fundamental Research

- NSF will issue a revised SaTC solicitation in FY 2023 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 global software supply chain; in virtual, augmented, and extreme

reality; and in 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 2023, NSF will continue to explore the role of cybersecurity and privacy research in future pandemics through the Pandemic Research for Preparedness and Resilience (PREPARE) Virtual Organization (VO)[2] that was established in FY 2020 to engage researchers, industry, government, and other stakeholders. To encourage research collaborations, the PREPARE VO will continue to hold workshops to identify future research directions and run the Science Before the Storm podcast exploring the frontiers of pandemic research. The VO serves as a resource to the community by conducting an annual meeting of researchers working in pandemic related challenges, providing links to data sets and upcoming workshops of interest, and disseminating all information collected as a result of this project with the aim of generating a community-driven research roadmap that identifies key research challenges and directions to bolster resilience and prepare the community for the next pandemic.
- In May 2021 NSF held a workshop in collaboration with NIH on "Establishing the Roadmap for Security, Privacy, and Ethics in Health and Biomedical Research"[3] that brought together leading researchers and stakeholders from the computing and information as well as the health and biomedical research fields to establish the vision and create a roadmap for security, privacy, and ethics in the intersection of computing health/bio-medical research. NSF will consider activities or new funding initiatives based on the roadmap produced by this workshop.
- NSF is working with the White House Office of Science and Technology Policy (OSTP), and the National Institute of Standards and Technology (NIST) to lead an interagency initiative to jointly develop, with the United Kingdom, prize challenges in the area of privacy enhancing technologies (PETs).[4] These PETs present an important opportunity to harness the power of data in a manner that protects privacy and intellectual property and enables cross-border and cross-sector collaboration to accelerate work to overcome technical gaps and adoption challenges. This effort was also motivated by the discussion in the NSF-NIST workshop "To Develop a Roadmap for Greater Public Use of Privacy-Sensitive Government Data" [5] held in May 2021, which focused more broadly on impediments to broader use of government data.
- NSF issued a DCL in February 2022 that invites proposals related to information integrity including detecting, mitigating, and countering threats to accuracy of information, and understanding the interactions of people with information systems. In FY 2023 NSF will continue to invest in information integrity research to analyze, among other areas, the flow of information and to mitigate the impacts of manipulated information in online and other computer-mediated 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 interdisciplinary research collaborations in information integrity 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.

[2] https://prepare-vo.org/events

[3] https://sites.rutgers.edu/idsla/spe-in-healthcare/

[4] www.whitehouse.gov/ostp/news-updates/2021/12/08/us-and-uk-to-partner-on-a-prize-challenges-to-advance-privacy-enhancing-technologies/

[5] https://may2021privacy.github.io/

Accelerating TTP

Through the SaTC program and in collaboration with TIP, 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. These projects must demonstrate how technology from prior successful research results will be deployed into an organization, system, or community. The outcome of a TTP-designated project should be demonstrable advancement in the technology's readiness, robustness, validation, or functionality. 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 2023, with the aims of (a) building and sustaining an unrivaled cybersecurity workforce; (b) promoting the development and maintenance of inclusive learning settings to improve diversity in cybersecurity; and (c) raising cybersecurity awareness across the general population.
- In FY 2023 NSF will further expand or initiate new cybersecurity education programs), which improve education delivery methods for K-12 students, teachers, counselors, and post-secondary institutions and encourage students to pursue cybersecurity careers. NSF will provide education supplements to SaTC research projects, leveraging the original SaTC projects to rapidly transition advances in cybersecurity research to novel educational materials that can lead to new ways of teaching and learning cybersecurity concepts and principles and enable the co-evolution of cybersecurity curricula with the state-of-the-art in the cybersecurity body of knowledge. These supplements could focus on educational innovations at any level from K-12 to graduate school and are complementary to NSF's efforts to strengthen the national cybersecurity workforce pipeline via the CyberCorps®: SFS program highlighted below, and part of this program ($5.0 million) is also complementary to the Cyber Defense Education & Training program at the Cybersecurity and Infrastructure Security Agency.
- CyberCorps®: SFS will seek to increase investments in K-12 as well as post-secondary education) with the aim of growing interest in cybersecurity careers and their intersection with other key areas of national interest such as data science and AI. Such investments will promote learning of foundational cybersecurity principles and safe online behavior; develop curriculum materials and improve teaching methods to help K-12 teachers and college professors integrate cybersecurity and privacy into formal and informal learning settings; develop new knowledge on how people learn the concepts, practices, and ways of thinking in cybersecurity; and promote teacher recruitment in the field of cybersecurity. Part of this program ($5.0 million) is complementary to the Cyber Defense Education & Training program at the Cybersecurity and Infrastructure Security Agency.
- CyberCorps®: SFS will address a critical shortage of cybersecurity educators and researchers by preparing up to 10 percent of 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 privacy, and other priority areas such as quantum information science and engineering as well as next-generation wireless networks.

- With the aim of increasing the participation of populations traditionally underrepresented in the cybersecurity workforce, CyberCorps®: SFS will make investments to (a) understand barriers to diversity, equity, and inclusion at SFS institutions; and (b) implement best practices to address such barriers.