SECURE AND TRUSTWORTHY CYBERSPACE (SaTC)

Secure and Trustworthy Cyberspace Funding[1]
(Dollars in Millions)

	FY 2023 Base Plan	FY 2024 (TBD)	FY 2025 Request
CISE	$75.00	-	75.00
EDU	72.93	-	74.00
ENG	3.25	-	3.25
MPS	1.25	-	1.25
SBE	4.00	-	4.00
Total	**$156.43**	**-**	**$157.50**

[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 protecting the security of that infrastructure 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 economic 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 highly capable adversaries. Achieving a truly secure and trustworthy cyberspace therefore requires addressing not only scientific and engineering problems involving many components of a complex system, but also issues that arise from human behaviors and choices, as well as societal and cultural factors. Examining the fundamental principles of security and privacy as an inter- and multi-disciplinary 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 and privacy. Achieving these goals not only requires expertise in computer and information science; engineering; mathematics; statistics; the social, behavioral, and economic sciences; laws, policies, and regulations; and education research, but also the translation of new concepts and technologies into practice.

The SaTC program is a multi-year investment area that began in FY 2012 and continuously evolves to address new cybersecurity threats. SaTC is aligned with the 2023 *Federal Cybersecurity Research and Development Strategic Plan,*[1] which provides federal agencies guidance on the overall priorities for federally funded research and development in cybersecurity. Outcomes from SaTC include an organized scientific body of knowledge that informs the theory and practice of cybersecurity and privacy, an improved understanding of the causes and mitigations of current and potential threats, assessment, and mitigation of harms to individuals and society posed by cyber-threats, and investments in cybersecurity education research and workforce development.

[1] www.whitehouse.gov/wp-content/uploads/2024/01/Federal-Cybersecurity-RD-Strategic-Plan-2023.pdf

SaTC contributes to the development of foundational, preventative, and countermeasure techniques leveraging sound mathematical and scientific foundations, principled design methodologies, and socio-technical approaches that consider people, social, organizational, economic, and technical factors, as well as design metrics and measurement techniques for evaluating the efficacy or effectiveness of these approaches. This foundational research is paired with awards focusing on transitioning results into practice; collectively, NSF's security and privacy research portfolio seeks to ensure that (a) new and existing technologies are secure from both current, emerging, and potential future threats as technologies evolve, and (b) information about individuals and groups is protected from violations of privacy despite the new attack surfaces that these technologies may present.

SaTC also supports education research and workforce development activities that lead to the development of new instructional approaches and materials, degree programs, and educational pathways. These activities span educational and life stages. Work supported by SaTC focuses on helping middle and high schoolers to be more knowledgeable and interested in learning about cybersecurity topics; curricula and resources to advance undergraduate and graduate education related to trustworthy cyberspace; and training and education beyond formal educational systems, aimed at both the general public and at people already in the workforce. NSF's support in this area contributes to the development of a robust American workforce and citizenry with an understanding of broad cybersecurity and privacy issues.

Ultimately, through SaTC, NSF funds a broad and deep inter- and multi-disciplinary research and education portfolio spanning cybersecurity and privacy, whose results underlie methods for securing critical cyber and cyber-physical infrastructure. As the goals of SaTC contribute to national security and maintaining U.S. leadership in cybersecurity and privacy R&D, 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 building trustworthy and usably secure systems and appropriate privacy safeguards that account for the role of people's behavior and decision-making processes.
2. *Accelerating Translation to Practice (TTP)*: Translate promising fundamental research results to practice.
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. This goal includes NSF's investment in the CyberCorps®: Scholarship for Service (SFS) program.

FY 2025 Investments

<u>Fundamental Research</u>

- NSF is undertaking a major revision of the SaTC program in FY 2024 that will lead to a new solicitation in FY 2025. The new solicitation is intended to significantly broaden the scope of the SaTC program by including emerging scientific cybersecurity and privacy research areas, as well as activities around building infrastructure and community, that have been identified in conjunction with key stakeholders over the past few years (for instance, through a community-led

workshop assessing the current and future state of the field).[2] Through the revised solicitation, NSF will continue to fund innovative projects that advance the science and engineering of cybersecurity and privacy, with emphases on: 5G and Beyond wireless networks; integrity of information especially in the context of images, audio, and video; security of the open source ecosystem; learning enabled systems such as autonomous vehicles and robots; 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; ensuring the safety, security and robustness of AI/ML assisted systems; smart infrastructure including advanced manufacturing and precision agriculture; countering new threats in virtual and augmented reality (AR/VR); securing the next generation of hardware and semiconductors from fabrication to design to operation; and ensuring safety and security in biometric authentication while also preserving privacy.

- NSF will continue its efforts to grow the cybersecurity and privacy 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 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 cybersecurity and privacy in virtual, augmented, and extreme reality; biotechnology; post-Moore computing hardware, architectures, and systems; autonomous cyber defense; and robust and resilient wireless networks beyond 5G.
- In FY 2022, NSF was part of the Open-Source Software Security Initiative (OS3I) Working Group tasked by the National Cyber Director to engage public and private stakeholders to learn about risks and opportunities to improve the security of the open-source software ecosystem. NSF convened a workshop in the summer of 2022 with diverse representatives from the open-source software community, which resulted in a publicly released report[3] containing recommendations for the federal government. This activity directly aligned with the NSF Pathways to enable Open-Source Ecosystems (POSE) program discussed below. In FY 2023. NSF released a "Dear Colleague Letter" (DCL) seeking fundamental and applied research proposals to address Open Source Software (OSS) ecosystem security, targeting software engineering frameworks, unsafe legacy code, dependency management, trust and safety, incentive and organizations' structures, and education and workforce development. In FY 2024 and FY 2025, NSF expects to continue to support projects in response to the OSS DCL.
- In FY 2022, under the leadership of the White House Office of Science and Technology Policy (OSTP), NSF and the Office of the Director of National Intelligence led an interagency working group that developed a report that lays out a "Roadmap for Researchers on Priorities for Information Integrity Research and Development,"[4] published in December 2022. In alignment with this report, NSF released a Dear Colleague Letter (DCL)[5] encouraging the research community to submit novel and high impact proposals to the SaTC program that advance knowledge on the integrity of information. In FY2025 NSF will continue to encourage meritorious proposals on the priorities identified in the report.

[2] Draft Report: https://arxiv.org/pdf/2308.00623

[3] Keromytis, Angelos, D., "Recommendations from the Workshop on Open-Source Software Security Initiative," September 2022, OSSI-Final-Report.pdf.

[4] www.whitehouse.gov/wp-content/uploads/2022/12/Roadmap-Information-Integrity-RD-2022.pdf

[5] www.nsf.gov/pubs/2022/nsf22050/nsf22050.jsp

Accelerating Translation to Practice (TTP)

- Through the SaTC program, NSF will continue its focus on translating research results that are ready for experimental deployment, early adoption, commercial innovation, and/or implementation through supporting 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 focused efforts to mature technologies emerging from fundamental research. For example, in FY 2023, following the successful end of the Privacy-Enhancing Technologies (PETs) Prize Challenges, NSF is fostering collaborative efforts with OSTP, NIST, and the Government of the United Kingdom, to mature PETs to the point of demonstrating their viability in the context of specific use cases.
- NSF will also continue to support research infrastructure, including testbeds, in cybersecurity and privacy through the Community Infrastructure for Research in Computer Information Science and Engineering (CIRC) and POSE programs.

Education and Preparation of Cybersecurity Researchers and Professionals

- In alignment with the 2023 *Federal Cybersecurity Research and Development Strategic Plan*, NSF will continue its focus on cybersecurity education in FY 2025 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 2025, NSF will fund programs that lead to innovation and strengthen pathways for the national cybersecurity workforce at the K-12, community college, and four-year university levels. This funding is intended to expand or initiate programs that will improve access to and delivery of cybersecurity education for K-12 students, teachers, counselors, and post-secondary institutions while simultaneously encouraging students to pursue cybersecurity careers.
- The CyberCorps®: SFS program will address the nation's critical shortage of cybersecurity educators and researchers by allowing up to 10 percent of SFS scholars to fulfil their government service obligation through service as faculty members engaged in undergraduate- and graduate-level education in cybersecurity. SFS will also continue to support collaborative efforts among the AI, cybersecurity, and education research communities to foster a robust workforce with integrated AI and cybersecurity competencies; and explore new collaborations at the intersection of cybersecurity and privacy, as well as other priority areas such as quantum computing and aerospace as authorized by the CHIPS and Science Act of 2022.
- 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 at the 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 into the field of cybersecurity.
- With the aim of building inclusive environments and increasing the representation of students of all races, ethnicities, and genders earning cybersecurity graduate degrees, SFS will continue to make investments to (a) understand barriers to diversity, equity, and inclusion at SFS institutions; (b) implement best practices to address such barriers; and (c) empower SFS institutions to build

bridge programs that connect graduate degree-seeking individuals who are members of populations currently underrepresented in computing to advanced degrees in cybersecurity.