CyberCorps®

Defending America's Cyberspace

2025 **BIENNIAL REPORT**

CyberCorps® Scholarship For Service (SFS)

U.S. National Science Foundation | January 2026

TABLE OF CONTENTS

LETTER FROM DR. SYLVIA BUTTERFIELD, DIRECTORATE HEAD FOR STEM EDUCATION

For decades, the U.S. National Science Foundation (NSF) has funded research to protect national and personal security in today's highly connected, digital world.

Cybersecurity is critical for safeguarding the nation's digital infrastructure, keeping supply chains moving and ensuring the safety and privacy of personal data.

Achieving security in the cyber realm requires more than strengthening cyberinfrastructure — the hardware, software, networks, data and people that underpin today's computing technologies. It also requires continued vigilance as the threats posed by attackers and emerging technologies evolve.

To do this, NSF, in coordination with the U.S. Office of Personnel Management (OPM) and the Department of Homeland Security (DHS), launched the CyberCorps® SFS Program to recruit, train and grow the next generation of cybersecurity professionals. The program has experienced tremendous growth – from 31 students in 2001 to graduating more than 5000 scholars, who defend our nation's cyberspace by lending their expertise to federal, state, tribal and local organizations.

Many new technologies, including quantum computing and Artificial Intelligence (AI), present both risks and opportunities for a secure cyberspace.

This is why NSF, OPM and DHS officially integrated AI into the CyberCorps® SFS program, now referred to as CyberAICorps SFS (CybcerAI SFS). With this additional emphasis, the program will continue to expand its cybersecurity investments to include AI in a variety of projects – from undergraduate cybersecurity curriculum to expanding security research and training to space engineering and much more.

By building a workforce equipped to handle the rapidly changing cyber environment in this new era, the CyberAI SFS program is ensuring the nation's ability to address new and evolving threats.

In closing, it is my pleasure to announce the publication of the 2025 CyberCorps® SFS Program Biennial Report to Congress.

/s/
Sylvia Butterfield, EdD Directorate Head
Directorate for STEM Education (EDU)
U.S. National Science Foundation

CYBERCORPS® SFS PROGRAM OVERVIEW

In a digital era with rapid technological advancement, the role of cybersecurity education has never been more critical. Emerging technologies, such as Artificial Intelligence (AI) and quantum computing, are transforming every component of our society — from critical infrastructure and healthcare to national defense.

While these innovations offer unprecedented opportunities, they also introduce new risks to our digital society. This challenge demands a cybersecurity workforce equipped with advanced knowledge, critical thinking and adaptive skills. Training a competent workforce to understand and defend against these evolving threats is crucial for national security, economic prosperity and global leadership.

While AI is transforming how we detect and respond to cyber threats, adversaries leverage this powerful tool to launch AI-powered attacks that are faster, stealthier and more complex than traditional methods, such as deepfake deception and AI-generated phishing. These developments underscore the importance of training cybersecurity professionals for the era of agentic warfare who understand both the capabilities and the risks of AI technologies. Defenders are not just using AI, they must also secure their AI infrastructure against data poisoning, exfiltration and other threats introduced by AI-related attack surfaces. Quantum computing poses another critical challenge to cybersecurity. Although still in its early stages, quantum computers have the theoretical potential to break widely used encryption algorithms that protect sensitive data today. This calls for cybersecurity education in quantum-safe cryptography and a deep understanding of how quantum algorithms could impact secure communications and data protection.

Cybersecurity education must continue to evolve to meet the demands of this new era. It should integrate interdisciplinary training that spans AI, quantum computing and other emerging technologies. By cultivating a skilled cybersecurity workforce, we can ensure that our society not only leverages the power of emerging technologies but also can be safeguarded against evolving threats.

Presidential Directive 63 issued on May 22, 1998, envisioned the U.S. National Science Foundation (NSF) CyberCorps® Scholarship for Service (SFS) program. This directive marked a milestone in the endeavor to secure cyberspace and protect critical information systems. Subsequently, on January 8, 2000, the National Plan for Information Systems Protection was introduced as an initiative to devise a comprehensive strategy for safeguarding cyberspace.

The Cybersecurity Enhancement Act of 2014 codified the Federal Cyber Scholarship-for-Service Program (15 USC 7442) and laid the foundation for its expansion. This act was further amended by the National Defense Authorization Acts for 2018 and 2021, empowering NSF to collaborate with the U.S. Office of Personnel Management (OPM) and the Department of Homeland Security (DHS) to sustain and advance the CyberCorps® SFS program.

In 2020, the program began a transition to the era of AI. As required by the CHIPS and Science Act of 2022, the Director of NSF, in coordination with Director of OPM, submitted a report[1] to Congress, entitled "Artificial Intelligence Scholarship for Service Initiative: Need, Feasibility and Implementation," on the need, feasibility and implementation of an AI SFS program based on the CyberCorps® SFS model. Informed by the contents of that report, the program's name was changed to CyberAICorps Scholarship for Service (CyberAI SFS) and the first CyberAI SFS solicitation (NSF 26-503) was published in February 2026. The term CyberAI is meant to encompass AI for cybersecurity as well as the security and resilience of AI systems. In this report, we continue to use the program's legacy name, CyberCorps® SFS, because most of the reported activities occurred before the name change.

[1] https://nsf-gov-resources.nsf.gov/files/2024SFSAIReport-r.pdf

The CyberCorps® SFS program develops a cybersecurity workforce for the era of AI and aligns with national priorities at the intersection of cybersecurity and AI as outlined in America's AI Action Plan of 2025[2] and Executive Order 14277 "Advancing Artificial Intelligence Education for American Youth"[3] to prioritize AI within scholarship for service programs. Through collaborative efforts among various government entities, the CyberCorps® SFS program plays a critical role in cultivating a skilled cybersecurity workforce that is well-prepared to tackle the ever-evolving challenges of cyberspace. By nurturing cyber talent, the program helps the Nation to remain resilient in the face of cyber threats. For Fiscal Years 2024 and 2025, the CyberCorps® SFS budget was approximately $63 million and $72 million, respectively, for new or continuing SFS schools.

Originally, the CyberCorps® SFS program featured two distinct tracks. The first track, known as the Scholarship Track, provided funding to SFS institutions, enabling them to grant scholarships lasting up to three years to students pursuing undergraduate or graduate degrees in cybersecurity. All scholarship recipients are required to work after graduation in an approved organization in a position related to cybersecurity for a period equal to the duration of the scholarship.

The second track, referred to as the Capacity Building Track, had a goal of increasing the ability of the U.S. higher education enterprise to produce skilled cybersecurity professionals. From 2018 to 2025, the Capacity Building Track merged with the Education Designation (EDU) track of the NSF cross-agency Secure and Trustworthy Cyberspace (SaTC) program to promote engagement of a broad network of cybersecurity experts, researchers and educators. The EDU designation played a role in facilitating knowledge exchange and promoting cutting-edge cybersecurity education research. In 2026, the capacity building efforts returned to the CyberAI SFS program.

The first cohort of 31 CyberCorps® SFS students enrolled in Fall 2001. Over the years, the program has grown substantially with a total of 6,146 students enrolled since its inception. Figure 1 illustrates the number of students that were on active scholarship during any part of a specific calendar year since 2018. As of October 2025, a total of 5,341 talented individuals graduated from the CyberCorps® SFS program.

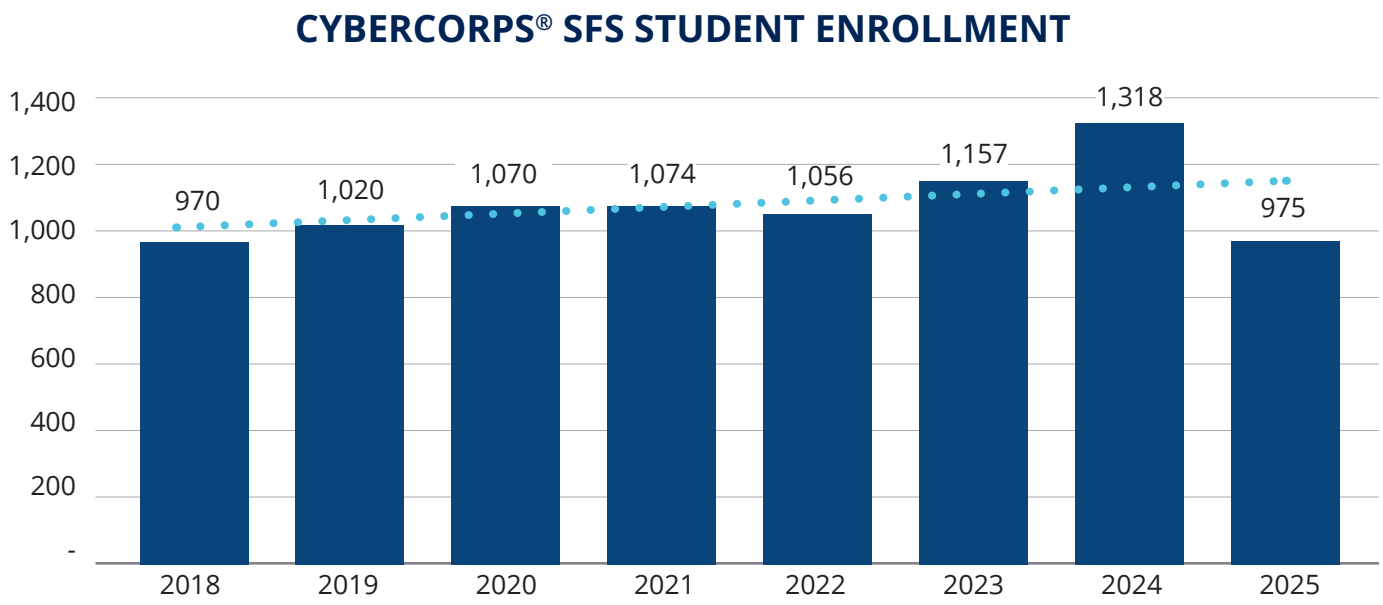
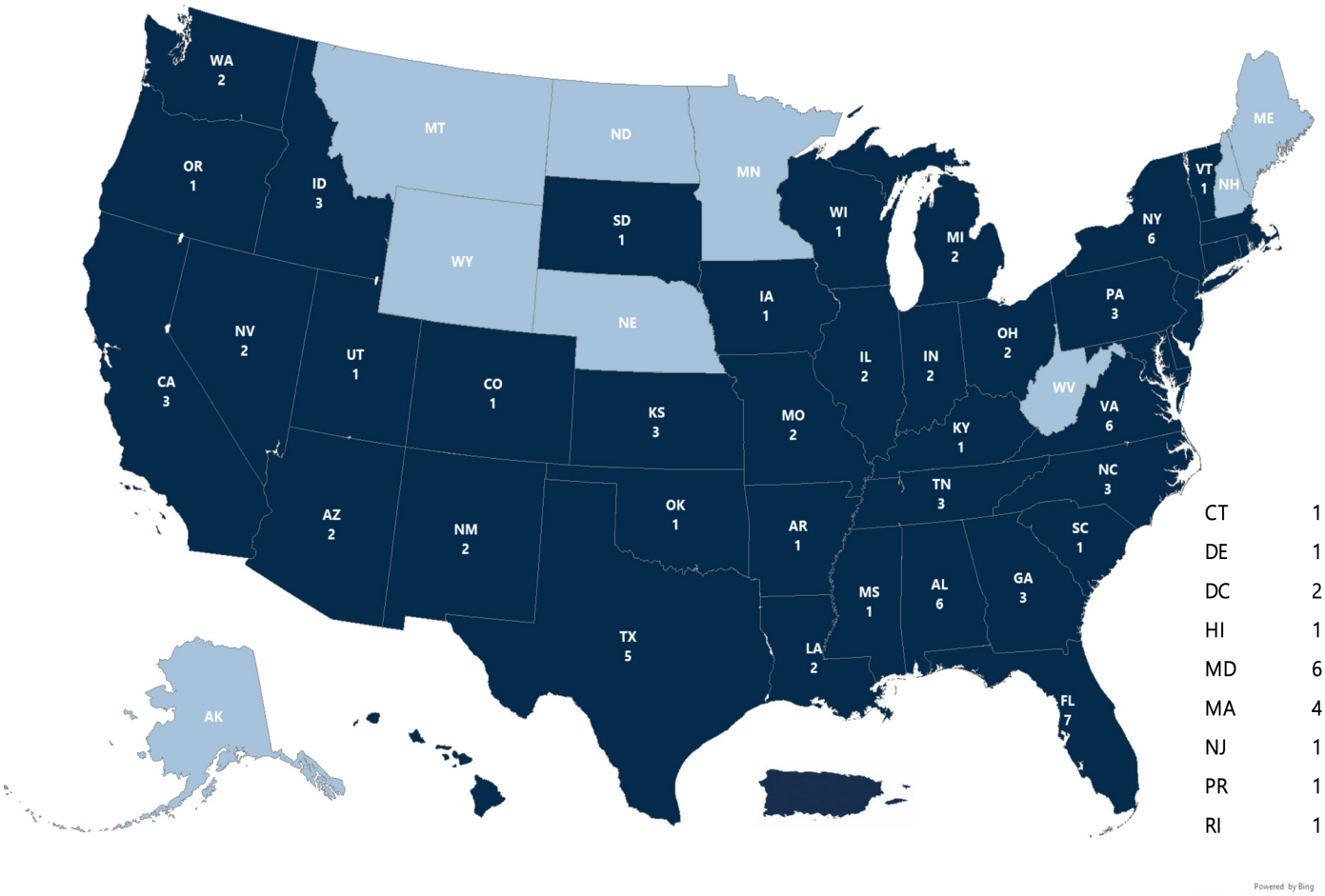


Figure 1 CyberCorps® SFS Student Enrollment

There was an enrollment drop in 2022 due to COVID and a temporary pause in the new scholar enrollment in the fall 2025, which was lifted in January 2026. The most recent enrollment data was collected in October 2025.

[2] https://www.whitehouse.gov/articles/2025/07/white-house-unveils-americas-ai-action-plan/
[3] https://www.whitehouse.gov/presidential-actions/2025/04/advancing-artificial-intelligence-education-for-american-youth/

Figure 2 CyberCorps® SFS Participating Institutions with Active Awards as of January 2026



As illustrated in Figure 2, the CyberCorps® SFS program's reach extends across 106 higher education institutions located in 41 states, the District of Columbia (D.C.) and Puerto Rico. Appendix G provides the complete list of SFS institutions.

Community colleges play an important role in the efforts to create an unrivaled cybersecurity workforce by offering degrees and industry-recognized credentials that prepare students to fill high-demand cybersecurity jobs. Community college students are included in the CyberCorps® SFS program via Community College (CC) Pathways in which second-year students at community colleges become eligible for one year of support if there is a formal agreement between their community college and a four-year CyberCorps® SFS institution that allows students to transfer to the four-year institution to complete a bachelor's degree. At the four-year institution, students are eligible for two more years of CyberCorps® support (total of three years). Currently there are 24 community colleges participating in the CC Pathways.

A CyberCorps® SFS funded project, entitled Catalyzing Computing and Cybersecurity in Community Colleges (C5) at Whatcom Community College (WCC), has designed a mentoring program that became the national model adopted by the National Security Agency and is credited with the dramatic increase of the number of community colleges holding the Center of Academic Excellence (CAE) designation. With continued NSF support, WCC now hosts the National Cybersecurity Training and Education Center (NCyTE) funded by NSF's Advanced Technological Education program. The center includes 543 member institutions. It has offered 163 professional development opportunities for 2,381 faculty and supported 118 Faculty-Industry Externship applicants and 342 Faculty Fellows. It also sustains the C5-funded cybersecurity-themed version of the Advanced Placement course Computer Science Principles (CSP) that enrolled almost 10,000 high school students from 2021 to 2025.

Through the CyberCorps® SFS program, NSF contributes to the multi-agency efforts facilitated by the National Initiative for Cybersecurity Education (NICE), which are intended to strengthen collective work to address the Nation's cybersecurity challenges.

CYBERCORPS® SFS PROGRAM OVERVIEW

The goals of the CyberCorps® SFS program during the 2024-2025 reporting period were to:

1. Increase the number of qualified cybersecurity candidates for federal cybersecurity positions;
2. Improve the national capacity for the education of cybersecurity professionals and research and development workforce;
3. Hire, monitor and retain high-quality CyberCorps® SFS graduates in the cybersecurity mission of the federal government; and
4. Strengthen partnerships between institutions of higher education and federal, state, local and tribal governments.

The recently announced CyberAI SFS program solicitation (NSF 26-503) expanded the scope of the CyberCorps® SFS program and has the following goals:

1. Increase the number of CyberAI experts and support their placement and retention in the mission of government organizations; and
2. Enhance the national capacity for the education and training of AI and cybersecurity professionals, educators and researchers.

To recruit and train the next generation of cybersecurity professionals to meet the needs of the cybersecurity mission for federal, state, local and tribal governments, the program ensures that a minimum of 70% of scholarship recipients secure positions within the executive branch of the federal government, no more than 20% are placed in non-executive federal, state, local, or tribal government organizations or Federally Funded Research and Development Centers (FFRDCs) and up to 10% become educators at SFS institutions.

SCHOLARSHIPS

The CyberCorps® SFS program provides awards to higher education institutions through multi-year grants. The grantee institutions in turn award scholarships to students pursuing studies in cybersecurity and related fields, through a competitive student selection process and use some of the funding provided by NSF for administrative costs associated with preparing and supporting the scholars.

CyberCorps® SFS scholarships cover up to three years of stipends, tuition and professional development allowances for students. CyberCorps® SFS scholarship recipients must be U.S. citizens or lawful permanent residents. Additionally, they must be enrolled as full-time students in a coherent formal degree program with a specific focus on cybersecurity.

The program accommodates students across more than 69 distinct areas of study, with Computer Science being the most common major. As shown in Figure 3, SFS students come from across the Nation, with California, Texas, New York, Alabama, Maryland and Florida being the primary home states. The universities with the largest enrollment of SFS scholars are shown in Table 1; the cumulative new enrollment is the sum of the new SFS enrollment each year from 2018 to 2025.

Students range from sophomores in associate's degree programs through doctoral degree candidates in research-oriented Institutions of Higher Education. In the eight years covering the period 2018 through 2025, graduates mostly attained master's degrees (averaging approximately 55%), followed by bachelor's degrees (averaging approximately 40%) and doctoral degrees (averaging approximately 3.5%). Note: Community college students are required to continue their education and earn a bachelor's degree, therefore their numbers are included with the other bachelor's degree recipients.

Figure 3 CyberCorps® SFS Students' Home States (based on high school attendance). Cumulative new enrollment (sidebar) is the sum of the new SFS enrollment each year from 2018 to 2025.

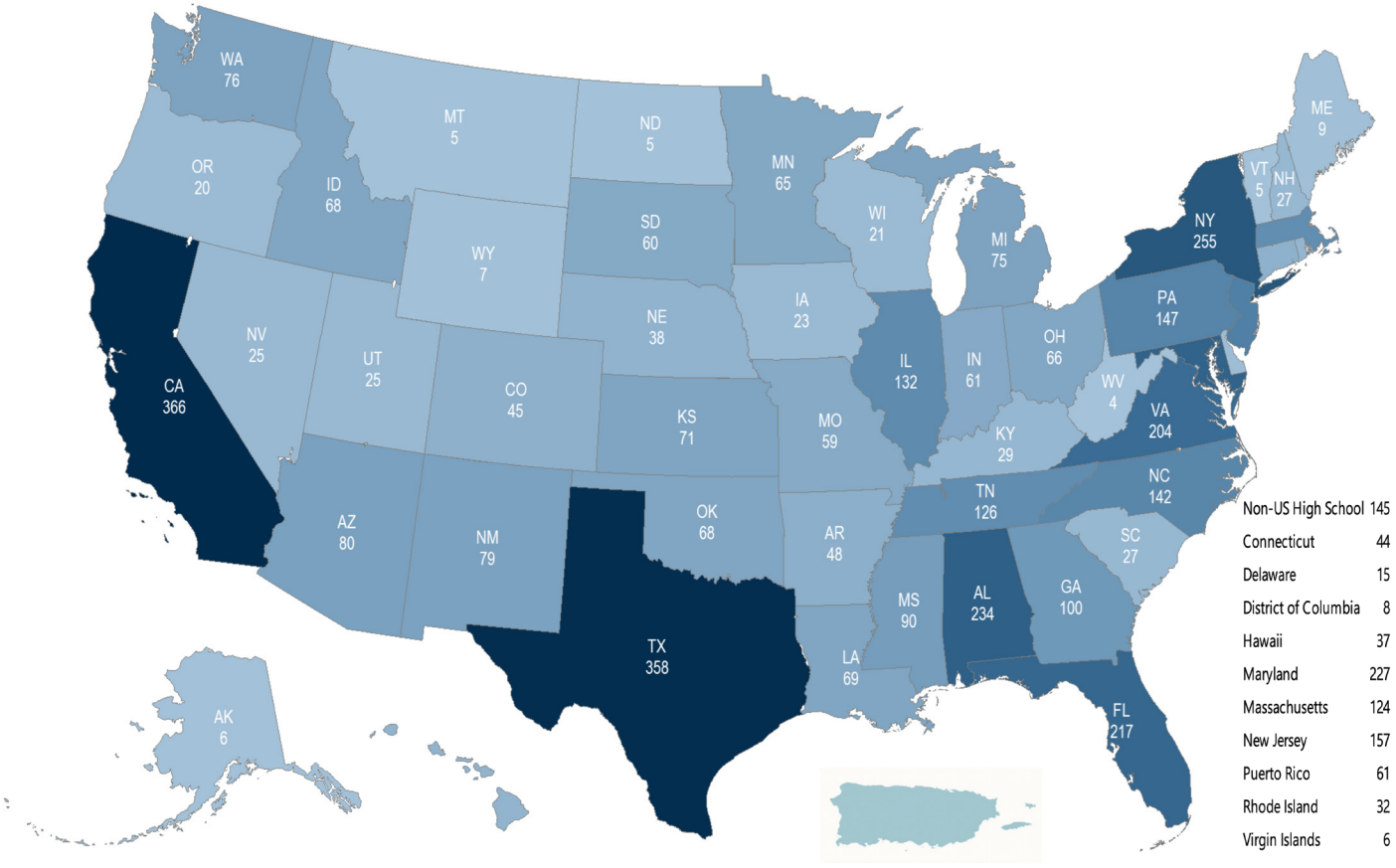


Table 1 - Top Universities by Cumulative New Enrollment (2018-2025)[4]

CyberCorps® SFS Institution	Total Cumulative Enrollment
University of Alabama in Huntsville	77
University of Tulsa	69
University of Texas at El Paso	61
Dakota State University	61
University of Texas at San Antonio	54
California State University - San Bernardino	54
University of Maryland, Baltimore County (UMBC)	52
University of Texas at Dallas	51
Tennessee Tech University	49
Georgetown University	47
Florida State University	46
New Jersey Institute of Technology	45
Rochester Institute of Technology	44
Northeastern University	44
University of North Carolina at Charlotte	43

[4] Data as of October 1, 2025

SFS scholarship recipients agree to work after graduation in the cybersecurity mission of a federal executive agency, Congress (including any agency, entity, office, or commission established in the legislative branch), an interstate agency, a state, local or tribal government or government-affiliated non-profit considered to be critical infrastructure as defined in 42 U.S. Code § 5195c(e), or as an educator in the field of cybersecurity at one of the CyberCorps® SFS institutions. Table 2 outlines the top employers for SFS students, a list that includes the National Security Agency (NSA), various branches of the armed forces and national laboratories.

Scholars' employment must last for at least a period equal to the duration of their scholarship and must start within 18 months after graduation and be completed within five years of entering the post-graduation Commitment Phase of the SFS program. Failure to satisfy the academic requirements of the program or to complete the service obligation results in forfeiture of the scholarship award, which must either be repaid or treated as a Direct Unsubsidized Loan subject to repayment unless the Scholar is granted a time extension or a repayment waiver due to extenuating circumstances.

© Courtesy of Loyola University in Chicago, 2024.

Table 2 - CyberCorps® SFS Student Top Placements (2001-2025)[5]

Post Graduation Agency	No of Graduates Employed
National Security Agency	846
U.S. Navy	443
MITRE Corporation	355
U.S. Air Force	256
U.S. Army	234
Sandia National Laboratories	207
Johns Hopkins University: Applied Physics Laboratory	142
Cybersecurity and Infrastructure Security Agency	135
Federal Bureau of Investigation	113
Defense Information Systems Agency	88
Lincoln Laboratory - MIT	78
Central Intelligence Agency	73
Software Engineering Institute - CMU	70
Idaho National Laboratory	59
Federal Deposit Insurance Corporation	57

[5]Data as of October 1, 2025.

PROGRAM MANAGEMENT

As outlined in the SFS statute, oversight and administration of the CyberCorps® SFS program are entrusted to NSF in collaboration with Office of Personnel Management (OPM) and Department of Homeland Security (DHS). This collaborative framework ensures the program's effectiveness and alignment with national cybersecurity objectives. The SFS Program Office, an office managing the SFS program through partnership between NSF and the OPM, is supported by teams from NSF and OPM. The program has four goals as described in the SFS program overview above. While the three agencies work together on all four goals, NSF's strength is in the first two goals; OPM's in the third goal; and DHS in the fourth goal. The partnership continues to evolve while serving goals of the program. The SFS Program Office receives feedback and outcomes from an independent evaluation team, to inform strategic planning and continuous improvement of the program.

U.S. National Science Foundation

The NSF Team, with the SFS Program Office, plays a central role in overseeing program operation. This role encompasses a broad spectrum of responsibilities, ranging from issuing program solicitations, to overseeing the merit review process, conducting site visits and managing awards. Review of annual and final reports from SFS awardees ensures that projects adhere to program objectives.

Beyond these administrative functions, the NSF Team, with the SFS Program Office, manages financial aspects of the program and represents the program in interactions with federal agencies and the academic and scientific communities. Another duty of the NSF Team lies in outreach and engagement with current and prospective CyberCorps® SFS institutions and principal investigators (PIs) to accomplish the program's goals.

The NSF Team partners with OPM for SFS scholar monitoring. Additionally, the NSF Team partners with both OPM and DHS to host the CyberCorps® SFS Job Fairs, which facilitate connections between students and government agencies. The NSF Team, with the SFS Program Office, also receives deferral or discharge requests from scholarship recipients. Deferrals are approved extensions of the period for completion of the service obligation. A deferral can be requested based on enrollment in a program of study or engagement in approved professional activity for further professional development or CyberCorps® SFS workforce readiness, a condition under the Family and Medical Leave Act (FMLA), a call or order to federal or state active duty or active service, or other exceptional circumstances significantly affecting the scholarship recipient's ability to serve, as determined by the NSF Director. A discharge of service obligation or repayment can be requested based on the circumstances of death, total and permanent disability, or extreme hardship.

A scholarship recipient who fails to complete the service obligation must repay the scholarship. If not repaid, the CyberCorps® SFS scholarship amount paid to the scholarship recipient, together with interest accruing from the date of the scholarship award shall be treated as a Direct Unsubsidized Loan. The scholarship recipient remains liable for any amounts that are not repaid. Such amounts, if not repaid, shall be referred to the U.S. Department of the Treasury for collection.

U.S. Office of Personnel Management

The OPM Team plays a critical and fundamental role in the administration of the CyberCorps®: (SFS) Program. OPM is responsible for implementing the program's federal service components, ensuring that SFS supports the development and retention of a highly skilled federal, state, local or tribal cybersecurity workforce.

The OPM Team, with the SFS Program Office, develops and issues official program documentation, such as Student Service Agreements, policy directives and implementation guidance, that establish the operational framework for the program. The OPM Team, with the SFS Program Office, facilitates onboarding for new scholars, monitors academic progress in collaboration with participating institutions and oversees post-graduation service fulfillment. The OPM Team also reviews and approves student job offers to ensure they align with program objectives and federal workforce needs. For scholars who do not fulfill their service obligations, OPM manages data collection and processes related to repayment and waiver requests.

To strengthen federal recruitment and awareness, the OPM Team actively facilitates the connection between agencies and SFS scholars by broadcasting federal cybersecurity hiring opportunities directly to the SFS scholar community. The OPM Team also supports governmentwide hiring through the CyberCorps® SFS website (https://sfs.opm.gov) a platform where scholars can access program information, post résumés and engage with registered federal agencies. In addition, the OPM Team coordinates CyberCorps® SFS Job Fairs and works closely with agencies to support candidate outreach, selection and placement across the federal enterprise.

Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA) within DHS is a strategic partner in advancing cybersecurity education and workforce development. It helps to foster partnerships between CyberCorps® SFS institutions and various levels of government—federal, state, local and tribal. CISA serves as a technical advisor, leveraging its expertise to guide the program.

CISA also collaborates with NSA for the National Centers of Academic Excellence in Cybersecurity initiative. Together, CISA and NSA establish standards for cybersecurity curricula and academic excellence, promote competencies development among students and faculty and highlight the value of community outreach and leadership in professional development. The partnership also aims to promote integration of cybersecurity practices across academic disciplines. Finally, the partners collaborate to address and find solutions to the evolving challenges for cybersecurity education.

Selection of CyberCorps® SFS Institutions

NSF operates as a proposal-driven funding agency, committed to propelling innovative research and development initiatives in STEM research and education. All proposals submitted to NSF are assessed on their intellectual merit and broader impacts as mandated by the National Science Board. Additional program-specific criteria existed for the CyberCorps® SFS program, which were listed in the program's solicitation:[6,7]

CyberCorps® SFS New PI Boot Camp

New SFS Principal Investigators (PIs) participate in a comprehensive one-day New PI Boot Camp during their inaugural year. The primary objective of this boot camp is to furnish new PIs with a holistic understanding of the CyberCorps® SFS program. Furthermore, the boot camp serves as a forum for delving into lessons learned and best practices identified by successful CyberCorps® SFS projects. Experienced SFS faculty and students share insights gained from their experiences through panels and presentations.

The boot camp features presentations by the CyberCorps® SFS program staff, representing NSF, OPM and DHS, as well as from experienced PIs, SFS students and alumni. They provide a comprehensive overview of program requirements, ensuring that new PIs are fully informed about the fundamental expectations and obligations associated with their roles. Additionally, these sessions cover the latest program developments, to make PIs aware of any updates or modifications that may impact their projects.

SFS New Scholars Seminar Series (NS3)

The CyberCorps® SFS program has supported the New Scholars Seminar Series (NS3), as a part of the Tennessee Tech SFS award, NSF #2043324. This SFS onboarding program helps SFS students understand the responsibilities of being an SFS scholar, acquire knowledge of resources, access training in soft skills for cybersecurity professionals and more.

In 2024, the NS3 consisted of 12 sessions held over an 8-week period beginning in September and attended virtually by 81 SFS students from 39 SFS schools across the U.S. The NS3 covered a broad range of topics, including weekly updates from OPM, the security clearance process, research ethics, technical writing skills, interpersonal skills and resume writing. A ceremony took place during the SFS Job Fair in January 2025, in which SFS participants who completed the NS3 series received a certificate of completion and a challenge coin. The NS3 program was not offered in 2025 due to the new student enrollment pause but it will continue in Fall 2026.

FACILITATING GOVERNMENT HIRING

Securing qualified cybersecurity professionals for government organizations poses a significant challenge. The CyberCorps® SFS program addresses this challenge by offering scholarships to exceptional candidates enrolled in institutions with top-tier cybersecurity programs who are committed to working for government organizations.

In alignment with the provisions set forth in the SFS statute, a special hiring authority allows federal organizations to make non-competitive appointments for CyberCorps® SFS graduates. This authority, exempt from any provision governing appointments in the competitive service, enables federal agencies to streamline the recruitment process for SFS graduates. Furthermore, upon completion of their service term, SFS graduates may undergo non-competitive conversion to a term, career-conditional, or career appointment. Agencies also have the flexibility to non-competitively convert a term appointment to a career-conditional or career appointment before its expiration for SFS graduates.

Hiring managers and human resources consultants of agencies can register as agency officials at the OPM SFS Portal, gaining access to the pool of SFS scholars. They may also engage SFS students for internships during the students' academic training period, laying the groundwork for potential permanent placements upon graduation.

[6]The CyberCorps® SFS Program solicitation, https://www.nsf.gov/funding/opportunities/sfs-cybercorps-scholarship-service/nsf23-574/solicitation
[7]The CyberAICorps SFS Program solicitation, https://www.nsf.gov/funding/opportunities/cyberai-sfs-cyberaicorps-scholarship-service

CYBERCORPS® SFS JOB FAIRS

The CyberCorps® SFS program organizes closed hiring events for SFS scholars to enhance direct engagement with agencies every year. The Winter CyberCorps® SFS Job Fair is an in-person job fair jointly sponsored by NSF and DHS. It typically takes place over a three-day period at a DC metro-area hotel.

New awardee school induction ceremony during 2025 SFS Job Fair featuring George Mason University, alongside agency officials

Traditionally, there was an annual Virtual Career Fair as well, typically held in October. Beginning in 2023, the Virtual Career Fair was restructured as a series of agency information and resource sessions for SFS scholars. Table 3 below illustrates the attendance of Winter SFS Job Fairs in 2024 and 2025.

Table 3 - SFS Job Fairs Attendance

Job Fair Year	2024	2025
Number of students	835	946
Number of faculty	175	175
Number of agency booths	84	72
Number of agency representatives	426	338

The 2024 Winter Job Fair was held at the Washington Hilton hotel on January 8-10, 2024. There were 835 scholarship recipients and 175 faculty attending the Job Fair, which had 84 agency booths with 426 agency representatives. Seven agencies, including CISA, scheduled onsite interviews with separate interview rooms. Additional agencies used high-top tables to conduct informal interviews. Seventeen agencies conducted agency information sessions during the fair.

The 2025 Winter Job Fair was also held at the Washington Hilton hotel from January 7 to January 9, 2025. 946 scholarship recipients and 175 faculty attended the Job Fair, which included 72 agency booths with 338 agency representatives. Nine agencies scheduled onsite interviews with separate interview rooms and additional agencies used high-top tables to conduct informal interviews. Scholars and university faculty or principal investigators represented 110 institutions, including four newly designated SFS institutions.

The primary objective of the CyberCorps® SFS Job Fairs is to facilitate interactions and networking opportunities among CyberCorps® SFS students, PIs, government representatives and invited guests. More specifically, the Job Fair's aims to address the themes are listed below.

Career Opportunities: Provide SFS students with a platform to explore and connect with potential employers from various sectors within the cybersecurity field.

Knowledge Exchange: Foster the exchange of knowledge, ideas and best practices among SFS students and faculty.

Professional Development: Enhance the professional development of SFS students by exposing them to industry trends, advancements in the cybersecurity field and career paths.

Stakeholder Collaboration: Promote collaboration and engagement between government agencies and SFS institutions, to address cybersecurity workforce needs.

During the Job Fairs, SFS students have an opportunity to interact with potential employers, learn about job openings and showcase their skills. The SFS Team discusses the current state of the CyberCorps® SFS program with PIs, offering updates and insights. There are also panels and sessions, e.g., conversations with CyberCorps® SFS faculty to discuss the long-term development of the SFS programs and other topics.

A federal employer conducting an interview during the SFS Job Fair

MONITORING

The monitoring framework for the CyberCorps® SFS program encompasses various elements, including NSF annual reports, core monitoring by OPM's SFS Program Management Office and the implementation of the Quality Monitoring System (QMS).

Comprehensive annual reports submitted by each SFS award institution (or awardee) serve as an important monitoring component because they document projects' progress and findings. These reports describe each project's advancement toward specific goals and include financial information that ensures effective utilization of allocated funds. In instances where a project deviates from its planned progression, NSF can defer disbursement of annual budget increments, ensuring effective stewardship of federal funds.

The OPM Core Monitoring, carried out by the OPM SFS Program Management Office, continuously monitors SFS students' progress through their scholarship and commitment phases. This includes the registration of new students, monitoring of students' academic status, approval of internships and post-graduation positions and the processing of annual employment verification throughout the post-graduation employment-obligation phase. In cases where a student fails to fulfill their obligation, information is collected or generated to support the processing of waiver requests, repayment agreements, or collection actions by the U.S. Treasury, ensuring accountability and adherence to program requirements.

The QMS, initiated in 2015, was developed in response to a recommendation from a cybersecurity human capital report by the U.S. Government Accountability Office. Managed in collaboration with the OPM Assessment and Evaluation Branch (AEB), the QMS uses annual data collections to monitor program implementation, outputs and outcomes, contributing to accountability, program management and continuous improvement of the SFS program. The QMS comprehensively tracks scholarship recipients from their entry into the SFS program to the end of their reporting requirement as required by law. Annually, the QMS collects information from new students, continuing students, recent graduates, graduates meeting their service obligations, graduates at least one year beyond their service obligations and SFS academic teams. Moreover, focus groups are conducted at the annual CyberCorps® SFS Job Fair to obtain deeper insights into the participant's experience.

EVALUATION

The CyberCorps® SFS program evaluation aims to assess whether the program achieved its desired outcomes and the desired degree of implementation. The program has undergone periodic evaluations, developed and executed by the OPM AEB. The most recent comprehensive evaluation, spanning a five-year period, concluded in 2025. The evaluation process employs a multi-method approach, incorporating various data sources, including focus groups, annual data collections, on-site visits to colleges, interviews with scholars and associated faculty and staff, analysis of SFS Program Office data and review of external data spanning multiple years.

A logic model, included in Appendix H, serves as a visual representation of the program's inputs, initiatives, intended intermediate and ultimate outcomes, unintended outcomes and contextual factors. The CyberCorps® SFS program monitoring systems and evaluation provide a comprehensive understanding of the participants' experiences within the program and support continuous improvement of the program.

Evaluation Overview

The evaluation completed in 2025 assessed the program's overall effectiveness. It also presented findings relevant to the implementation of the program, including support provided through communication and marketing efforts.

Several stakeholder groups are involved in the SFS program evaluation, each with distinct interests in ensuring the program's success. SFS schools are responsible for recruiting, selecting and educating students and preparing them for careers in the cybersecurity workforce. Key outcomes include student placement in government cybersecurity roles upon graduation, targeting at least 70% of scholarship recipients for hiring by executive agencies.

The SFS program has seven main participant groups: 1) students, 2) graduates under and beyond service obligation, 3) Principal Investigators (PIs)/Co-Principal Investigators (co-PIs)/ Program Coordinators (PCs), 4) faculty, 5) university leadership, 6) agency recruiters and hiring officials and 7) supervisors of graduates under and beyond their service obligation.

Evaluation Methods

The evaluation examined the effectiveness of the SFS program through a rigorous, multi-method approach that analyzed data from various sources (focus groups, annual surveys, university site visits, interviews, SFS Program Office data and external data) over multiple years.

The evaluation examines the journey of the students from the time they enter the SFS program through their employment. Multiple perspectives (students and graduates, schools, employers) are considered. The evaluation plan, models, research design and analyses address key research questions to inform NSF and other stakeholders on the program's goal achievements and areas for improvement.

Summary of Results

Employers report strong satisfaction with CyberCorps® SFS interns and graduates, consistently rating them as higher quality than their non-SFS peers. Seventy percent of supervisors agreed that SFS interns outperform comparable non-SFS interns, while 89% of non-supervisors reported receiving positive feedback from supervisors on intern performance. Overall, 92% of supervisors and 81% of non-supervisors indicated they were satisfied or very satisfied with the quality of SFS interns, reflecting broad confidence in the program's ability to prepare students for professional roles. Similar positive perceptions extend to full-time SFS graduates. Seventy-two percent of supervisors stated that SFS graduates are higher-quality employees than non-SFS graduates in similar positions and 86% of non-supervisors reported hearing favorable evaluations of SFS graduates' performance from supervisors. These findings suggest that the program is contributing high quality professionals to the government workforce.

Strong partnerships between employers and SFS institutions contribute to these outcomes. Approximately three-quarters of supervisors and non-supervisors agreed that their organizations actively recruit both interns and graduates through collaborations with SFS university and college program officials.

Academically, many SFS programs emphasize AI and Machine Learning (ML) through course offerings in emerging specialized AI and cybersecurity topics, while promoting cross-disciplinary collaboration within and across institutions to strengthen students' technical and analytical skills in those subject areas.

PUBLIC INFORMATION

In accordance with the stipulations of P.L. 116-283, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Director of NSF, in coordination with the Director of OPM, shall periodically evaluate and make public, in a manner that protects the personally identifiable information of scholarship recipients, information on the success of recruiting individuals for scholarships and hiring and retaining those individuals in the public sector cybersecurity workforce, including information on (A) to (G) below. The Director of NSF, in coordination with OPM, shall submit, not less frequently than once every two years, to the Committee on Commerce, Science and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Science, Space and Technology and the Committee on Oversight and Reform of the House of Representatives a report, including information on (A) to (I).

A. Placement rates;
B. Where students are placed, including job titles and descriptions;
C. Salary ranges for students not released from obligations under this section;
D. How long after graduation students are placed;
E. How long students stay in the positions they enter upon graduation;
F. How many students are released from obligations;
G. What, if any, remedial training is required;
H. The disparity in any reporting between scholarship recipients and their respective Institutions of Higher Education; and
I. Any recent statistics regarding the size, composition and educational requirements of the federal cyber workforce.

A. Post Graduate Placement Rates

As of October 2025, the CyberCorps® SFS program has achieved a post-graduate placement rate of 95.3% in more than 300 federal and state government entities, national labs and higher education institutions. For a comprehensive breakdown of the placement rates for each year, please refer to the detailed information provided in Appendix A.

B. Post-Graduation Placement

Appendix B includes a breakdown of placements categorized by agency, showing where the CyberCorps® SFS scholars have found post-graduation employment.

Appendix C provides a list of job titles.

Appendix D offers sample job descriptions, providing a perspective on the responsibilities and duties for SFS scholars post-graduation.

C. Salary Ranges 2020-2025

The salary ranges of SFS scholars that graduated from 2020 to 2025 are shown in Table 4.

Table 4 - Salary Ranges of SFS Graduates (2020-2025)

Degree (Sample Size)	Salary Range*	Average Salary
Master's (500)	$15,782 - $205,000	$87,539
Bachelor's (813)	$24,629 - $212,000	$81,807
**Associate's (32)	$35,471 - $133,368	$69,131
Doctoral (42)	$40,000 - $210,000	$115,056
Total (1,387)	$15,782 - $212,000	$84,587

Notes:

*Excludes Hourly Salary Range Type

**Associate degree was an option as a pilot from 2019 to 2022

D. Average Time from Graduation to Employment

CyberCorps® SFS scholars are given 18 months from their graduation date to commence fulfilling their service requirement. Requests for deferring this service obligation are evaluated on a case-by-case basis. Factors such as eligibility for Family and Medical Leave Act (FMLA) coverage or pursuit of further education or professional development within the cybersecurity domain are among the factors taken into consideration when deferrals are requested. Table 5 shows the time from graduation to employment for SFS scholars who were first employed between 2015 and October 2025 (Appendix A provides more detailed data on students who were released or placed on repayment status).

Table 5 - Time from Graduation to Employment

Number of Months	Number of Students	% of Students
0-3	1,650	55.4%
4-6	779	26.1%
7-9	204	6.8%
10-12	108	3.6%
13-15	72	2.4%
16-18	76	2.6%
Over 18	90	3.0%

E. Time Students Stay in the Positions They Enter upon Graduation

Since the last Biennial Report, the OPM CyberCorps® SFS Program Management Office has been performing SFS student portal system updates to collect information about the length of time students stay in the positions they enter upon graduation; The PRA and associated updated have been completed as of May 2025. The time between clearance approval and the reporting deadline was insufficient to collect data for inclusion in this report. In the interim, the QMS continues to be used to address this item.

OPM's AEB administered the annual SFS graduate data collection instrument in the summer of 2025. The effort is part of the QMS and includes Service Obligation Completed (SOC) and Pulse graduates. The SOC graduates are scholars who completed their service obligation within the last year. The Pulse graduates are scholars who completed their service obligation the previous 1 to 8 years. The data collection was conducted over a 6-week period.

The 2024 SOC graduates reported the time they stayed in the positions they entered upon graduation. Promotions to a higher grade or more pay within a career ladder (e.g., Series 2210 GS 9/11/12/13) were considered to be the same position. Promotions to different positions with the same employer at the same or different grade were not considered to be the same position. Table 6 presents the SOC graduate data.

Table 6 - Time Students Stay in the Positions They Enter upon Graduation from SOC Graduate Data*

	Frequency	Percent
Less than 1 year	19	10.3%
1-2 years	51	27.7%
2-3 years	73	39.7%
3-4 years	33	17.9%
4-5 years	7	38.0%
5-6 years	1	5.0%
TOTAL	**187**	**100.0%**

*Results from 2024 SOC Surveys

Note. Promotions to a higher grade or more pay within a career ladder (e.g., series 2210 GS 9/11/12/13) are considered the same position here

The 2024 Pulse graduates also reported the time they stayed in the positions they entered upon graduation. Table 7 shows the 2024 Pulse graduate data.

Table 7 - Time Students Stay in Positions They Enter upon Graduation from Pulse Graduate Data*

	Frequency	Percent
Less than 1 year	25	5.7%
1-2 years	90	20.5%
2-3 years	98	22.3%
3-4 years	86	19.5%
4-5 years	75	17.0%
5-6 years	46	10.5%
6-7 years	13	3.0%
7-8 years	5	1.1%
8-9 years	1	0.2%
9-10 years	1	0.2%
Total	440	100.0%

*Results from 2024 Pulse Surveys

Note. Promotions to a higher grade or more pay within a career ladder (e.g., Series 2210 GS 9/11/12/13) are considered the same position here.

F. Students Released from Obligation

Between 2018 and 2025, a total of 21 students were released from their obligations. This comprised three full waiver releases within the academic phase, four full waiver releases during the employment phase and eleven partial releases within the employment phase. Additionally, there are currently three pending release requests. Detailed data can be found in Appendix E.

G. What, if any, Remedial Training is Required

The QMS continues to be used for data collection on remedial training and the annual SFS data collection included SOC and Pulse graduates in the summer of 2025.

The SOC graduates reported on whether they were directed to take training outside the mandatory agency training (e.g., Travel Card training), types of training and if their supervisor identified the training as remedial. Remedial training was defined as basic technical or non-technical knowledge or skills needed to perform their jobs.

The data indicates that 14.1% of graduates were directed to take remedial training. Types of training varied from non-technical training (e.g., leadership, project management) to cybersecurity-related training and other technical training. Table 8 presents the detailed breakup for each category of training.

Table 8 - Percentage of Graduates Directed to Take Remedial Training from SOC Graduate Data

Types of Training	Percent
Cybersecurity	7.6%
Other Technical	5.4%
Non-technical	5.4%
Other	1.6%
Not Required	85.9%

Results from 2024 SOC Surveys: one respondent could select multiple types of remedial training.

Remedial is defined here as basic technical or non-technical knowledge or skills needed to perform one's job that one did not receive from their SFS program

The 2024 Pulse graduates also reported whether they were directed to take remedial training. The data indicates that 8.8% of graduates were directed to take remedial training. Types of training varied from non-technical training (e.g., leadership, project management) to cybersecurity-related training and other technical training. Table 9 presents the detailed breakup for each category of training.

Table 9 - Percentage of Graduates Directed to Take Remedial Training from Pulse Graduate Data

Types of Training	Percent
Cybersecurity	4.5%
Other Technical	2.9%
Non-technical	4.1%
Other	0.7%
Not Required	91.2%

Results from 2024 Pulse Remedial Training Surveys: one respondent could select multiple types of remedial training.

Remedial is defined here as basic technical or non-technical knowledge or skills needed to perform one's job that one did not receive from their SFS program

H. Disparity in Reporting (2018 – 2025)

There are no documented cases of discrepancies in reporting between the CyberCorps® SFS scholarship recipients and the higher education institutions they attend or attended.

I. Federal Cybersecurity Workforce Statistics

OPM has shared a dashboard for public use to inform cyber workforce planning efforts and support agencies in data-driven decision making related to current and future cyber workforce needs. OPM's Cyber Workforce dashboard is accessible at https:// www.opm.gov/data/data-products/cyber-workforce-dashboard/. The dashboard provides interactive data and visuals on the information technology, cybersecurity and cyber-related functions that make up the federal cyber workforce as defined by the National Initiative for Cybersecurity Education (NICE) work roles. The details of the available data can be found in Appendix F.

INCREASING NATIONAL CAPACITY IN CYBERSECURITY EDUCATION

The CyberCorps® SFS program has supported efforts to increase the ability of the United States higher education enterprise to produce cybersecurity professionals. Proposals were submitted to NSF by Institutions of Higher Education in response to the SFS solicitation, the NSF-wide Secure and Trustworthy Cyberspace program solicitation under Education Designation (SaTC-EDU), Dear Colleague Letters and other mechanisms like targeted supplements. The supported capacity-building efforts include investigations and development of evidence-based and evidence-generating approaches to improve cybersecurity education and workforce development at the K-12, undergraduate, graduate and professional education levels.

SaTC-EDU funded projects focused on improving cybersecurity learning and learning environments in both formal and informal settings, conducting cybersecurity education research, developing new educational materials and methods of instruction, developing new assessment tools to measure student learning and promoting teacher recruitment and training in the field of cybersecurity. In addition to innovative work at the frontier of cybersecurity education, the SFS program also supported replications of research studies at different types of institutions and with different student populations to produce deeper knowledge about the transferability of prior findings. Such efforts include using the results of basic research in cybersecurity to define an evolving cybersecurity body of knowledge and establish curricula for new courses, degree programs and educational pathways. The efforts also contribute to wide dissemination and adoption of designs for graduate programs that will produce future faculty and cybersecurity professionals with research expertise in critical areas, such as AI, quantum computing, aerospace, advanced manufacturing and emerging wireless technologies. Further, the efforts support improvements in teaching methods for delivering cybersecurity content to K-12 students that promote safe online behavior and understanding of the foundational principles of cybersecurity. Institutional collaborations between community colleges and four-year institutions, cybersecurity competitions and other engagement, outreach and retention activities all enhance development of the cybersecurity workforce. The complete list of SaTC-EDU projects funded in FY 2024-2025 is in Appendix I.

In 2026 and beyond, the CyberAICorps SFS program will continue to support capacity building efforts through its education innovation track for projects that enhance production of AI or cybersecurity professionals. The education innovation track will focus on expanding existing educational opportunities, curricula, degree programs, educational pathways, methods and interventions and partnerships among Institutions of Higher Education, government and employers. It will support transformative education proposals in the areas of AI, cybersecurity, or the integration of AI and cybersecurity with potential for wide adoption and sharing of outcomes. These efforts may include developing cutting-edge instructional materials and methods in AI or its role in cybersecurity; fostering experiential learning through curricular innovations, competitions and applied research in AI, cybersecurity, or their intersection across STEM domains; expanding professional development for researchers, educators and practitioners in AI or cybersecurity at all levels; integrating basic or advanced AI or cybersecurity training with other fields to address human interaction with AI systems; and building communities of practice with sharable datasets, AI models and computing resources through partnerships.

An SFS scholar demonstrating his project at the University of Texas at Dallas

K-12 INITIATIVES

The National Defense Authorization Acts for Fiscal Years 2018 and 2021 modified the SFS statute and indicated that the SFS program, through coordination with other agencies as needed, should grant awards to improve pre-college cybersecurity education, by providing funding to summer cybersecurity camps or similar programs across the Nation at the K-12 level.

The objectives are to: (1) increase students' interest in cybersecurity careers; (2) help students practice appropriate/safe online behavior and understand the principles of cybersecurity; (3) improve teaching methods for delivering cybersecurity content in K-12 computer science curricula; and (4) promote the recruitment, training and retention of teachers in the field of cybersecurity.

In response to this legislation, the CyberCorps® SFS program supported investments in K-12 education through the SaTC-EDU designation. In addition to the SaTC-EDU projects, the SFS program also partners with other agencies to support GenCyber, an initiative focused on K-12 students and teachers. The SFS program also parters with other NSF programs to support K-12 level education on integration of cybersecurity with microelectronics.

GENCYBER – INSPIRING THE NEXT GENERATION OF CYBER STARS

Starting in 2014, the CyberCorps® SFS program has partnered with NSA to offer the "Inspiring the Next Generation of Cyber Stars" (GenCyber) program. This program has supported summer cybersecurity camp opportunities for both students and teachers at the K-12 level. It is closely aligned with the National Centers of Academic Excellence in Cybersecurity Program. The program has served as a first cybersecurity educational engagement for many K-12 students and teachers across the Nation.

In the summer of 2024, GenCyber awards were made for 74 student camps, 29 teacher camps and three combined student and teacher camps. A total of 76 institutions, including 15 new institutions, from 42 states, District of Columbia and Puerto Rico, participated. The GenCyber program served approximately 1,900 students and teachers. Arkansas, Delaware, Iowa, New Hampshire, Ohio, Vermont, West Virginia and Wyoming were the only states that did not host a GenCyber program during this period. The program was suspended in 2025.

MICROELECTRONICS EDUCATION

In spring 2024, the SFS program partnered with the NSF Advancing Informal STEM Learning (AISL) program to launch a special initiative on cybersecurity and microelectronics education. This initiative aims to advance learning and education in cybersecurity and microelectronics through informal STEM learning (ISL) experiences, leveraging community-based education, intergenerational outreach and STEM media.

The initiative, as a result of a competitive process, funded nearly 20 supplemental projects with a total amount of approximately $5 million. These awards support cybersecurity education tightly integrated with microelectronics, both representing national security priorities.

The initiative targeted a broad range of public audiences—including K-12 students, families and community college learners—by integrating microelectronics content into existing SFS projects, community STEM programs and informal learning environments such as libraries, museums, after-school clubs and online platforms. Activities include interactive workshops, maker-space challenges, public science events and collaborative projects involving citizen science and public participation in scientific research related to microelectronics. Expected outcomes include increased public awareness of the role of microelectronics in national security and emerging technologies, improved science communication strategies around microelectronics and greater participation in STEM pathways. The initiative also aimed to create reusable media resources and toolkits for informal STEM practitioners and community leaders, fostering sustainable microelectronics engagement beyond the funding period.

SFS scholar presentation at the Tennessee Technological University

SFS PROGRAMS AND INSTITUTIONS CONTRIBUTE TO BUILDING AI EDUCATION CAPACITY

SFS programs and institutions are active in contributing educational innovation in AI education and workforce development.

Faculty Summer AI Institute

To prepare the next generation of cybersecurity professionals, educators must integrate AI concepts, ranging from Large Language Models that automate phishing to adversarial attacks that evade detection, into their curricula. George Washington University, in collaboration with University of Hawaii, will be offering the first Faculty Development Summer Institute entitled AI in Cybersecurity Education in June-July 2026. It will provide cybersecurity faculty with dedicated time, technical resources and expert mentorship to support modernization of their curricula. Participants will leave this institute with:

- **Technical Fluency:** Hands-on experience with PyTorch, LLMs and Adversarial ML tools.
- **Course Materials:** A "Fall-ready" curriculum module tailored for the home institution's specific teaching context.
- **A Community:** A network of peers and experts to support long-term teaching goals.

Curricular Development

The NSF AI Research Institute, ACTION, involving faculty from UC Santa Barbara, Georgia Tech and the University of Washington, have received CyberCorps® SFS funding to develop six courses on AI and Cybersecurity:

1. ML for Cybersecurity (ML4Cyber),
2. AI Alignment for Safe Downstream Applications,
3. AI for Edge Intelligence (TinyML),
4. AI/ML-based Security Analytics,
5. Robustness of AI to Adversarial Manipulation and
6. Iterative Approaches to AI/ML Security.

These courses can be offered as a full-term curriculum of 10 weeks in duration, or as mini courses, depending on the instructor and the course audience. The courses bring cutting edge research in AI and cybersecurity to classrooms, both in-person and online.

Other recent CyberCorps® SFS supported projects to build AI education capacity include:

NSF Award No: 2434416 CUE-M: LEVEL UP AI: Developing Strategies to Increase Capacity and Inclusion in AI Education, Computing Research Association

LEVEL UP AI, led by the Computing Research Association and New Mexico State University with partners AAAI, ACM and IEEE-CS, is a national effort to expand AI education. Through virtual roundtables and in-person workshops, the initiative aims to build consensus on strategies for growing AI curriculum, faculty capacity and infrastructure. Its outcomes will include reports that articulate a shared vision, best practices for scaling AI education, definitions of resource needs and metrics to assess educational capacity and quality.

NSF Award No: 2528533/2528534 - Oakland University/ Worcester Polytechnic Institute, EAGER: NAIRR Pilot Expansion: FA1: Advancing AI Research with NAIRR Workshop Series on Cybersecurity, Edge AI and Autonomous Driving

This project aims to increase National Artificial Intelligence Research Resource (NAIRR) adoption by organizing two 12-workshop series over two years, offering hands-on training for developing AI systems in cybersecurity, edge computing and autonomous driving. The workshops will provide practical guidance on integrating NAIRR's computational resources, datasets and AI frameworks, empowering participants to build secure, efficient and impactful AI systems for real-world applications.

NSF Award No: 2528858 EAGER: NAIRR Pilot Expansion: FA1: AI Horizon: Forecasting Cybersecurity Workforce Evolution and Adaptive Skill Development, UC San Bernadino

AI Horizon is an initiative that leverages the NAIRR Pilot to forecast how AI will transform cybersecurity tasks—identifying which will be automated, augmented, or remain human-driven—and translate these insights into agile curriculum updates. Using a data-driven framework and a three-committee model, the project connects emerging AI capabilities with cybersecurity research and education, addressing national security needs. It will train roughly 1,000 faculty and 1,000 students across 470 institutions through workshops and online training, guiding participants in applying NAIRR resources to develop AI-augmented cybersecurity practices.

CYBERAI DESIGNATION INITIATIVE

The goal of the CyberAI Designation Initiative, an NSF-NSA collaboration, was to develop a CyberAI Program of Study and a new CyberAI designation. Towson University received CyberCorps® SFS funding to convene experts working in both Cyber and AI to develop the Knowledge Units (KUs) for the CyberAI program and run a pilot with institutions designated as CAE-Cyber Defense and CAE-Cyber Operations. The project was completed through a series of workshops and virtual webinars in 2024. Attendees included representatives from the government and academic institutions across the country. Over 150 individuals have attended the in-person workshops and over 200 faculty members have attended virtually to contribute to the final knowledge units.

KUs were developed by twelve lead authors representing nine different institutions, all of which hold CAE-CD, CAE-CO, CAE-R designations, or a combination of these. CyberAI KUs align with the NICE Cybersecurity Workforce Framework and Defense Cyber Workforce Framework. The development involved workshops, peer reviews and validation workshops conducted by an NSA internal working group and was completed in September 2024. Two distinct programs of study were defined under the CyberAI initiative:

- Security of AI (SecureAI) – Securing AI systems and infrastructure throughout their lifecycle and
- AI for Cybersecurity (AICyber) – Leveraging AI to support traditional cybersecurity.

WORKSHOP ON BUILDING EDUCATIONAL CAPACITY IN AI ACROSS DISCIPLINES

On March 11–12, 2025, NSF hosted a workshop on Building Educational Capacity in AI Across Disciplines with the goal of gathering insights on approaches to building educational capacity in this area at IHEs. The workshop convened 18 faculty members and administrators from IHEs across the United States to share experiences and insights about existing programs, help elucidate enablers and barriers for their establishment and sustainment and come up with new ideas for building capacity. Participants were drawn from multiple disciplines and institution types. The following are excerpts from the report[8]:

- The drive for creating interdisciplinary AI educational programs and activities can come from the top down (as initiatives of funding organizations or IHE administrators) or bottom up (student demand or faculty interest). Workshop participants described a variety of approaches to AI education across disciplines that have been established or could be leveraged in the near term.
- IHEs can begin by leveraging the resources already at their disposal, including their unique strengths as an institution, in any capacity-building effort. Faculty with necessary core or interdisciplinary AI expertise are critical, especially given competition with other IHEs and with the private sector.
- IHE can recruit students and advertise their programs, including through student ambassadorships, social media, advertisements, presentations to new enrollees, high-school events, or "road shows," to make students aware of educational opportunities or pathways.
- Funding for research and educational programs is also an important resource.
- Participants suggested that flexible or AI-knowledgeable IHE administrators and streamlined administrative processes can be enabling.
- Technical and curricular resources identified included computing capacity, including graphics processing units and high-performance computing, data for model training and sandboxes or enterprise licenses that protect data when using commercial AI models. Such resources can be obtained via partnerships or donations, which may come with complicated intellectual property protection clauses. Alternatively, campuses may already have or can either establish such resources on-site or leverage those available from other sources, for example through the National AI Research Resource (NAIRR) Classroom resource. Curricular resources could be developed for, or shared among, IHEs.

[8] https://idalink.org/3005150-LP

CYBERCORPS® INSTITUTIONS GRADUATING SCHOLARS WITH AI COMPETENCIES

The CyberCorps® SFS program supports transformation of cybersecurity education to meet the needs of the era of AI by embedding AI into the curriculum. The following institutions received such support to offer AI-enhanced cybersecurity education in 2023:

- University of Alabama at Birmingham ($4.6 million) - focuses on teaching students to apply AI and ML to real-world cybersecurity challenges.
- Georgia State University ($3.9 million) - emphasizes a curriculum that integrates cybersecurity, privacy, AI and ML.
- Tuskegee University ($2.86 million) - integrates AI/ML with cybersecurity for both Computer Science and non-CS majors via its Cyber Bridge program.
- Johns Hopkins University ($3.66 million) - focuses on Assured Autonomy, blending "AI for security" and "security for AI."

In FY 2024, NSF CyberCorps® SFS program invested in the following institutions, all emphasizing AI within cybersecurity training. The awardees include:

- Florida Atlantic University ($2.6 million) - supports education at the nexus of cybersecurity, AI, post-quantum cryptography and hardware security.
- University of Nevada at Las Vegas ($3.11 million) – develops cybersecurity experts skilled in AI/ML for national infrastructure protection in government organizations.
- Boise State University ($3.5 million) - builds scholars' competencies at the intersection of AI and cybersecurity.

In 2025, the CyberCorps® Scholarship for Service Program (CyberCorps® SFS) invested over $13 million for projects that explicitly focus on preparation of future professionals in AI for cybersecurity and the cybersecurity of AI systems at the intersection of AI and cybersecurity. The awardees include:

- University of Maryland Baltimore County ($1 million) – aims to increase the number of qualified professionals in both cybersecurity and AI.
- Dakota State University ($3.6 million) - prepares next generation of public professionals in AI and cybersecurity.
- Pennsylvania State University - University Park ($1.5 million) – trains AI-targeted future cybersecurity workforce.
- Carnegie Mellon University ($1 million) – defends the Nation through education innovation in AI and information security.
- University of Hawaii ($4.1 million) – secures America's future through AI-empowered cyber talent.
- University of California-Santa Barbara ($2 million) - supports faculty development on AI teaching ability and capacity.

A complete list of recent and active awards for CyberCorps® institutions that offer AI-enhanced cybersecurity education for scholars is presented in Appendix J.

REPORT ON FUTURE AI SCHOLARSHIP FOR SERVICE (AI SFS) PROGRAM

As required by the CHIPS and Science Act of 2022 (P.L. 117-167) Section 10313(d), the Director of NSF in coordination with the Director of OPM, created a report[9] entitled "Artificial Intelligence Scholarship for Service Initiative: Need, Feasibility and Implementation," on the need for and feasibility of, establishing an AI scholarship for service (AI SFS) program. The purpose of the AI SFS program would be to recruit and train the next generation of AI professionals to meet the needs of federal, state, local and Tribal governments. In August 2024, the report was submitted to the Committee on Commerce, Science and Transportation of the Senate; the Committee on Science, Space and Technology of the House of Representatives; the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Reform of the House of Representatives.

As statutorily mandated, the report includes the following elements:

- Recent statistical data on the size, composition and educational requirements of the federal AI workforce, including an assessment of current and future demand for additional AI professionals across the federal government;
- The capacity of institutions of higher education (IHEs) to produce graduates with degrees, certifications and relevant skills related to AI that meet the current and future needs of the federal workforce; and
- An evaluation of the need for establishing an AI SFS program as described in Sec. 10313(d) of the CHIPS and Science Act; and
- Feasibility and implementation of an AI SFS program.

The AI SFS program, as outlined in the CHIPS and Science Act, would encompass three components: (a) scholarship for service, (b) capacity-building efforts and (c) graduate fellowships. These components are designed to support students in AI-related degree programs, enhance interdisciplinary AI studies and promote the ethical, social and legal understanding of AI technologies.

[9] https://nsf-gov-resources.nsf.gov/files/2024SFSAIReport-r.pdf

PRESENTATION AND POSTER SESSIONS AT SFS PI MEETING AT THE 2025 SFS JOB FAIR

The January 2025 SFS Job Fair at the Washington Hilton in the District of Columbia included the opportunity for SFS PIs to share best practices in education and research as well as a special showcase for outstanding SFS projects, which was included for the first time. The presentation sessions covered topics in several categories such as (but not limited to): Innovative strategies for SFS program management (recruitment, selection, monitoring and administration; SFS scholar's engagement in emerging technology areas (skill training, research); experiential learning opportunities for SFS scholars; and K-12 outreach through SFS programs. Highlights from presentations include: Integrating AI and Space into Cybersecurity Curriculum by Indiana University, Training SFS Scholars with Emerging Technologies such as Quantum, Blockchain and Healthcare by University of Missouri - Columbia and Educating Offensive AI Model Security Experts by Florida State University. PIs were invited to present posters highlighting their programs, including project details, research contributions, student experiences, outreach, alumni success and best practices. Highlights include Robert Morris University's new course "AI in Cybersecurity" and Tennessee Tech University's cutting-edge research in AI-assisted security, drone swarms and quantum cryptography combined with top finishes in national competitions and mobile GenCyber outreach. The University of Kansas shared strong alumni success stories, NSA- and DARPA-supported research and military high school engagement through CyberBlitz. Oakland University showcased GenCyber camps and new degree pathways and Pace University shared experiential learning and AI-driven student projects. The University of Rhode Island highlighted their career-focused curriculum and professional certification initiatives.

AEROSPACE SECURITY

The Embry-Riddle Aeronautical University (ERAU) organized the inaugural ERAU-NASA-NSF aviation cybersecurity workshop on April 17-18, 2024 and a second workshop on April 16-17, 2025, at the Prescott campus in Arizona. Both workshops were NSF SFS sponsored and NASA supported initiatives addressing aviation cybersecurity research and education needs, recognizing the rapidly evolving threats to connected, automated and innovative aviation systems. While cybersecurity in aviation has been an ongoing concern, this workshop uniquely convened over a hundred participants to share and discuss critical challenges and chart a course for future research directions and workforce development.

Group photo of participants at the 2025 NSF Workshop on Aerospace Cybersecurity

The workshop in 2024 highlighted the importance of the NSF SFS program to national security, ERAU as the SFS institution for aviation and aerospace cybersecurity and acknowledging the 45+ government, industry and academic organizations participating in this workshop. The workshop participants, over two days, included panel discussions and breakout groups and provided recommendations on topics such as:

- Critical technology and research issues in aviation cybersecurity, including the protecting avionics, communication, navigation, surveillance and air traffic control systems and securing flight operations from cyber and cyber-physical threats.
- Future directions and challenges posed by emerging threats to aviation systems, especially due to increasing reliance on cyber-physical systems, IoT, cloud computing, data analytics and AI/ML, automation and connectivity.
- Innovative approaches to secure aircraft, satellite systems, Advanced Air Mobility (AAM) and commercial space travel vehicles at the intersection of cybersecurity, aviation, engineering and computer science.
- Interdisciplinary research collaboration across academia, government and industry to address complex, multi-layered security challenges.
- Workforce education initiatives with a focus on integrating cybersecurity into aviation and aerospace engineering curricula at both the undergraduate and graduate levels and developing specialized awareness and training programs for professionals such as pilots, air traffic controllers and maintenance crew.
- Directing funding agency resources to promote joint efforts in aviation and aerospace cybersecurity, enhancing the quality of research, education and leadership in this critical area.

The workshop also engaged over 55 students from 26 institutions, including 16 SFS institutions, providing travel grants to several applicants. These students had a unique opportunity to participate in the world's only aviation cybersecurity capture-the-flag (CTF) competition offered by ERAU-Prescott during the workshop and to compete for cash prizes. This CTF competition challenged participating teams to solve aviation cybersecurity problems in the context of a major airport under cyberattack, including issues such as compromised passenger check-in, baggage handling and many more complex scenarios.

One recommendation of this workshop was that NSF consider initiating a program focusing on research and education in aviation cybersecurity. Aviation is a critical infrastructure for national security and as the industry advances, cybersecurity and cyber-physical resilience challenges will become more pervasive. A special initiative to support key areas was identified during the workshop.

University of South Alabama SFS scholars on a site visit

CYBERSECURITY OPERATION CENTERS

A Cybersecurity Operations Center (SOC) serves as the central hub of an organization's cyber defense, where security professionals continuously monitor, detect, analyze and respond to cyber threats and attacks to safeguard data, infrastructure and the organization's mission. Many cybersecurity graduates begin their careers working in SOC environments as their first job. Establishing a university-based SOC model can give students early exposure to real-world cybersecurity challenges, enhancing their hands-on learning and complementing classroom-based theory and simulations.

In collaboration with ONR, NSF provided funding to three SFS schools in 2024 to explore possibilities to provide a SOC-like experiential learning environment for their SFS scholars.

Oregon State University

The Oregon Research and Teaching Security Operations Center (ORTSOC) is the cornerstone of Oregon State University's undergraduate cybersecurity program. Modeled after the "teaching hospital" clinical rotation system, ORTSOC provides CyberCorps® SFS scholars and other students with a year-long residency embedded directly into their curriculum. Under the mentorship of experienced professionals, students build an experiential bridge from the classroom to professional practice. Students hone their skills in critical areas—including threat intelligence and hunting, incident response and penetration testing—by providing managed cybersecurity services to underserved regional entities, such as K-12 schools, local governments and nonprofits. Beyond workforce development, ORTSOC serves as a living laboratory for cutting-edge research and a regional center of excellence for information sharing. By putting knowledge into action, ORTSOC develops well-rounded practitioners ready to address the national shortage of cybersecurity professionals.

Arizona State University

To address the gap between university curricula emphasizing generalized knowledge and employer-driven training prioritizing task-specific skills, ASU students are exposed to both academic training and CTF-style environments. This initiative explores the limitations of current training models, evaluates their operational impact and develops strategies to integrate both generalist and specialist competencies. The effort not only advances cyber training methodologies but also strengthens SFS scholars' analytical and problem-solving skills, preparing them to become more adaptable and effective cyber professionals. Insights from this work have already been incorporated into ASU's cybersecurity curriculum.

University of South Florida

The MockSOC project research is jointly funded by NSF's SFS and ONR's Expert Cyber Training programs. The goal is to investigate how to design effective training methods to elevate trainee skills to expert levels. In this research, the USF team is experimenting with a tool-agnostic approach to cyber training, where trainees are asked to solve realistic cyber incidents absent any requirement of using specific tool or play books. The goal is to focus on developing analytical intuitions and reasoning skills. The training scenarios are designed in collaboration with a leading cybersecurity company which has a large footprint in managed security services. All USF SFS scholars are invited to participate in those sessions. Some preliminary findings from the research have been published.

RISK MANAGEMENT OF CYBERCORPS® SFS PROGRAM

In a report of the U.S. Government Accountability Office (GAO) (22-105187) titled: "Cybersecurity Workforce: Actions Needed to Improve CyberCorps® Scholarship for Service Program", GAO recommended that the "Director of the National Science Foundation should develop and implement a risk management strategy that includes a process to effectively identify, analyze, mitigate and report CyberCorps® Scholarship for Service Program risks and challenges."

To address that recommendation, NSF developed and implemented a risk management strategy in accordance with OMB Circular No. A-123 and GAO's Standards for Internal Controls in the federal government. Afterwards, the NSF SFS Program team underwent an extensive exercise in Risk Management Planning where program staff used a framework based on guidance from OMB Circular No. A-123 to identify, assess, plan, monitor and report risks associated with the SFS program.

During this process, the SFS Program team reviewed existing risks with internal control information, key control matrices and GAO audit reports to conduct an initial identification of program risks in coordination with the other key stakeholders. The exercise led to the creation of a suite of Risk Profiles for the SFS program in which program staff identified risks and validated these risks with the applicable risk management stakeholders through multiple meetings. After relevant risks were identified, key stakeholders collaborated to analyze, score and document the risks in the Risk Profiles. SFS program staff consulted with experts from the NSF agencywide internal controls team to validate the accuracy of the steps taken for the risk exercise, while ensuring that the content, risk assessment and analysis was conducted at the program level. Finally, executive-level leadership reviewed and provided input on the work as it progressed towards completion.

The SFS program has since implemented a structured process to embed identified risk mitigation actions into its operations. Risk management for the SFS program has become an ongoing, integrated practice.

ADVANCING CYBERSECURITY THROUGH RESEARCH (ACT-R25): SUMMER 2025 RESEARCH EXPERIENCE

Acknowledging the critical need for meaningful summer opportunities in cybersecurity for current scholars with internship requirements, Auburn University and University of Florida facilitated an intensive summer research experience in 2025 that provided students from the SFS Community with practical, hands-on training in cybersecurity research.

Twenty-seven SFS institutions hosted their own SFS scholars (a total of 76 scholars) that summer for research experiences supervised by faculty mentors. This sponsored initiative merged rigorous academic inquiry with real-world applications, offering participants a dynamic environment where they could engage with leading-edge tools and investigations into cyber threats, secure systems and defense mechanisms.

Each SFS scholar participant received a stipend for their research work, reinforcing the program's commitment to enhancing SFS scholars' research experiences. Over the summer, students immersed themselves in advanced cutting-edge research in cybersecurity and related technologies, fostering a deeper understanding of emerging challenges and problem solving.

CYBERCORPS® SFS HALL OF FAME

Each year, the CyberCorps® SFS program inducts one outstanding alumnus into the SFS Hall of Fame. The CyberCorps® SFS Hall of Fame recognizes the outstanding accomplishments of alumni working in cybersecurity for federal as well as state, local, territorial and tribal governments, or those working in the private industry after completing their service requirement. Selection for this distinction is highly competitive.

Institutions can nominate more than one candidate for consideration. A committee then evaluates each nominee based on their achievements and contributions to the cybersecurity community. After the committee selects a finalist, CISA announces the annual Hall of Fame recipient at the Winter CyberCorps® SFS Job Fair. Since recognizing the first three recipient inductees into the Hall of Fame in 2018, a total of ten alumni have earned this distinction as presented below.

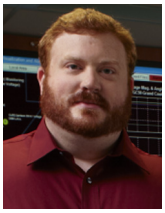
Josiah Dykstra (2018), author of "Essential Cybersecurity Science," a 2016 guide for using the scientific method to build, test and evaluate systems, received both the Presidential Early Career Award for Scientists and Engineers (PECASE) and the Hope College Young Alumni Award in 2017. In 2013, he received the Director of National Intelligence Galileo Award and the U.S. Department of Defense David O. Cooke Excellence in Public Administration Award. Ever motivated to share and apply his extensive knowledge, Dykstra mentors university students and junior NSA employees. Dykstra graduated from an SFS program at Iowa State University with a master's degree in information assurance in 2004. He also received a doctoral degree from the University of Maryland Baltimore County, another SFS school, in 2013. Dykstra is currently a cybersecurity expert employed by the NSA.

Mischel Kwon (2018) graduated from an SFS program operated jointly by Marymount University and George Washington University in 2005, receiving a master's degree in computer science with an emphasis in information assurance. While serving as the deputy director for information technology security staff at the U.S. Department of Justice, she built the first Justice Security Operations Center to monitor and defend the department against cyber threats. Kwon also served as the director of the DHS U.S. Computer Emergency Readiness Team (US-CERT), spearheading the organization responsible for analyzing and reducing cyber threats and vulnerabilities in federal networks and coordinating national incident response activities. After leaving government service, Kwon served as vice president of public sector security for RSA Security, leading the company in assisting with public-sector security solutions, strategies, technologies and policy.

Steven Hernandez (2018) has held information assurance positions at the U.S. Department of Education, the U.S. Department of Agriculture and a National Security Administration Center of Academic Excellence Research Institute in Idaho. In 2010, he joined the Department of Health and Human Services, where he has served as chief information security officer for the Office of Inspector General. In 2016, the Department of Education hired Hernandez as chief information security officer. In this role, he maintains the department's integrity and privacy and coordinates and integrates all aspects of its cybersecurity, telecommunications and information security programs. Hernandez graduated from the SFS program at Idaho State University with a Master of Business Administration in information assurance/computer information systems in 2007. He received a bachelor's degree in computer information systems and an associate degree in electronic systems from the same institution.

Patrick Kelly (2019) has a master's degree in public policy from the SFS program at George Washington University. Patrick began to serve his country after graduation at the Federal Reserve and the Department of Health and Human Services where he served as Senior Official for Privacy and the Information Security Branch Chief in the Office of Inspector General. He currently is with the Office of the Comptroller of the Currency (OCC) where he is the Critical Infrastructure Policy Director. He also chairs the Federal Financial Institution Examination Council Cybersecurity and Critical Infrastructure Working Group that collaborates on cybersecurity guidance and assessments related to systemic operational risk to the national banking system. Patrick is an outstanding supporter of the SFS program; as an adjunct faculty member, he led the GW Scholarship for Service Seminar course on Cybersecurity Governance since 2012 and in that role has mentored dozens of CyberCorps® SFS students.

CYBERCORPS® SFS HALL OF FAME



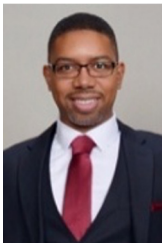
David Manz (2020), at the time of this recognition, was serving as a Chief Cybersecurity Scientist in the National Security Directorate at the Pacific Northwest National Laboratory. He leads a team of a dozen engineers, scientists and support staff. He holds a B.S. in Computer and Information Science from the Robert D. Clark Honors College at the University of Oregon and an M.S. and a Ph.D. in Computer Science from the University of Idaho. David also has experience teaching undergraduate and graduate computer science courses and is an adjunct faculty at Washington State University. David has co-authored numerous papers and presentations on cybersecurity, control system security and cryptographic key management.

Dan Guido (2021) is the founder of an industry-leading software security firm that employs 80 professionals and other SFS grads. He has contributed to an array of government programs and publications and nurtured the cybersecurity community in New York City. His SFS internships at NSA and his post-graduation employment at the Federal Reserve Bank of NY helped steer his career, marked by continuing government and community service to help policymakers, students and entrepreneurs. In 2012, Dan founded Trail of Bits to address software security challenges with cutting-edge research. In his tenure leading Trail of Bits as CEO, Dan has grown the team to 80 engineers, led their work on more than a dozen programs with DARPA and the DOD and routinely transitioned research to practice. In 2019, Trail of Bits was recognized by Forrester as the leader for "Small Cybersecurity Consulting Services."

Sagar Samtani (2022) is an Assistant Professor and Grant Thornton Scholar at Indiana University's Kelley School of Business. He is also a Fellow at the Center for Applied Cybersecurity Research (CACR) within the university. His research revolves around Artificial Intelligence for Cybersecurity, with a focus on deep learning, network science and text mining techniques for various applications, including open-source software security, Cyber Threat Intelligence (CTI), advanced cyberinfrastructure security, AI risk management and Dark Web analytics. Dr. Samtani has an impressive publication record, with over fifty papers in renowned Information Systems (IS), cybersecurity and Machine Learning venues. He has secured substantial funding for his research from NSF's cybersecurity programs and has co-founded workshops on AI for Cybersecurity topics. Dr. Samtani actively serves as a Program Committee member or Chair in leading AI and cybersecurity conferences. He is deeply engaged with industry, serving on advisory councils and boards and regularly presenting at industry events. His outstanding research has earned him several prestigious awards and numerous media citations. Dr. Samtani is a member of various professional organizations, contributing actively to the advancement of his field.

Devon Rollins (2023) is the Vice President of Cyber Engineering and Machine Learning at Capital One, where he oversees teams working on security monitoring platforms at petabyte scale. With a decade of experience in security operations, cyber intelligence and risk management, Devon's engineering background has been essential in combating cyber-attacks. He received the Circle of Excellence Award for incident response at Capital One in 2020. Previously, he worked at MITRE Corporation, leading teams at the National Cyber Joint Investigative Task Force and the National Intellectual Property Rights Coordination Center, receiving accolades for his contributions. Beyond his professional achievements, Devon is actively involved in the community, advocating for STEM education through his nonprofit, STEMLY. He is also a policy fellow for New America's Cybersecurity Initiative and the Center for American Progress Leadership Institute. Devon holds two degrees in computer science from North Carolina A&T State University, a master's degree in information security policy and management from Carnegie Mellon and is a CISSP certified professional.

CYBERCORPS® SFS HALL OF FAME



Samuel Edoho-Eket (2024) is a leader, entrepreneur and a certified cybersecurity, telecommunications and project management subject matter expert. He has over 23 years of experience supporting both the Department of Defense (DoD) and commercial sectors. He received a bachelor's degree from Princeton University in Electrical Engineering (receiving the John Ogden Bigelow Prize in Electrical Engineering) and received a master's degree in information networking from Carnegie Mellon University (CMU)'s prestigious Information Network institute (INI) funded by the NSF Scholarship for Service (SFS). After graduating from CMU, he established a successful track record as a civilian Technical Director within the DoD while supporting national and international communications interoperability efforts. He went on to consult as a Systems Engineer for several years before establishing and founding PrismSix Technologies in 2012. His many significant career accomplishments include leading the establishment of some of the largest DoD Voice over Internet Protocol (VoIP) infrastructure environments during the last two decades. This infrastructure today enabled the DoD to successfully pivot towards newer technologies while phasing out higher priced legacy infrastructure. In addition to leading system deployment activities, his firm also conducts Cybersecurity training and audits for commercial organizations. During the COVID-19 pandemic, he helped lead the establishment of a secure Cloud-based voice gateway for the DoD alongside critical capacity increases required to handle Voice and Video over IP (VVoIP) traffic, supporting remote workers.

Elizabeth Schweinsberg (2025) is a Senior Technical Advisor at the Centers for Medicare and Medicaid Services specializing in Zero Trust Architecture. Before that, she spent 9 years in corporate threat detection and incident response with Facebook and Google. She works to keep the internal networks safe from malware, hackers and the Internet. Ms. Schweinsberg has been in the computer industry for over two decades and in digital forensics since 2005 in both the Government and private sector. She has a Master of Information Security degree from Carnegie Mellon University where she participated in Scholarship for Service program. When not behind the computer, Ms. Schweinsberg can often be found behind a book or a sewing machine.

APPENDIX A: POST GRADUATE PLACEMENT RATE BY ENROLLED YEARS

Source: SFS Master Roster and Placement Log as of October 1, 2025.

Enrolled Year	Placed	Still Looking within 18 Months	Released	Repayment	Total Graduated	PG Placement Rate[10]	Still Looking within 18 Months	Still in School	Non Grad Release	Non Grad Repayment	Total Awarded SFS
2001	25	0	6	0	31	81%	0	0	0	0	31
2002	95	0	16	1	112	85%	0	0	2	1	115
2003	196	0	16	2	214	92%	0	0	1	4	219
2004	171	0	3	2	176	97%	0	0	0	9	185
2005	166	0	2	5	173	96%	0	0	4	5	182
2006	124	0	0	3	127	98%	0	0	1	5	133
2007	100	0	0	5	105	95%	0	0	1	5	111
2008	93	0	0	0	93	100%	0	0	0	1	94
2009	117	0	1	8	126	93%	0	0	4	3	133
2010	169	0	1	6	176	96%	0	0	2	3	181
2011	178	0	2	8	189	95%	0	0	2	4	195
2012	173	0	0	6	179	97%	0	0	2	5	186
2013	245	0	1	7	254	97%	0	0	1	13	268
2014	252	0	3	12	267	94%	0	0	0	10	277
2015	258	0	1	12	271	95%	0	0	0	6	277
2016	288	0	0	8	304	96%	0	1	2	6	313
2017	329	1	0	9	347	97%	1	1	2	6	357
2018	308	2	1	10	330	95%	2	1	1	5	339
2019	312	11	1	7	353	92%	11	10	2	8	384
2020	258	47	0	4	312	86%	47	10	2	4	375
2021	155	86	0	2	174	96%	86	95	0	9	364
2022	31	31	0	0	38	92%	31	320	0	2	391
2023	0	1	0	0	0	0%	1	462	0	0	463
2024	13	0	0	1	14	92.9%	30	428	2	3	477
2025	0	0	0	0	0	-	1	61	0	2	64
Total	**4,724**	**1**	**64**	**170**	**4,959**	**95.3%**	**410**	**621**	**33**	**123**	**6,146**

[10] PG placement rate is calculated as the percentage of scholarship recipients that have graduated and that are in a placed status.

APPENDIX B: POST GRADUATE PLACEMENT BY AGENCY

Post Graduate Agency	4,724

Department of	632
Agriculture	18
Commerce	72
Education	6
Energy	13
Health And Human Services	19
Homeland Security	193
Housing And Urban Development	8
Interior	19
Justice	150
Labor	4
State	44
Transportation	12
Treasury	58
Veterans Affairs	16

War (formerly Department of Defense)	1,970
Air Force	256
Army	251
National Security Agency	846
Navy	443
Space Force	7
U.S. Marine Corps	3
Other	164

Department of Energy Labs	478
Ames Laboratory	2
Argonne National Laboratory	8
Brookhaven National Laboratory	1
Fermi National Accelerator Laboratory	2
Idaho National Laboratory	59
Lawrence Berkeley National Laboratory	2
Lawrence Livermore National Laboratory	45
Los Alamos National Laboratory	50
National Renewable Energy Laboratory	8
Oak Ridge National Laboratory	37
Pacific Northwest National Laboratory	52
SLAC National Accelerator Laboratory	3
Sandia National Laboratories	207
Savannah River National Laboratory	1
Y-12 National Security Complex	1

Other Federal Agencies and Sub-Agencies	425
Administrative Office of The U.S. Courts	4
Central Intelligence Agency	73
Environmental Protection Agency	6
Federal Communications Commission	4
Federal Deposit Insurance Corporation	57
Federal Housing Finance Agency	5
Federal Reserve System	61
Federal Retirement Thrift Investment Board	1
Federal Trade Commission	12
Food And Drug Administration	2
Foreign Agricultural Service	4
General Services Administration	13
National Aeronautics And Space Administration	12
National Science Foundation	8
Other Independent Agencies	2
Privacy And Civil Liberties Oversight Board	1
Railroad Retirement Board	6
Securities And Exchange Commission	4
Small Business Administration	2
Smithsonian Institution	1
Social Security Administration	13
Tennessee Valley Authority	5
U.S. Agency For Global Media	2
U.S. Agency For International Development	4
U.S. Courts Of Appeal	1
U.S. Government	34
U.S. House Of Representatives	55
U.S. Nuclear Regulatory Commission	11
U.S. Office Of Personnel Management	9
U.S. Postal Service	8
U.S. Senate	5
Judicial Branch	4
National Aeronautics & Space Administration (NASA)	11
Nuclear Regulatory Commission	6
U.S. National Science Foundation (NSF)	7
U.S. Office Of Personnel Management (OPM)	10
Privacy & Civil Liberties Oversight Board (PCLOB)	1
Railroad Retirement Board (RRB)	6
Securities and Exchange Commission (SEC)	4
SFS Cyber Educator	4
Small Business Administration (SBA)	2
Social Security Administration (SSA)	13
Smithsonian	2
State/Local/Tribal	288
Tennessee Valley Authority (TVA)	3
U.S. Agency for Global Media (USAGM)	2
U.S. Agency for International Development (USAID)	4
U.S. Government	22
U.S. Postal Service (USPS)	8
U.S. Senate	5

APPENDIX B: POST GRADUATE PLACEMENT BY AGENCY

FFRDC and Other Federal Agencies and Sub-Agencies	1,203
Aerospace Federally Funded Research and Development Center	23
CI non-profit	6
Center For Internet Security, Inc.	9
Center For Naval Analyses	2
Federal Reserve Bank of Atlanta	1
Federal Reserve Bank of Boston	1
Federal Reserve Bank of Chicago	4
Federal Reserve Bank of Dallas	4
Federal Reserve Bank of Kansas City	3
Federal Reserve Bank of Minneapolis	1
Federal Reserve Bank of New York	16
Federal Reserve Bank of Richmond	14
Federal Reserve Bank of San Francisco	24
IDA - Center for Communications and Computing	1
IDA - Science and Technology Policy Institute	1
IDA - Systems and Analyses Center	10
In-Q-Tel	1
Johns Hopkins University: Applied Physics Laboratory	142
Lincoln Laboratory - MIT	78
Local Government	74
MITRE - CMS Alliance To Modernize Healthcare	1
MITRE - Center for Enterprise Modernization	63
MITRE - Homeland Security Systems Engineering and Development Institute	8
MITRE - National Cybersecurity Center of Excellence	33
MITRE - National Security Engineering Center	58
MITRE Labs	25
NASA Jet Propulsion Laboratory	11
North American Electric Reliability Corporation	2
Other Approved Organizations	47
RAND Corp. - Homeland Security Operational Analysis Center	2
RAND Corp. - National Defense Research Institute	2
RAND Corp. - Project Air Force	1
Seattle University (internship only)	1
Software Engineering Institute - CMU	70
Southwest Research Institute - Center for Nuclear Waste Regulatory Analyses	1
State Government	291
TRMC Internship Program (INTERNSHIP ONLY)	1
Tribal Government	4

Faculty Member as Cyber Educator at Universities	16
Cal Poly Pomona	1
Citadel	1
Dakota State University	2
Georgia State University	1
Hampton University	1
Louisiana State University	2
Louisiana Tech University	1
North Carolina Agriculture and Technical State University	1
University Of Colorado - Colorado Springs	1
University Of Maryland	1
University Of Rhode Island	1
University of Kansas	1
University of South Alabama	1
Virginia Polytechnic Institute and State University	1

APPENDIX C: JOB TITLES

Position Titles of SFS Recipients, Source: Recipients self-report position titles via their profile in the OPM SFS system.

DOE Omni Technology Alliance Internship Program - Summer 2024
Early Career Network Security Engineer R and D
IT Cybersecurity Specialist (Technical Support)
IT Security Analyst Intern
IT Specialist (INFOSEC)
Research Scientist
Student Trainee (Computer Engineer)
Student Trainee (Computer Scientist)
Student Trainee (Information Technology)
Student Trainee - U.S. Secret Service Pathways Internship
X-Force Fellowship Program
(Cyber) Engineering, Associate Professional Staff I
2024 Graduate - Cybersecurity/Reverse Engineering - Systems Exploitation
A-4 Cyber Research Intern
A-4 Undergraduate Student
ACE Program Intern
ACE Program Participant
Administrative Assistant/Cybersecurity Consultant
Advanced Technologist
AFCS IT Student Trainee
Air Force Research Laboratory "Advanced Course in Engineering" Intern
Analyst
APL RISE Intern
Application Security Engineer
Applications Developer 2
Applied Cybersecurity Engineer
Applied Research Mathematician
Apprentice Language Analyst
Assistant in Research Software Development (Cybersecurity)
Assistant Professor
Assistant Professor of Computer Information Systems
Assistant Professor of Practice
Associate Professional Staff I
Associate AI Security Researcher
Associate Cybersecurity Engineer
Associate Embedded Security Engineer
Associate Software Engineer
Assuring AI/ML within Safety-Critical Applications OSTEM Intern
Attorney Advisor
BTS Risk and Compliance Intern
CAE INSuRE+E Summer Research Workshop
CAE-CO Summer Intern
Camp Counselor
Capabilities Development Specialist
Capabilities Development Specialist, Cyber Summer Program
Center for Cyber Defenders Intern
CEROC SOC Analyst intern
Child Exploitation Investigations Intern
CISA Cybersecurity Intern
CIT Program Navigator
Civilian Temporary
Clerkship
Cluster Institute Student
CNODP Participant
Co-op
Compliance and Training Bureau Auditor I
Computer Data Scientist Student Assistant
Computer Engineer
Computer Engineer II
Computer Engineer intern
Computer Engineer Trainee
Computer Engineering Intern
Computer Forensic Specialist
Computer Investigative Forensic Specialist
Computer Network Defense Analyst
Computer Network Defense Analyst (Intrusion Analyst Skill Development Program)
Computer Network Defense Analyst - Cybersecurity Operations Development Program
Computer Science Instructor
Computer Science Intern
Computer Scientist

APPENDIX C: JOB TITLES

Computer Scientist (CES SFS NLLP Intern)
Computer Scientist - Student Trainee
Computer Scientist / Information System Security Officer
Computer Scientist PAQ Intern
Computer Scientist/Cybersecurity Analyst
Computer Systems and Services Office
Computer Systems Professional 1
Computer Systems Researcher
Computer Technology Educator
CONCISE Cyber intern
Cooperative Education Intern
Cooperative Education Student
Cooperative Education Student – Information Technology
Corporate Alliance Manager
Crime Analyst
Criminal Analyst
Criminal and Cyber Intelligence Analyst
Criminal Investigator
Critical Infrastructure Cybersecurity Intern
Critical Infrastructure Security Specialist
Critical Protection Infrastructure Group - Internship
Critical Skills Recruiting Program
Cryptanalytic Computer Scientist
Cryptologic Computer Scientist
Cryptologic Computer Scientist (Computer Science Development Program)
Cryptologic Intelligence Analyst - CAE-CO Summer Internship
CT Judicial Branch ITD Endpoint Management Intern
CTE Computer Science Teacher
CTE Network Engineer
Cyber Analyst
Cyber Analyst Intern
Cyber Capabilities Development
Cyber co-op
Cyber Crime Intern
Cyber Defense Analyst
Cyber Defense Analyst (SYSANALYSIS)
Cyber Dominance Group Intern
Cyber Engineer 2
Cyber Engineer Intern
Cyber Engineering Group Associate Professional Staff I
Cyber Futures Intern
Cyber Intern
Cyber Intern 1
Cyber investigations and forensics research and practice internship
Cyber Investigations Intern
Cyber Lab Intern
Cyber Operations and Digital Forensics Research Intern
Cyber Operations and Incident Response Internship
Cyber Operations Intern
Cyber Operations Researcher
Cyber Operations/Incident Response Intern
Cyber Policy Analyst
Cyber Range Engineer
Cyber Research Intern
Cyber Resilience and Intelligence Division Intern
Cyber Resilience and Intelligence Division Research Intern
Cyber Resilience Engineer
Cyber Resilience Intern
Cyber Resiliency Graduate Intern
Cyber Risk Analyst
Cybersecurity Analyst I
Cybersecurity Advisor
Cybersecurity Analyst
Cybersecurity Analyst 2
Cybersecurity Analyst Intern
Cybersecurity Associate
Cybersecurity Engineer
Cybersecurity Engineer 1
Cybersecurity Graduate Intern
Cybersecurity IA/ML Student Program Internship
Cybersecurity Intern
Cybersecurity Officer
Cybersecurity Researcher Intern
Cybersecurity Researcher/Developer
Cybersecurity Specialist Intern
Cybersecurity Student Trainee

APPENDIX C: JOB TITLES

Cybersecurity Undergraduate Research Intern
Cybersecurity Weapon Systems Grad Intern
Cyber Summer Program Intern
Cyber Systems Assessments Co Op
Cyber Systems Exploitation Researcher
Cyber Systems Research Intern
Cyber Test and Evaluation Engineer
Cyber Threat Analyst
Cyber Threat Intelligence Analyst
Cyber Threat Intelligence Lead
Cyber Training Program Coordinator
Cyber Trust and Analytics Intern
Cyber Warfare Officer (25A)
Cyber Warfare Systems Group (QCR) Intern
Cyber/Office Assistant
CyberOps Analyst Intern
Cybersecurity - Graduate Intern
Cybersecurity - Graduate Intern - Cyber and Critical Infrastructure Summer Institute
Cybersecurity Analyst
Cybersecurity Analyst I
Cybersecurity Analyst III
Cybersecurity Analyst Intern
Cybersecurity and Military Space Engineer
Cybersecurity and Networking Intern
Cybersecurity Automation Engineer (Information Services IV)
Cybersecurity Consultant/Administrative Assistant
Cybersecurity Engineer
Cybersecurity Engineer (MITRE National Security New Professionals Accelerator Program)
Cybersecurity Engineer intermediate
Cybersecurity Engineer Intern - Cloud Focus
Cybersecurity Engineering Intern
Cybersecurity Fellow
Cybersecurity for Grid Modernization Intern
Cybersecurity Grad CSI Summer 25
Cybersecurity Graduate Intern
Cybersecurity Instructor
Cybersecurity Intelligence Analyst
Cybersecurity Intern
Cybersecurity Intern at the Information Trust Institute
Cybersecurity Outreach Intern
Cybersecurity Program - Project Coordinator
Cybersecurity Program Specialist Intern
Cybersecurity Research and Development Intern
Cybersecurity Research Fellow
Cybersecurity Research Intern
Cybersecurity Researcher
Cybersecurity Researcher II
Cybersecurity Researcher Intern
Cybersecurity Reverse Engineer
Cybersecurity Risk Management
Cybersecurity Software Engineer
Cybersecurity Specialist
Cybersecurity Student Assistant
Cybersecurity Summer Research Intern
Cybersecurity Teaching and Research Assistant
Cybersecurity Teaching Associate
Cybersecurity Technical Staff
Cybersecurity Technical Staff 2
Cybersecurity Undergraduate Intern
Cybersecurity Undergraduate R/D Intern
Cybersecurity/Data Science Intern
Cybersecurity Teaching Assistance
Cyberspace Effects Operations Officer
Data Analyst
Data Analyst II
Data Exploitation Intern
Data Science Institute Graduate Student Intern
Data Warehouse Engineer
DCART Developer Intern
Departmental Analyst
DEVCOM AC Intern
Digital Forensic Examiner
Digital Network Exploitation Analyst
Digital Networks Exploitation Analyst (DNEA)
Digital Operations Specialist
Digital Supply Chain Cybersecurity Intern

APPENDIX C: JOB TITLES

Diplomatic Technology Officer

Director of Industrial Training and Assessment Center for Cybersecurity

Directorate of Science and Technology Intern

Distribution Grid Engineer - Modeling and Simulation

Doctoral Research Assistant

DOE Omni Technology Alliance Intern

DoIT Security Student Intern

E-7 Production Cybersecurity Engineer

Early Career Computer Software Engineering Technologist

Early Career Security Systems Engineer - R and D

Educational Participant

EEDIP Undergrad Technical Intern - Energy Infrastructure and Building Research

Electronics Engineer

Embedded Cybersecurity Research

Embedded Security Engineer

Embedded Security Intern

Engineering Intern

Engineering, Associate Professional Staff I

ENVOY Intern

EUCOM Volunteer Internship Program

Experiential Learning Program Intern

Exploitation Analyst

Faculty Associate - Research

Fellow

Financial Systems Specialist (Cybersecurity) and IT Specialist (Infosec)

Foreign Affairs Officer

Full Stack Software Developer

Future Leaders in Public Service Data Analysis Intern

FY 24 FLETC College Intern

General Engineer

General Student Trainee (Security Administration)

Geospatial Analyst

Global Security Graduate Student Intern

Graduate Assistant/Research Assistant

Graduate Cyber Analysis Intern

Graduate Cybersecurity Intern

Graduate Cybersecurity Summer Institute Intern

Graduate Fellow

Graduate Fellow - Digital Engineering

Graduate Intern

Graduate Research Assistant

Graduate Researcher

Graduate Services Assistant

Graduate Student Assistant

Graduate Student in Advanced Research in Cyber Systems

Graduate Student in HPC Environments

Graduate Summer Research Intern

GRC Intern Analyst

Hawaii Department of Transportation Summer Intern

Hele Imua Internship

Homeland Security Legislative Aide

Homeland Security Professional Opportunities for Student Workforce to Experience Research (HS POWER)

Honor Law Graduate

Honors Intern

HPC Cybersecurity Engineer

HPC Engineer

HPC Storage Systems Engineer

HSI Cyber Unit Volunteer Intern

ICS Attack Analyst

ICS Cybersecurity Intern

ICS Cybersecurity Researcher

ICS Expert

IDP Student/Graduate Assistant

Info Security Analyst Jr and IT Security Program Coordinator

Information Assurance Intern

Information Assurance Specialist

Information Management Specialist

Information Sciences/Cyber Operations, Associate Professional Staff I

Information Sciences/Cyber Operations, Senior Professional Staff I

Information Security Analyst

Information Security Analyst Intern

Information Security Officer

Information System Security Designer

Information Systems Security Analyst

APPENDIX C: JOB TITLES

Information Systems Security Engineer
Information Systems Security Officer
Information Systems Specialist 5
Information Technology and Cyber Risk Management Analyst
Information Technology and Cybersecurity Auditor Intern
Information Technology and Cybersecurity Undergraduate Student Trainee
Information Technology Auditor
Information Technology Cyber Risk Management Analyst
Information Technology Cybersecurity Specialist
Information Technology Cybersecurity Specialist (INFOSEC)
Information Technology Cybersecurity Specialist Intern
Information Technology Examination Analyst
Information Technology Examination Intern
Information Technology Intern
Information Technology Intern (Cybersecurity)
Information Technology Management
Information Technology Management (Application Software)
Information Technology Management Student Trainee
Information Technology Project Manager (Policy and Planning)
Information Technology Specialist
Information Technology Specialist (Customer Support)
Information Technology Specialist (Data Management)
Information Technology Specialist (Information Security)
Information Technology Specialist (Infosec)
Information Technology Specialist (INFOSEC)/IT Auditor
Information Technology Specialist (Policy and Planning)
Information Technology Specialist (Security)
Information Technology Specialist I
Instructor
Instructor of Information Systems and Technology
INSuRE Summer Researcher
Intelligence Analyst
Intelligence Officer
Intelligence Operations Specialist
Interactive Operator
Interdisciplinary (Computer Science)
Intern
Intern - Engineer, Senior
Intern - TITANS Cybersecurity – R&D Undergraduate Summer
Intern Conversion - 2025 Graduate – Cybersecurity – Cyber Dominance
Intern for NIRT (National Incident Response Team)
Intern in A4J Cyber Dominance Group
Intern R&D Graduate Summer CA CCD
Intern TITANS Cybersecurity R/D Graduate Summer
Intern with the VICEROY MAVEN intern program
Intern/Coop
International Security and Risk Management Intern
IT Analyst
IT and Security Intern
IT Cybersecurity Student
IT Cybersecurity Specialist
IT Cybersecurity Specialist (AI/MIL)
IT CYBERSECURITY SPECIALIST (INFOSEC)
IT Cybersecurity Specialist (Intern)
IT Cybersecurity Specialist (SOC Analyst)
IT Cybersecurity Specialist (Technical Support)
IT CYBERSECURITY SPECIALIST(Security)
IT Director
IT Intern
IT Network and Security Specialist
IT Operations Engineer - Windows System Administrator
IT Programmer / Analyst
IT Programmer/Analyst 11
IT Project Manager
IT Security Analyst
IT Security Analyst Intern
IT Specialist
IT Specialist (APPSW)
IT SPECIALIST (APPSW/SYSANALYSIS)
IT Specialist (Cyber)
IT Specialist (INFOSEC)
IT Specialist (INFOSEC/SYSADMIN)
IT Specialist (Operating Systems)
IT Specialist (PAQ Program)
IT Specialist (PLCYPLN/ENTARCH)
IT Specialist (Policy and Planning)

APPENDIX C: JOB TITLES

IT Specialist (Security)
IT Specialist (Sysadmin)
IT Specialist (SYSADMN/CUSTSPT)
IT SPECIALIST (SYSANALYSIS)
IT Specialist (System Administration)
IT Specialist (Systems Analysis)
IT Specialist - Cyber
IT Specialist - Digital Forensic Examiner
IT SPECIALIST I
IT Specialist Policy/Planning
IT Specialist-Digital Forensic Examiner Trainee
IT Specialist: Cybersecurity
IT Student Trainee
IT Support Technician I
IT Systems Analyst
IT Technician 2
IT/Cybersecurity Technical Intern
ITC Student Internship
ITEA Intern
ITS Cybersecurity Analyst Internship
Jr. Information Systems Security Officer (ISSO) - IT Specialist (INFOSEC)
Judicial Branch Experiential Learning Program Intern
Junior Cybersecurity Analyst Intern
Junior IT Security Analyst
Junior VMware Engineer
Lead Cybersecurity Intern
Lecturer
Lecturer - Faculty
Lecturer in the Department of Computer Science and Electrical Engineering
Legislative Cybersecurity Fellow
Louisiana State Police Cyber Crime Unit Intern
Malware Analyst
MARFORCYBER Intern
Masters Intern (NSIP)
Maven Assistant
Maven Intern
Maven Mentor
Member of Technical Staff
Metro Area Crime Center Intern
Military and Space Cybersecurity Engineer Intern
MITRE Cyber Futures - Cyber Graduate Intern
MSOC Student
National Defense and Intelligence Intern
National Security Cyber Fellow
Naval Information Warfare Center Atlantic: Cybersecurity Intern
NAVSEA (SSEP) Secure Software Development Intern
NCFI Lab Intern
NCIS (Naval Criminal Investigative Service) Honors Intern
Network Administrator
Network Analyst
Network Engineer
Network evaluator
Network Intrusion Hardware Intern
Network Manager
Network Operator
Network Security Technician
Network Specialist I
NNSA - MSIIP Intern
North Alabama Multi-Agency Crime Center Intern
NREIP Intern
NSA Co-op Student
NSA Summer 2025 Internship Program cybersecurity
NSA/NSF Funded GenCyber Student and Teacher Camp Counselor
NSF REU SITE: ASSET: Advanced Secured Sensor Enabling Technologies
NSF REU Undergraduate Researcher in Cybersecurity + AI
NSIN XForce Fellow
NSIP Master Intern Emerging Threats and Tech Division
NSIP Tech Intern - Emerging Threats and Technology
Nuclear Cybersecurity Specialist
ODA Cybersecurity Analyst
Office of the National Cyber Director Intern
Officer in Charge, Base Cybersecurity Office
OIT Security Student Assistant
OIT Security Student Assistant II
OMNI Technology Alliance Intern

APPENDIX C: JOB TITLES

Open Source Intelligence Officer
Operational Computer Systems Analyst
Operations Research Analyst
OPS Systems Programming Consultant
ORAU SSE Student Researcher at ARL
ORISE Graduate Intern at ORNL
ORISE OMNI Intern
ORISE RSI Intern
ORISE Undergraduate Intern at ORNL
ORTSOC Security Operations Analyst
Palace Acquire Program (PAQ) Cyber Intern
PAQ Computer Scientist
PAQ Science and Engineering - Computer Scientist (Project Lead Engineer)
Production Analyst
Patent Examiner
Patent Examiner (Computer Engineer)
Patent Examiner (Computer Science)
Pathways (IEP) Student Trainee (Program Analysis)
Pathways Internship - Business IT support intern
PCIP Cyber Analyst
PCIP Intern
PCTE Operations Group Intern
Penetration Tester Intern
Personnel Security General Student Trainee
Personnel Security Specialist
PhD Researcher
Policy Intern
Postdoctoral Researcher
Postdoctoral Scholar
Power Systems - Grad Intern - Cyber and Critical Infrastructure
Premier College Intern
Premier College Intern - Information Technology
Premier College Intern Program (PCIP) Student Trainee (Cyber Operations)
PREP Associate - Empirical Analysis of Emerging Technologies for 5G/6G RAN Intelligent Control
PREP Research Associate
Program Analyst
Program Assistant
Program Assistant (Cyber)
Program Associate
Program Manager
Program Support Specialist (Cybersecurity)
QNI Critical Infrastructure Protection Group Internship
R and D S and E, Cybersecurity
R and D Undergrad
Unified Platform/JCC2 Intern
RD Cybersecurity Software Engineer
Reactor Systems Engineer (Cyber)
Red Team Operator
Repperger Research Intern Program Participant
Research Aide
Research and development cybersecurity
Research and Development Graduate Summer Intern
Research and Development Intern
Research and Development Science and Engineering Computer Science
Research and Development Undergraduate Intern
Research and Development, Computer Science
Research Assistant
Research Assistant for Midwest VICEROY Institute (MVI)
Research Assistant I
Research Assistant II
Research Associate
Research Engineer
Research Engineer II
Research Experience Student Program
Research Experiences for Undergraduates
Research for Intelligence and Security Challenges Intern
Research intern
Researcher
Researcher II
Researcher III
Researcher/Co-Author
REU Student
REU TA
Reverse Engineer -- Offensive Cyber Capabilities
Reverse Engineering Intern

APPENDIX C: JOB TITLES

Reverse Engineering/Vulnerability Research Intern
RSI intern
RxIT Support Co-op
SCEP - Information Technology
Science and Technology Intern
Science Policy Fellow
Science Undergraduate Laboratory Internship (SULI) Intern
Science, Technology and Weapons Analyst
Sciences/Cyber Operations, Associate Professional Staff I
Scientist
Scientist (New Professional)
Security Analyst Intern
Security and Data Integration Intern
Security Department General Associate
Security Engineer
Security Engineering Officer
Security Intern
Security Operations Center Analyst - ITS2
Security Operations Center Intern
Senior Cybersecurity Engineer
Senior Data Engineer
Senior Embedded Security Engineer
Senior Professional Staff I
Service Desk Technician
SFS internship ORTSOC
SIP/IA Intern
SIPST Summer Intern
SOC Analyst
SOC Development Lead – Student Cybersecurity Initiatives
SOC Intern
SOC Manager
Software Developer 2
Software Development Intern
Software Engineer
Software Engineering Intern
Software Systems Engineer
Solar and Building to Grid Codified Attack Surfaces and Binary Analyses Summer Intern
Solar to Grid Codified Attack Surfaces Intern
SPARK Program Intern
Special Agent
Special Agent, Cybersecurity
SSA-OIG Non-paid intern
STEM Intern
STIPDG Intern
Student Trainee (Computer Science)
Student (IT Specialist)
Student Assistant
Student Co-op
Student Cybersecurity Analyst
Student Intern
Student Intern (Information Technology)
Student Intern - Digital Engineering
Student Researcher
Student Seasonal Worker
Student Security Analyst
Student Systems Administrator
Student Technician
Student Trainee
Student Trainee (Computer Engineer)
Student Trainee (Computer Science)
Student Trainee (Computer Scientist)
Student Trainee (Cybersecurity)
Student Trainee (Electronics Technician CYBER)
Student Trainee (Engineering)
Student Trainee (Forensic Systems Assistant)
Student Trainee (Information Technology Cybersecurity)
Student Trainee (Information Technology Management)
Student Trainee (Information Technology Specialist)
Student Trainee (Information Technology)
Student Trainee (IT Cybersecurity)
Student Trainee (IT Cybersecurity Specialist INFOSEC) ICD Fellowship GS-2210-04/11
Student Trainee (Program Analysis) Pathways Internship Experience Program (IEP)
Student Trainee (Program Support)
Student Trainee (SCIENTIST)
Student Trainee - IT Examination Intern

APPENDIX C: JOB TITLES

Student Trainee, General Engineering
Student Trainee/Engineering Intern
Student Trainee: Immigration Service Analyst
Student Volunteer
Student Volunteer Research Intern
Student Worker
Student Workforce Trainee
Student Workforce Trainee With The Cyber Division
SULI Intern
Summer Associate
Summer Associate V
Summer Cadre Intern
Summer Graduate Research Assistant
Summer Intern
Summer NSAC Intern
Summer Research Intern
Summer Research Program intern
Summer Research Program Intern (Energy Systems)
Summer Research Program Intern - Software
Summer Researcher
SURF Researcher
System Administrator
System Administrator for Veteran Engineering Incorporated
System Analyst
System Analyst for Louisville Metro Police Department
Systems Engineer
Systems Security Engineer
Systems Vulnerability Analyst
Tech Intern 4
Technical Analyst
Technical and Professional Internship Participant
Technical Instructor - Cyber Fundamentals
Technical Intern
Technician II
Technology Systems and Services
Temporary Hire Student
Temporary Part-Time Faculty
Testing and Evaluation Specialist
TITANS Software Graduate Intern
Tutorial Assistant
Undergrad Researcher
Undergrad Research Analyst
Undergrad Student Intern in A-4/Advanced Research in Cyber Systems
Undergraduate Computer Research In Cybersecurity and AI
Undergraduate Cybersecurity Research Intern
Undergraduate Cybersecurity Researcher
Undergraduate Intern
Undergraduate Intern - DHS Wired Dev. Program
Undergraduate Intern - Research Computing and IT (GHC)
Undergraduate Intern Cyber Threat Analyst
Undergraduate Research Assistant
Undergraduate Research Fellow
Undergraduate Student
University of Maryland Applied Research Lab for Intelligence and Security (RISC Intern)
UP/JCC2 Intern
US Digital Corps Participant
VICEROY CVIC Graduate Student Research Intern
VICEROY ENVOY Intern
VICEROY Intern
VICEROY MAVEN Intern
VICEROY Research Assistant
Virtualization Support Specialist IT Student Assistant
Visiting Faculty Research Program Student Intern
VITA Intern - Threat Intelligence and Vulnerability Management Team
Vulnerability Assessment Analyst
Vulnerability Manager
Web Developer

The following pages include samples of job descriptions reported by scholarship recipients.

Source: Recipients upload their position descriptions via their profile in the OPM SFS system.

Federal Deposit Insurance Corporation (FDIC) Position Description

Job Code: 70S357

Classification: Information Technology Specialist, CG-2210-09

Organizational Title: Information Technology Examination Analyst (ITEA), Division of Risk Management Supervision

Location: Regional Offices

INTRODUCTION

The position is that of an Information Technology Specialist with assignment to a regional/field office located in one of the Corporation's regions. The developmental incumbent is engaged primarily in the routine review of information systems in support of FDIC risk management examinations. The incumbent performs a variety of technical and analytical duties related to Information Technology (IT) examinations in support of examination teams. The incumbent will use risk-based examination work programs for conducting IT examinations. These work programs provide baseline procedures applicable to all examinations, and support Uniform Rating System for Information Technology (URSIT) component and composite ratings assignment. These work programs include core modules for the component ratings of Audit, Management, Development and Acquisition, and Support and Delivery. The incumbent will perform functions that support completion of IT examination work program core modules, the cybersecurity work papers, and broader information security standards work papers to assess risk and document examination procedures used, findings, and recommendations for review by the examiner-in-charge (EIC).

MAJOR DUTIES:

- Performs routine and developmental examination and evaluation functions in support of information technology and cybersecurity areas that support the bank examination process.
- As career development occurs, the incumbent may work on segments of examination review functions or work in collaboration on more complex review functions.
- Based on examination specifications, evaluates and assesses existing and new IT systems for review of cybersecurity and operational risk requirements and compliance with governing laws and regulations.
- Identifies and evaluates risks associated with IT systems and architecture vulnerabilities.
- Based on examination specifications provided, evaluates and assesses the infrastructure hardware and software that are used to manage network defenses.
- Based on examination specifications provided, evaluates and assesses an institution's incident response practices and their effectiveness in mitigating immediate and potential threats.
- Applies knowledge of IT operations related industry practices and regulatory guidance to evaluate an institution's threat and vulnerability risk assessment practices and provide tentative findings based on examination specifications.
- Applies knowledge of industry standards regarding networking, how institution systems are connected to external systems, and of current network technologies and topologies.
- Applies knowledge of rules, regulations, and standards applicable to payment systems.
- Based on examination specifications, reviews boards of directors' strategic plans, oversight and management reporting structures, and policies.
- Identifies and reports potentially unusual transactions, irregularities, weaknesses, or deficiencies to the senior specialists, analysts, or examiners.
- Prepares evaluation findings or proposed recommended actions.
- Discusses proposed findings with the examiner supervising the examination and/or the EIC.
- Documents examination findings and writes draft comments to recommend and support appropriate URSIT ratings to the EIC.
- Prepares reports and recommended assessments with necessary context related to examination findings.
- Presents findings and recommendations to higher graded analysts and examiners and to institution management.
- Communicates the status of work assignments, problems, and possible delays regularly to the EIC so resource adjustments can be made if appropriate to ensure the timely and efficient completion of IT exams.
- Discusses any deviations or unusual circumstances. Makes adjustments and recommendations as necessary based on guidance and/or advisement of senior examination staff.
- Participates in discussions and collaborative working relationships to exchange relevant information with stakeholders regarding work program use, examination findings, and recommendations.
- Uses relevant software such as Excel, Word, and Outlook to perform administrative tasks such as drafting documents, work hour reporting, expense voucher preparation, and other tasks as necessary.
- Performs other related duties as assigned.

FACTOR STATEMENTS

Factor 1 - Knowledge Required: Knowledge of current information technology environments and industry trends, current information security principles and practices to perform routine assignments in support of the evaluation and review of information security programs and systems based on approved examination specifications. Knowledge of IT risk assessment and management, IT audit, and IT security functions. Knowledge of IT security products, tools, services, regulations, and policies to support information security programs. Knowledge to review internal information technology systems, inherent risks, and operating controls. Knowledge of the FDIC's mission and functions. Knowledge of current Federal and state laws, rules, and regulations pertaining to the supervision and examination of financial institutions insured by the FDIC. Knowledge of information technology examination and audit techniques, and internal control requirements sufficient to evaluate IT concerns and vulnerability threats. Knowledge of current technology issues related to banking and the financial services industry to identify IT concerns. Basic knowledge of current technology issues related to banking and the financial services industry sufficient to document and provide recommendations to initiate response to information technology review findings. Ability to assess information technology conditions and identify problems in support of examination findings. Ability to draft and/or prepare proposed written products including reports and analyses in support of exam findings. Ability to orally communicate findings, recommendations, and/or presentations. Knowledge and experience with various software programs (e.g., Word, Excel, PowerPoint, Adobe Acrobat Reader). Ability to complete work under strict timeframes. Ability to maintain confidentiality regarding FDIC matters. Ability to work in a team environment to accomplish examination-related tasks.

Factor 2 - Supervisory Controls: The supervisor or EIC provides assignments and instructions regarding the work to be accomplished, as well as objectives, priorities, and timeframes for completion. The incumbent independently plans and carries out assignments, exercises judgment in resolving routine or common problems and issues, and consults with the supervisor, EIC, and/or senior examination staff for guidance and direction on priorities, deadlines, and unusual or controversial issues and problems. The incumbent keeps the EIC and/or higher-graded specialist/examiner and supervisor informed of progress and potentially controversial matters. Completed work is reviewed for technical soundness, appropriateness, and conformity to policy. Work is reviewed upon completion for conformance with policies and instructions, effectiveness of approach and methods used, technical competence, and adherence to deadlines.

Factor 3 - Guidelines: Guides include the Federal Financial Institutions Examination Council IT Examination Handbook, the FDIC's IT and operations risk examination procedures, Information Technology Risk Examination or (InTREx Program), and other federal and state statutes, regulations, supervisory guidance, policy manuals, and statements. The incumbent may select and apply routine precedent and/or guideline(s) most appropriate to the particular task being performed. Deviations from guidance are referred to the supervisor, EIC, or senior examiner for further review and discussion of recommendation versus impact.

Factor 4 - Complexity: The work involves the execution of developmental and/or routine stages of information technology examinations, requiring analysis with regard to information systems and application integrity. Assignments consist of performing varied duties by applying a series of established methods, practices, and techniques involving a number of different administrative, technical, and analytical tasks. Assignments require the application of established work methods and procedures. The incumbent analyzes and evaluates systems and programs, identifies patterns and conditions, and develops findings and recommendations while conducting periodic information technology related reviews. Work requires making recommendations or collaborative decisions concerning interpretation of data, planning of work, and refinement of the methods and techniques to be used.

Factor 5 - Scope and Effect: The work involves investigating and analyzing a variety of routine problems, questions, or conditions associated with particular applications or information systems in the analysis of a bank examination or IT examination of a bank service provider. The incumbent evaluates current IT systems and structures, considering future changes in program requirements. Assignments involve preparation and completion of work programs, and proper and accurate documentation is essential to maintaining records in compliance with outstanding work paper guidelines. The incumbent uses standard methods to resolve conventional problems and issues. Advice provided, recommendations issued, and decisions made by the incumbent with an experienced co-worker must be of high quality to ensure decision and conclusion accuracy during the examination and evaluation process. Analyses and recommendations issued regarding the quality of a financial institution's IT program have a direct and significant impact on the institution's rating.

Factor 6 - Personal Contacts: Contacts include persons outside the organization, such as bankers, financial institution representatives, co-workers, representatives of other regulatory agencies and other interests, including agency staff and co-workers, in moderately unstructured settings.

Factor 7 - Purpose of Contacts: Contacts are for planning and coordinating work assignments, obtaining information, explaining bank laws and determinations, resolving differences, identifying options and alternatives, and proposing corrective action agreements. The incumbent learns the role and authority of each party during the course of meetings to gain or obtain information, assess, and discuss the program information reviewed.

Factor 8 - Physical Demands: This is a sedentary work position with occasional physical activity when moving examination materials. This position will require frequent overnight travel, as necessary.

Factor 9 - Work Environment: Work is performed in an office setting.

Department of the Interior (DOI) - IT Cybersecurity Specialist

Occupational Series: GS-2210 - Information Technology Management

POSITION OVERVIEW

Are you a high performer looking for a new adventure? Do you have a passion for working in a dynamic environment that offers new challenges and opportunities every single day? If so, consider applying as a cybersecurity specialist! As a cybersecurity specialist you can make a difference by protecting DOI's mission critical systems and defending them from domestic and foreign cyber-attacks. The cybersecurity specialist is responsible for a wide range of complex assignments to ensure the confidentiality, integrity, and availability of all systems. Potential assignments include protecting DOI's infrastructure, testing and implementing new technologies, implementing cybersecurity policies, managing vulnerabilities, and responding to incidents. The specialist is also called upon to provide advice, instruction, or any other expertise to key decision makers, other employees, or supervisors.

This position is represented at the following Department of the Interior (DOI) bureaus:

Bureau of Indian Affairs (BIA)	Bureau of Land Management (BLM)	Bureau of Ocean Energy Management (BOEM)	National Park Service (NPS)	U.S. Fish and Wildlife Service (FWS)
Bureau of Reclamation	Bureau of Safety and Environmental Enforcement (BSEE)	Department of the Interior (Main / Secretary's Office)	Office of Surface Mining Reclamation and Enforcement (OSMRE)	U.S. Geological Survey (USGS)

CANDIDATE DESCRIPTION

The ideal candidate is a creative thinker with a passion for cybersecurity who is willing to tackle complex problems. The candidate is also adaptable, with a willingness to learn and stay abreast of new cybersecurity threats, vulnerabilities, and technologies, and well versed in problem solving. The candidate will possess knowledge and skill in applying IT security and cybersecurity principles and methods, and an understanding of federal cybersecurity requirements, policies, procedures, guidelines, and standards.

SPECIALTY AREAS

Cyber Defense Analysis	Cyber Defense Infrastructure Support	Cyber Governance	Cybersecurity Management	Cybersecurity Operations
Incident Response	Information Assurance	Risk Management	Threat Analysis	Vulnerability Assessment and Management

WORK ENVIRONMENT

The work area is adequately lighted, heated, and ventilated. The work environment involves everyday risks or discomforts that require normal safety precautions. Some employees may occasionally be exposed to uncomfortable conditions in such places as research facilities.

RESPONSIBILITIES AND CAREER LEVEL REQUIREMENTS

- **Entry:** Assists higher-graded specialists in providing customer training. Identifies and resolves problems in response to customer reported issues, and researches, evaluates, and provides feedback on problematic trends and patterns. Implements security measures to ensure controlled access and maintains data integrity and confidentiality.
- **Mid:** Coordinates the implementation of security programs across platforms and establishes vulnerability reporting criteria working with communities. Recommends ways to protect the bureau/office's information and information systems. Modifies, adapts, and/or refines broader guidelines to resolve specific complex and/or intricate issues and problems; and identifies and researches trends and patterns in order to develop new methods and criteria and/or propose new policies and practices.
- **Journey:** Serves as the senior principal contact for DOI responsible for a wide range of complex assignments and projects relative to information systems and cybersecurity matters. As an expert, ensures the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools.

APPENDIX D: POSITION DESCRIPTIONS AND JOB SUMMARIES

COMPETENCY GRADE MATRIX

Competency / Attribute	Entry (GS 5-7)	Mid (GS 9-11)	Journey (GS 12-13)
Accountability	Level 5-7	Level 9-11	Level 12-13
Organizational Awareness	Level 5-7	Level 9-11	Level 12-13
Influencing/Negotiating	Level 5-7	Level 9-11	Level 12-13
Strategic Thinking	Level 5-7	Level 9-11	Level 12-13
Attention to Detail	Level 5-7	Level 9-11	Level 12-13
Partnering	Level 5-7	Level 9-11	Level 12-13
Information Management	Level 5-7	Level 9-11	Level 12-13
Teaching Others	Level 5-7	Level 9-11	Level 12-13
Compliance	Level 5-7	Level 9-11	Level 12-13
Problem Solving	Level 5-7	Level 9-11	Level 12-13
Interpersonal Skills	Level 5-7	Level 9-11	Level 12-13
Teamwork	Level 5-7	Level 9-11	Level 12-13
Creative Thinking	Level 5-7	Level 9-11	Level 12-13
Project Management	Level 5-7	Level 9-11	Level 12-13
Learning	Level 5-7	Level 9-11	Level 12-13
Technical Competence	Level 5-7	Level 9-11	Level 12-13
Customer Service	Level 5-7	Level 9-11	Level 12-13
Reasoning	Level 5-7	Level 9-11	Level 12-13
Oral Communication	Level 5-7	Level 9-11	Level 12-13
Writing	Level 5-7	Level 9-11	Level 12-13
Decision Making	Level 5-7	Level 9-11	Level 12-13
Resilience	Level 5-7	Level 9-11	Level 12-13

NASA Position Description #1078940

NASA Title: IT Cybersecurity Specialist | OPM Title: IT Cybersecurity Specialist

Plan-Series-Grade: GS-2210-09 | Full Performance Level: GS-13

Activity Location: John Glenn Research Center at Lewis Field, Brook Park, Cuyahoga, Ohio

Org Structure: V000 - Office of Chief Information Officer | VB00 - Enterprise Division | VBB0 - Cybersecurity Operations Office

Supervisor Certification: Certified by Gilbert Winter (11/05/2024) - SUPV IT Cybersecurity Specialist

Classification Certification: Classified by Kelly Elliott (09/28/2019) - Assistant Human Resources Officer

INTRODUCTORY STATEMENT

This position is located in NASA and is included within a specialty series that involves IT Cybersecurity. Examples of the work will vary depending on each Center's role and responsibility to the mission.

MAJOR DUTIES (TOTAL TIME: 100%)

Using specialty expertise as an Information Technology Cybersecurity Specialist, the individual performs a combination of some or all of the following duties. More specific duties, as determined by management and organizational needs, will be reflected in the individual's performance plan. This position includes individuals who manage, supervise, administer, lead, advise on, or perform work that involves the design, documentation, development, modification, testing, installation, implementation, and support of new or existing applications software. Individuals generate and/or apply theories, principles, practical concepts, systems, and processes related to some or all of the following areas:

- Network Services, Application Software, Operating Systems, Systems Analysis, Policy and Planning, Security, Cybersecurity, Data Management, Internet, Systems Administration, Customer Support, Enterprise Architecture.

Information Technology Individuals General Requirements:

- Apply the full range of subject matter methods, principles, practices, and evaluative methodologies sufficient to advise on and/or resolve a range of operational and/or strategic issues which may range from recurring through complex and unprecedented;
- Utilize a wide range of subject matter practices, laws, regulations, policies, and precedents and uses a range of analytical methods to identify, evaluate, and recommend appropriate solutions;
- Provide written and oral communication techniques sufficient to develop and deliver briefings, project papers, status/staff reports, and correspondence to managers to foster understanding and acceptance of findings and recommendations;
- Research, learn and apply a wide range of qualitative and/or quantitative methods to identify, assess, analyze and improve products and services;
- Plan, direct and/or coordinate subject matter work which requires the application of the appropriate knowledge of subject matter or program area.

Typical Duties Include:

- Identifies, mitigates, and/or eliminates system and/or application security threats;
- Develops software programs and/or hardware systems designed to neutralize security threats;
- Analyzes and refines system requirements;
- Supports new or existing applications software;
- Troubleshoots and resolves customer identified application and/or hardware issues;
- Translates systems requirements into applications prototypes;
- Plans, designs, and develops systems architecture;
- Writes, debugs, and/or maintains code;
- Identifies, determines, and designs applications architecture;
- Determines output media/formats;
- Designs, develops and/or implements user interfaces;
- Works with customers to design, develop, and/or test applications;
- Assures software and systems quality and functionality;
- Integrates hardware and software components;
- Drafts and/or maintains program documentation;
- Evaluates and/or tests new applications software technologies;
- Ensures the rigorous application of information security/information assurance policies, principles, and practices to the delivery of application software services;
- Leads and/or serves on team(s) as the subject matter specialist/representative or expert as appropriate.

POSITION REQUIREMENTS

- This position requires the incumbent to be proficient in the English language.
- This position may require the incumbent to successfully obtain and maintain a top secret/SCI clearance.

NASA Factor Evaluation System (FES) Summary

1. Knowledge (Level 6, 950 Points): Knowledge and skill to utilize standardized analytical tools when applying fundamental administrative principles and practices to evaluate complex, non-controversial, and factual issues for which there are one or more readily apparent solutions. Ability to perform management advisory services for specific requests related to immediate administrative problems of limited scope, and to analyze and recommend solutions to issues concerning broader specializations including their impact on the occupational area. Conducts fact-finding interviews with supervisors and employees to obtain information about organizational functions and work procedures.

Position Unique Knowledge 1: Knowledge of and skill in applying IT concepts, principles, methods, and practices. Knowledge of the mission and programs of customer organizations as well as the organization's IT infrastructure. Ability to apply acquisition management policies and procedures, cost-benefit analysis principles and methods, and analytical methods and practices. Knowledge of and skill in applying performance management/measurement methods, tools, and techniques sufficient to perform systems testing and evaluation principles. Knowledge of IT security principles and methods, requirement analysis principles and methods, and COTS products and components. Ability to apply Project management principles and methods and oral and written communication techniques. Knowledge of Internet technologies to analyze the Internet potential of systems, networks, and data to address new and emerging information technologies and/or industry trends. The above knowledge(s) are necessary sufficient to: Plan and carry out difficult and complex assignments and develop new methods, approaches, and procedures; provide advice and guidance on a wide range and variety of complex IT issues. Interpret IT policies, standards, and guidelines; conduct analyses and recommend resolution of complex issues affecting the specialty area. Evaluate and recommend adoption of new or enhanced approaches to delivering IT services. Test and optimize the functionality of systems, networks, and data. Identify and define business or technical requirements applied to the design, development, implementation, management, and support of systems and networks.

2. Supervisory Controls (Level 3, 275 Points): The supervisor makes assignments by defining objectives, priorities, and deadlines and assists the employee with unusual situations that do not have clear precedents. The employee plans and carries out the successive steps and handles problems and deviations in the work assignments in accordance with instructions, policies, previous training, or accepted practices in the occupation. Completed work is usually evaluated for technical soundness, appropriateness, and conformity to policy and requirements. The methods used in arriving at the end results are not usually reviewed in detail.

3. Guidelines (Level 3, 275 Points): Guidelines are available but are not completely applicable to the work or have gaps in specificity. The employee uses judgment in interpreting and adapting guidelines, such as agency policies, regulations, precedents, and work directions for application to specific cases or problems. The employee analyzes results and recommends changes.

4. Complexity (Level 3, 150 Points): The work includes various duties involving different and unrelated processes and methods. The decision regarding what needs to be done involves various choices that require the employee to recognize the existence of and differences among a few easily recognizable situations. Actions to be taken or responses to be made differ in such things as the source of information, the kind of transactions or entries, or other differences of a factual nature.

5. Scope / Effort (Level 3, 150 Points): The work involves treating a variety of conventional problems, questions, or situations in conformance with established criteria. The work product or service affects the design or operation of systems, programs, or equipment; the adequacy of such activities as field investigations, testing operations, or research conclusions; or the social, physical, and economic well-being of people.

6. Personal Contacts (Level 2, 25 tap Points): The personal contacts are with employees in the same agency but outside the immediate organization. People contacted generally are engaged in different functions, missions, and kinds of work, e.g., representatives from various levels within the agency, such as headquarters, regional, district, or field offices, or other operating offices at the immediate installation; AND/OR The contacts are with members of the general public, as individuals or groups, in a moderately structured setting.

7. Purpose of Contacts (Level 2, 50 Points): The purpose is to plan, coordinate, or advise on work efforts, or to resolve operating problems by influencing or motivating individuals or groups who are working toward mutual goals and who have basically cooperative attitudes.

8. Physical Demands (Level 1, 5 Points): The work is sedentary. Typically, the employee sits comfortably to do the work. However, there may be some walking; standing; bending; carrying of light items, such as papers, books, or small parts; or driving an automobile. No special physical demands are required to perform the work.

9. Work Environment (Level 1, 5 Points): The environment involves everyday risks or discomforts that require normal safety precautions typical of such places as offices, meeting and training rooms, libraries, residences, or commercial vehicles, e.g., use of safe work practices with office equipment, avoidance of trips and falls, observance of fire regulations and traffic signals. The work area is adequately lighted, heated, and ventilated.

Total Points: 1885 | Points Range: 1855 - 2100 = Grade GS-09

National Security Agency (NSA) Job Announcement

Title: Research Scientist / Computer Systems Researcher - Mid to Expert Level (Maryland)

Location: Fort Meade, MD | Salary Range: $102,477 - $191,900 per year

School Alumni Focus in Image: Morgan State University

ABOUT THE JOB & RESPONSIBILITIES

NSA Research Scientists are actively expanding the boundaries of what can be accomplished with artificial intelligence, machine learning, human-machine teaming, software reverse engineering, data science, novel architectures, cyber security, high performance computing, and computational linguistics. Our experts generalize mission problems, advance the scientific state-of-the-art to solve problems, and work with other NSA organizations to get solutions in front of mission users and decision-makers. Our researchers also have the opportunity to collaborate regularly with the scientific community, academia, industry, and other government laboratories; publish papers on unclassified aspects of our work in scientific journals and at conferences; transfer NSA technology to the marketplace through open source software releases and public-private partnerships; serve as faculty members at local universities; and participate in university and K-12 STEM outreach activities across the country. The ideal candidates must be able to demonstrate sound judgement, strong technical skills and the ability to work effectively in a dynamic team environment, as well as independently. Excellent oral and written communication skills, and a proven track record of analyzing and solving technical problems with innovative solutions are also preferred. The candidate should have demonstrated success in conducting Computer Science research to include turning research ideas into running prototype-grade systems. As a Research Scientist, other responsibilities may include:

- Conducting scientific experiments, documenting results, and communicating with colleagues, customers, and decision makers.
- Training, testing, and deploying machine learning models.
- Applying software engineering principles to design and/or develop software applications.
- Designing and optimizing algorithms, data structures, modeling, and analytics to solve real-world scientific problems.
- Using principles, techniques, procedures, and tools to architect and facilitate the development of hardware solutions.
- Developing methods and applications for tools to exploit and analyze computer systems and network vulnerabilities.
- Modeling, simulating, prototyping, and/or benchmarking high performance computing systems.
- Developing and implementing approaches to increase the productivity and/or efficiency of high performance computers.

QUALIFICATIONS & CAREER ENTRY LEVELS

Degree must be in Computer Science (CS) or Computer Engineering (CE). Other STEM fields (e.g., Engineering, Mathematics, or Information Systems (IS)) may be considered relevant if the programs contain, at minimum, a concentration of courses in the following foundational CS areas: algorithms; computer architecture (not network architecture); programming methodologies and languages; data structures; logic and computation; and advanced mathematics (for example, calculus, discrete mathematics). Relevant experience must be in one or more of the following: computer systems research, simulation/model development and prototyping, software design, programming, computational science, algorithm analysis and design, reverse engineering, designing/developing computer or information systems, including engineering hardware or software, machine learning, artificial intelligence, visualization, human-computer interaction, data science, or high performance computing.

FULL PERFORMANCE Entry: Bachelor's degree plus 3 years of relevant experience OR a Master's degree plus 1 year of relevant experience OR a Doctoral degree and no experience. An Associate's degree plus 5 years of relevant experience may be considered for individuals with in-depth experience that is clearly related to the position.

SENIOR Entry: Bachelor's degree plus 6 years of relevant experience OR a Master's degree plus 4 years of relevant experience OR a Doctoral degree plus 2 years of relevant experience. An Associate's degree plus 8 years of relevant experience may be considered.

EXPERT Entry: Bachelor's degree plus 9 years of relevant experience OR a Master's degree plus 7 years of relevant experience OR a Doctoral degree plus 5 years of relevant experience. An Associate's degree plus 11 years of relevant experience may be considered.

SKILLS AND DESIRED AREAS

Relevant experience in speech, image, video or text processing and/or data science, applied machine learning or artificial intelligence across the disciplines of Human Language Technology (HLT), Computer Vision (CV), Natural Language Processing (NLP) and Natural Language Understanding (NLU). Additionally, applicants with experience in visualization, data analysis, machine learning model research, development, and evaluation, data engineering, multilingual and multimodal modeling, automatic speech recognition (ASR) or language modeling, large language models (LLM) or related topics are especially encouraged to apply. Candidates with knowledge, skills and experience in high performance computing are also strongly encouraged to apply; in particular, processor and system architectures and networks, memory, tasking (accelerators, parallelism, resource management, heterogeneous computing), productivity (systems modeling & simulation, evaluation, prototyping and benchmarking), scalable algorithms, programming languages and libraries, and hardware-software co-design.

Desired Skills: Applicants should have excellent problem-solving, communication, and interpersonal skills, and possess a range of knowledge and experience in at least two of the following areas: - Programming (low level, high level, parallel) - Artificial Intelligence and Machine Learning - Simulation/model development and prototyping - Software engineering - Hardware engineering - Architectures and Distributed Computing - Algorithm analysis and design - Reverse engineering - Operating systems and/or device driver development (desktop/server/RTOS)

USDA Forest Service Position Description

Master Record Number: FS2802

Title/Pay Plan/Series/Grade: Information Technology Specialist, GS-2210-07 | FLSA Code: Non-Exempt

Organizational Setting: Located on a Forest Service Unit or performs work from a virtual location. Advanced trainee position.

MAJOR DUTIES

- Performs a variety of developmental basic/conventional IT tasks. Typical tasks include:
- Collecting specific information from reference sources, software utilities, or customers.
- Performing basic troubleshooting of networks, web pages, workstations, or personal computers under close direction of more senior IT staff.
- Providing advice and guidance on a wide range and variety of IT issues.
- Conducting analyses and recommending resolution of basic issues affecting a particular IT specialty area.
- Assisting customers in installing applications; troubleshooting post-installation problems; and coordinating the technical support of deployed applications.
- Performing routine maintenance of electronic files including tasks such as making tape/disk backup copies of hard disk information, retrieving files from backup tapes/disks, or using file transfer protocol (FTP) software to add or update files on Web servers.
- Performing minor editing of HTML documents.
- Staffing an IT help desk to record information on customer problems, offering basic solutions, and forwarding problems to the appropriate IT staff member.
- Performing basic installations or upgrades of common hardware or applications software.
- Providing basic computer security briefing to new employees. Issuing, resetting, and deactivating passwords and customer accounts.

FACTOR STATEMENTS

Factor 1. Knowledge Required by the Position (Level 1-6, 950 Points): Knowledge of basic IT principles and practices sufficient to perform structured, developmental work designed to provide broader and more in-depth knowledge and skill needed to perform higher-level assignments. Knowledge of acquisition management policies and procedures; cost-benefit analysis principles and methods sufficient to recommend the acquisition of products that provide for integration among a variety of systems. Basic oral and written communication skills to communicate factual and procedural information clearly to users and customers.

Factor 2. Supervisory Controls (Level 2-2, 125 Points): The supervisor provides continuing developmental assignments by indicating what is to be done, the quality and quantity expected, etc. The supervisor provides advice on new or difficult assignments. The incumbent uses initiative in carrying out recurring assignments independently without specific instructions and refers deviations to the supervisor for help or a decision. The supervisor reviews completed work closely for compliance with instructions and established procedures.

Factor 3. Guidelines (Level 3-2, 125 Points): The incumbent uses specific and detailed IT guidelines that cover most aspects of the work. The incumbent uses judgment in locating and selecting the most appropriate guidelines for each situation. The supervisor or designated employee must authorize any deviations from the guidelines.

Factor 4. Complexity (Level 4-2, 75 Points): The work consists of easily distinguishable tasks involving related steps, processes, methods, and procedures. Assignments are designed to provide the incumbent with experience and training in a variety of well-defined tasks, and to expose them to a variety of basic IT methods and practices. The incumbent decides what needs to be done by choosing from various alternatives and recognizing differences among a few easily distinguishable situations. The incumbent uses judgment regarding the most appropriate approach that is in accordance with established procedures and practices. Actions to be taken differ depending on the kind of IT related duty being performed.

Factor 5. Scope and Effect (Level 5-2, 175 Points): The primary purpose of the position is to provide the IT Specialist with the training and experience to perform work at a more responsible level. Assignments will include recurring duties that include a variety of separate tasks or procedures and those which familiarize the employee with a range of IT programs and services. Work affects the work of others but has little impact beyond the immediate organizational unit or beyond the delivery of limited services in a timely manner to others.

Factor 6 & 7. Personal Contacts & Purpose (Level 6/7-2A, 45 Points): Contacts are primarily within the immediate office or with IT specialists in other units, and with IT customers. The purpose of contacts is to obtain and provide information.

Factor 8. Physical Demands (Level 8-1, 5 Points): The work is sedentary but may involve extended periods working at a keyboard and monitor. Work may also involve carrying or moving computer components and supplies.

Factor 9. Work Environment (Level 9-1, 5 Points): The work area is adequately lighted, heated, and ventilated.

Total Points: 1405 | Point Range: 1355 – 1600 = GS-07

Network Enterprise Center (NEC) Fort Gordon Position Duties

Role: Systems Administrator and Information Technology (IT) Customer Support Specialist (Hosting and Hoteling Branch, Enterprise Systems Division)

Core Responsibilities: Responsible for all matters concerning IT Desktop Systems Administration, Customer Support and Service Operations associated with Commercial Solutions for Classified (CSfC), Multiple Independent Levels of Security (MILS) solutions and Cross Domain Solutions (CDS). Executes Tier II operational assistance.

MAJOR DUTIES

- Conducts installations and implementation of Operating System (OS), new system hardware, and software.
- Provides ongoing support, resolution of problems, and recovery of operating malfunctions involving various hardware components and software failures.
- Troubleshoots network connectivity, server connections, PC hardware, Mobile Wi-Fi (MIFI) Wireless Hotspot Devices and software to determine the cause of failure.
- Re-installs any software as needed and performs all required software upgrade(s).
- Resolves trouble tickets that cannot be resolved by Tier I and Tier II technicians, and provides consulting services to the network administrator, database analyst, for specifically difficult problems. Trouble calls cover hardware/software configuration, repair, and user training.
- Provides customer assistance to all users. Creates and provisions accounts/access to the Gordon CSfC/MILS/CDS solutions. Troubleshoots customer access using the Gordon Trusted Thin Client – Remote solution.
- Manages Windows and Red Hat Enterprise Linux Operating Systems, to include creating, deploying, and patching the image.
- Plans, coordinates, develops, tests, documents, installs, and maintains desktops associated with the Fort Gordon CSfC node, and user activities associated with it.
- Maintains constant system quality control to ensure that regulatory and security requirements are met. Maintains systems and software associated with the Fort Gordon MILS and CDS solutions.
- Represents NEC-Fort Gordon at Department of Defense (DoD), Department of the Army (DA), command and installation meetings and conferences.
- Identifies adverse trends and equipment shortcomings and manages operating systems such as Windows and Red Hat Enterprise Linux. Recommends methods and procedures and coordinates corrective action to optimize utilization of equipment and software.
- Works with technical support personnel in various organizations resolving critical problems within the Tier II Program and provides technical advice to users.
- Provides consultation and instruction to functional area users on file accessing techniques, search strategies, processing and space utilization efficiencies, security procedures, backup and program recovery techniques, and testing techniques.
- Oversees function tests of the hardware/software to maintain compliance with update hardware/software compliance lists as released.
- Conducts testing to ensure operability, efficiency, and compliance with existing procedures and regulations to maintain compliance with National Security Agency (NSA) regulations, Army Cross Domain Management Office, National Institute for Standards and Technology (NIST), Risk Management Framework (RMF) requirements, and other command/cyber requirements as directed.
- Maintains access control to system in accordance with (IAW) applicable regulations and directives. Develops standard operating procedures (SOP), system security plans, and other security relevant documentation. Provides central operational support for all shared computing equipment and devices attached to the network.

FBI Digital Operations Specialist

AN INSIDE LOOK

Digital operations specialists are technical experts on investigative teams who specialize in criminals' use of technology. This could range from identifying a bank robber by analyzing his or her digital footprint to targeting technologically sophisticated adversaries. This work illuminates relevant information while also minimizing the FBI's digital exposure during operations.

JOB DUTIES

- Maximize investigators' technical collection on their subjects by identifying new sources of collection (e.g. backup data, points of exploitation on a target's devices and networks).
- Assist investigators who are encountering subjects using anonymization techniques (e.g. VPN and Tor, virtual currencies, or conducting illegal activity on the Dark Web).
- Analyze and interpret technical data, such as iCloud, PCAP, or imaged servers to suit investigative needs.

KEY SKILLS

- Computer Science: Familiarity with different operating systems, physical computer components and architectures, virtual machines, and scripting.
- Network Fundamentals: Knowledge of networking and routing protocols, network securities methodologies, and operations of various communications media.
- Computer Vulnerabilities and Devices Security: Knowledge of common computer/network infections, methods of infection, and attack methods and techniques.

CJIS Technical Auditor II - Texas DPS

Division: Crime Records Division (CRD) | State Class/Group: Information Technology Auditor II (0248/B24)

General Description: Performs complex (journey-level) information systems auditing. Work involves conducting technical audits of statewide law enforcement agencies for compliance with the FBI CJIS Security Policy, interviewing law enforcement and government officials at agencies with connectivity to state and federal repositories, and preparing audit findings regarding the efficiency, accuracy, and security of financial and non-financial programs to ensure consistency in safeguarding CJIS data across agencies. Work is performed under general supervision with moderate latitude for the use of initiative and independent judgment.

ESSENTIAL DUTIES / RESPONSIBILITIES

- Provide general administrative support disseminating information internally and externally to the public, law enforcement and criminal justice communities.
- Schedule and coordinate law enforcement and Criminal Justice agencies for CJIS Security Policy technical audits as mandated.
- Interview senior law enforcement and government IT officials at agencies with connectivity to State and Federal repositories.
- Participate in planning and scheduling technical audit trips and coordinate the technical audit visits with user agency managers to assure availability of resources for audit activities; plan and implement personal travel schedules and itineraries accordingly.
- Prepare Security Review packages for each agency prior to trips to ensure that pre-audit data and necessary forms and information are readily available during audit performance at the user agency site.
- Maintain current and up-to-date knowledge regarding all changes to the security policy and how it impacts audit requirements.
- Prepare formal audit report of findings for each agency audited to identify compliance and deficiency factors and summarize results of each audit; track and receipt the compliance measures taken by audited agencies.
- Participate in training agencies on the policies and operating procedures required for obtaining and maintaining access to criminal justice data and advise agency on the penalties for non-compliance.
- Review the design of networks, system configuration, and physical security for compliance with the CJIS security policy, conduct post audits to agencies where modifications have been made.
- Prepare articles for Crime Records Newsletter and assist with preparing periodic reports; determine requirements and obtain supplies, equipment and materials for auditing activities.

California Department of Toxic Substances Control (DTSC) Duty Statement

Classification Title: Information Technology Specialist I | Working Title: Forensic Specialist

Division/Office: Hazardous Waste Management Program - Office of Criminal Investigations (OCI)

Reporting Location: Sacramento (Cal Center Regional Office) | Supervisor: Supervising Criminal Investigator II

POSITION DESCRIPTION & ESSENTIAL FUNCTIONS

Primary Domain: Information Security Engineering; Secondary Domain: IT Project. The ITS I is responsible for gathering, compiling, and analyzing data from electronic information processing systems as evidence of violations of California's Hazardous Waste Law. The ITS I works closely with the Office of Criminal Investigations IT III in assisting in the oversight of DTSC's Sacramento Laboratory. The ITS I safeguards, operates, and maintains in working condition surveillance equipment owned by DTSC that is used in the course of investigations.

DUTIES INCLUDE:

55% - Computer Forensics Investigative Support: Assists OCI Investigators on cases alleging violations of California Hazardous Waste Control Law by accessing and analyzing electronic data from a variety of electronic data processing networks, systems, devices, and storage media. Defines requirements for draft search warrants to ensure the inclusion of appropriate electronic data processing devices to be seized. Respond to environmental crime scenes and participate in searches and inspections to ensure electronic data processing devices at the scenes are identified and investigated. Interview employees and representatives of entities being searched to ascertain the locations and status of data processing equipment as well as data practices at the site to ensure all needed data processing and storage devices are identified and imaged. Documents the removal and/or imaging/copying of equipment contents from/at crime scenes and ensures that chain-of-custody mandates are followed as the equipment/contents are transported and handled. Computer forensics software retrieves information systems and reviews and analyzes information for use as evidence of hazardous waste violations. Retrieval of digital evidence can be from complex multi-user and multi-location computer networks and is done in a manner consistent with computer forensic practices which allows such evidence to be admissible in legal proceedings. Provides technical advice to investigatory staff, management as well as legal staff on complex information technology matters, provides testimony in civil and criminal proceedings. May attend environmental enforcement task force meetings, assist other agencies with non-DTSC cases and perform forensic computer work at non-DTSC facilities.

25% - Surveillance Camera Investigative Support: Maintains and operates surveillance camera equipment owned by DTSC that is deployed to observe and record violations of California Hazardous Waste Control Law. Consults with the lead Investigator and IT III to develop a surveillance plan that includes, but is not limited to, pinpointing a camera location, securing approval from property owners for camera installation, getting access to electric power for camera operation, scheduling installation, testing the camera operation, and ensuring proper visual resolution of images. Downloads evidence from the camera, compiles, and documents camera evidence of violations, and maintains records on camera use. Maintains database of camera images and is responsible for retrieving camera when surveillance is over, checking, and prepping camera for upcoming cases and safeguarding camera and associated equipment while in storage.

10% - Operational and Security Support: The incumbent is responsible for operations and maintenance in the deployment of technologies supporting OCI. The incumbent must adhere to the Office of Environmental Information Management's (OEIM) Operational and Security policies, guidelines, standards, and practices to support DTSC. All technology equipment, services, and tools must be implemented and aligned to OEIM's best practices. Collaborate with technical experts to ensure compliance and respond to security incidents promptly. Follow directives from the Information Security Office (ISO) regarding assessments/audits, vulnerability management, and incident response procedures. Ensure the confidentiality, integrity, and availability of production systems and aid in the continuous improvement of security strategies to evolving threats and regulatory requirements.

10% - Training, Forensics, Surveillance Education and Training: Participates in ongoing computer forensic training, surveillance camera training, new information technology training and professional development classes through involvement with computer forensics professional organizations. The incumbent must obtain and maintain the technology certificates required to operate the technologies used by the OCI Forensic and Surveillance unit. Provides, directs, conducts, oversees, and delivers forensic and surveillance education and training for all DTSC and CalEPA enforcement employees on an annual basis. Provides presentations, and briefings for enforcement programs and various discrete audiences and venues on information forensic and surveillance issues. Collaborates with CalEPA's enforcement programs and senior managers to implement the best available forensic processes and procedures.

MARGINAL FUNCTIONS

5% - Administrative Duties: Performs administrative duties including, but not limited to: adhering to Department policies, rules and procedures, submitting administrative requests including leave, overtime, travel and training in a timely and appropriate manner; accurately reporting time in the Daily Log system, and submitting timesheets by the due dates. Accurately documents time and expenses spent on each case for possible reimbursement to the Department at case closure/settlement.

5% - New Equipment Research and Purchases: Researches, tests, and gives feedback to IT III and OCI management about new computer forensic hardware and software applications and surveillance equipment; communicates with vendors regarding the use of hardware and software and surveillance equipment, and initiates and monitors procurement of new computer forensic hardware and software and surveillance equipment.

USAJOBS Announcement: IT Specialist (Artificial Intelligence)

Department: Department of the Treasury (Agency Wide) | Salary Range: $89,508 to $197,200 per year

Pay Scale & Grade: GS 12 - 15 | Series: 2210 Information Technology Management

SUMMARY & DUTIES

- As an IT Specialist (Artificial Intelligence), you will be responsible for formulating technical strategies, standards, & architectures that advance the secure & ethical deployment of AI across Treasury and, by extension, the federal government. You will ensure Treasury's systems meet mission, cybersecurity, & performance requirements using best practices including Agile, DevSecOps, and Digital Engineering. Duties include:
- Formulate and direct enterprise-wide AI engineering strategies for AI-enabled systems, computer hardware/software integration, and cloud-native architectures, ensuring compliance with federal mandates and Executive Orders.
- Design, develop, and evaluate advanced computer engineering solutions for secure AI system deployment, incorporating cybersecurity-by-design and DevSecOps principles.
- Lead and coordinate cross-agency AI engineering projects involving large-scale digital transformation, data platforms, and secure computing infrastructures.

SPECIALIZED EXPERIENCE REQUIREMENTS

- **GS-15:** One year of specialized experience equivalent to the GS-14 level. Includes directing collaborative projects AND leading enterprise cloud-native modernization efforts AND advising high-ranking officials on AI, cloud, and data initiatives.
- **GS-14:** One year of specialized experience equivalent to the GS-13 level. Includes collaborating with Senior Executives to ensure alignment of emerging technology adoption with Administration priorities AND conducting cybersecurity risk assessments for AI-enabled systems.
- **GS-13:** One year of specialized experience equivalent to the GS-12 level. Includes applying cybersecurity practices in AI or cloud environments AND participating in Agile development teams, contributing to sprint planning or execution.
- **GS-12:** One year of specialized experience equivalent to the GS-11 level. Includes assisting in designing, developing, testing, or deploying AI models and prototypes.

APPENDIX E: STUDENTS RELEASED FROM OBLIGATIONS

Number of Students awarded the scholarship that were granted a waiver or have a request pending.

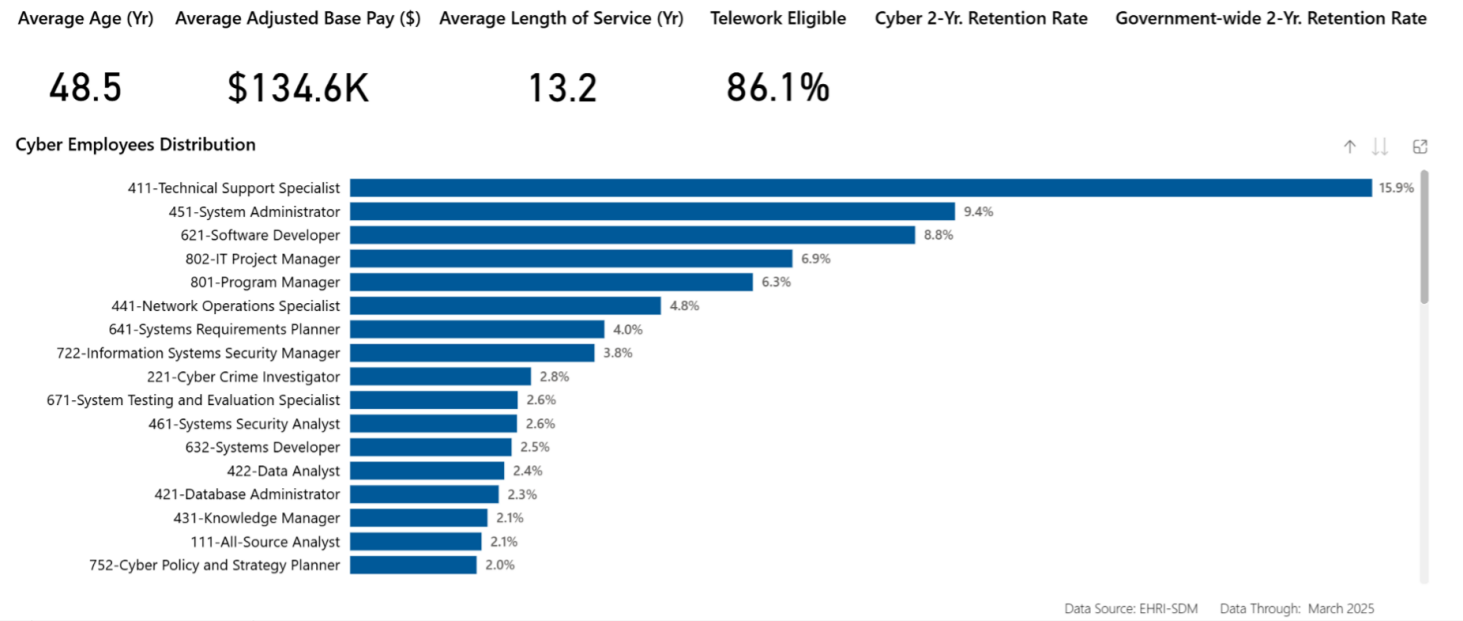
Source: SFS Master Roster and Placement Log as of October 1, 2025.

Enrolled Year	Scholarships Awarded	Full Waiver: Academic Phase	Full Waiver: Employment Phase	Partial Waiver: Employment Phase	Waiver Request Pending Decision	Waiver Totals
2001	31	0	6	0	0	6
2002	115	0	16	2	0	18
2003	219	0	16	1	0	17
2004	185	0	3	0	0	3
2005	183	0	2	4	0	6
2006	134	0	0	1	0	1
2007	111	0	0	1	0	1
2008	93	0	0	0	0	0
2009	133	1	1	3	0	5
2010	181	0	1	2	0	3
2011	196	0	1	3	0	4
2012	188	1	0	1	0	2
2013	268	1	1	0	0	2
2014	277	0	3	0	0	3
2015	277	0	1	0	0	1
2016	314	0	2	0	0	2
2017	357	0	0	2	0	2
2018	339	0	1	1	0	2
2019	384	0	2	2	1	5
2020	375	2	1	3	0	6
2021	364	0	0	0	0	0
2022	393	0	0	2	1	3
2023	488	1	0	2	0	3
2024	477	0	0	1	1	2
2025	64	0	0	0	0	0
Total	**6,146**	**6**	**57**	**31**	**3**	**97**

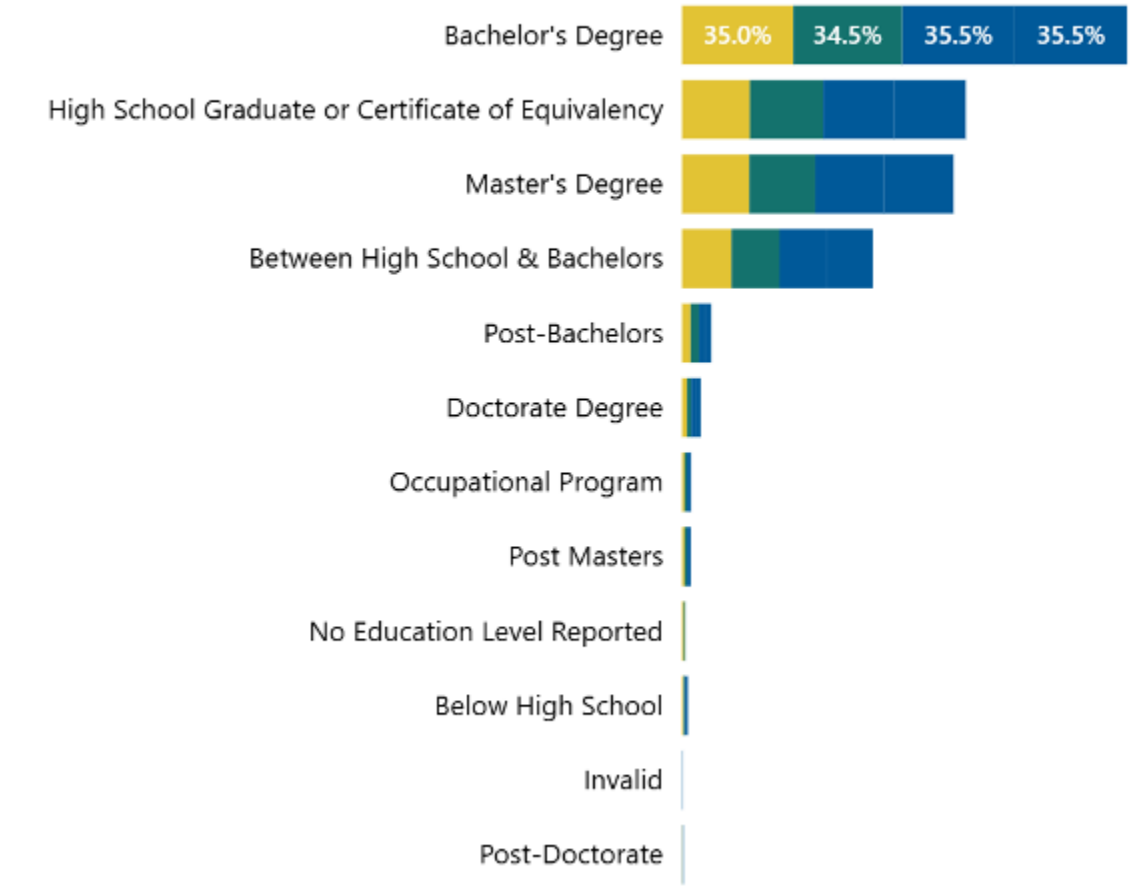
APPENDIX F: FEDERAL CYBERSECURITY WORKFORCE STATISTICS

OPM's Cyber Workforce Dashboard, https://www.opm.gov/data/data-products/cyber-workforce-dashboard/, is the source of the following data. The current data shown as of March 2025 on the dashboard was pulled as of November 2025.

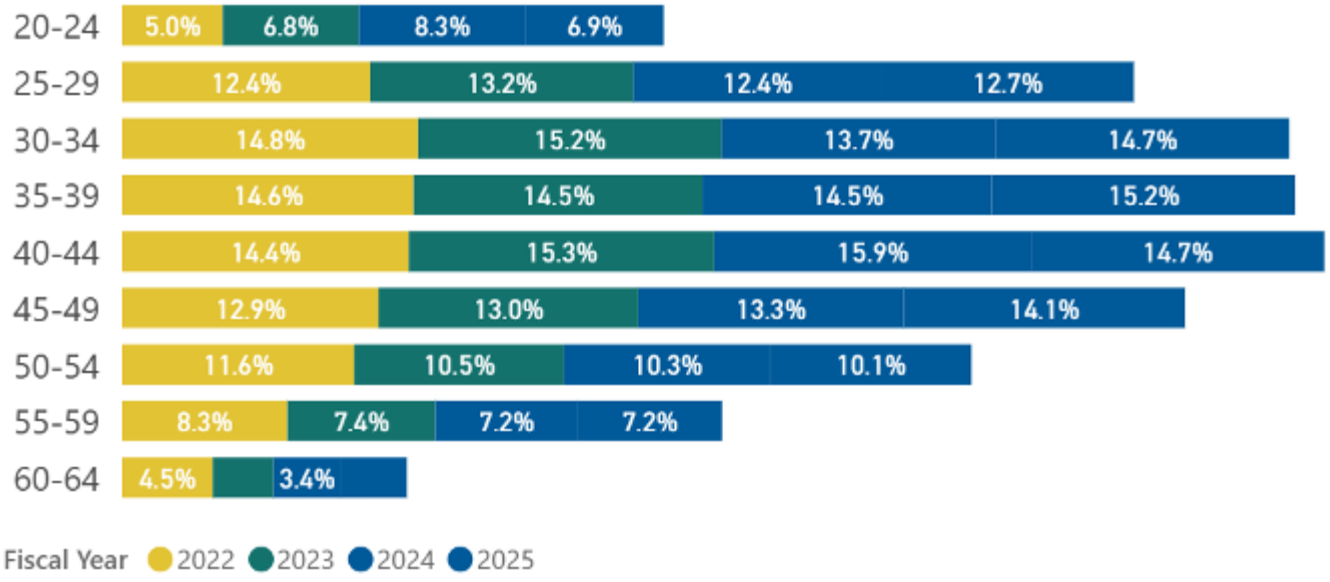
FEDERAL CYBER WORKFORCE SUMMARY

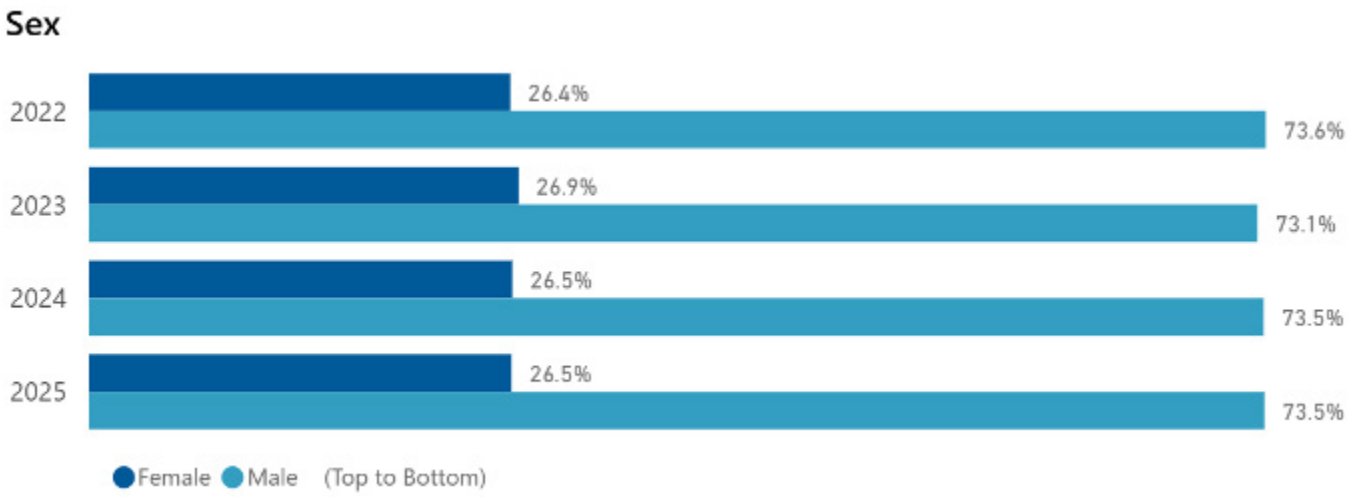


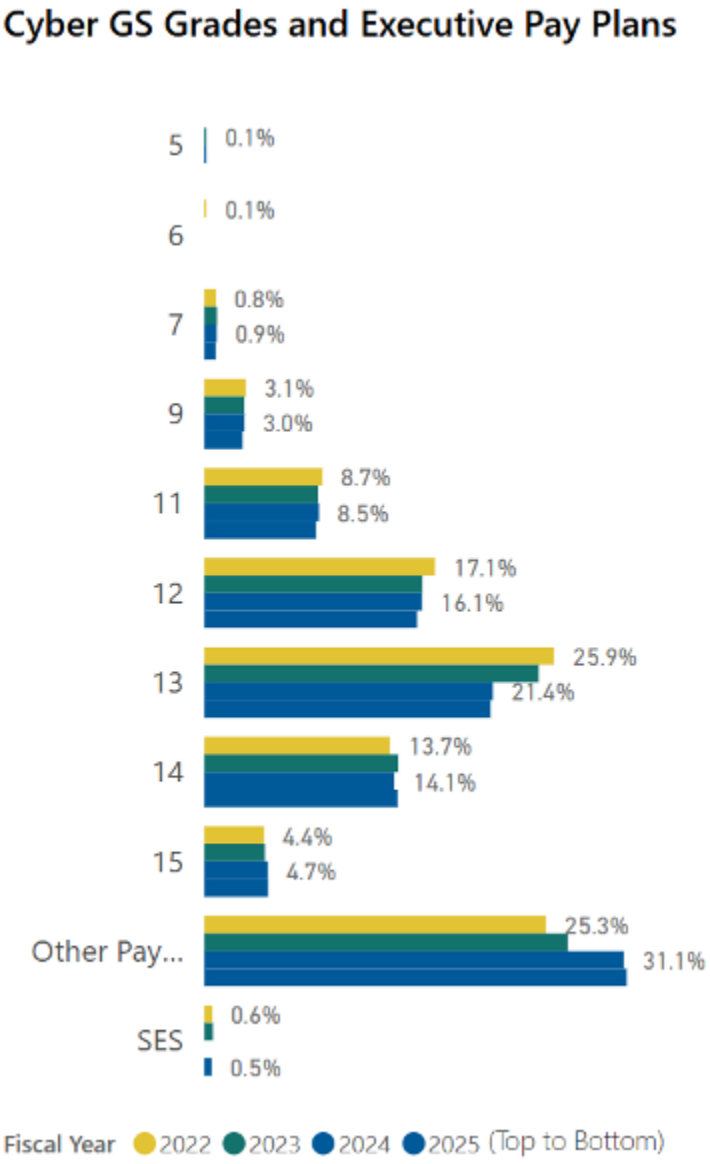
Cyber Employee Education Distribution



Age




Sex
2022
26.4%
73.6%
2023
26.9%
73.1%
2024
26.5%
73.5%
2025
26.5%
73.5%
Female
Male
(Top to Bottom)

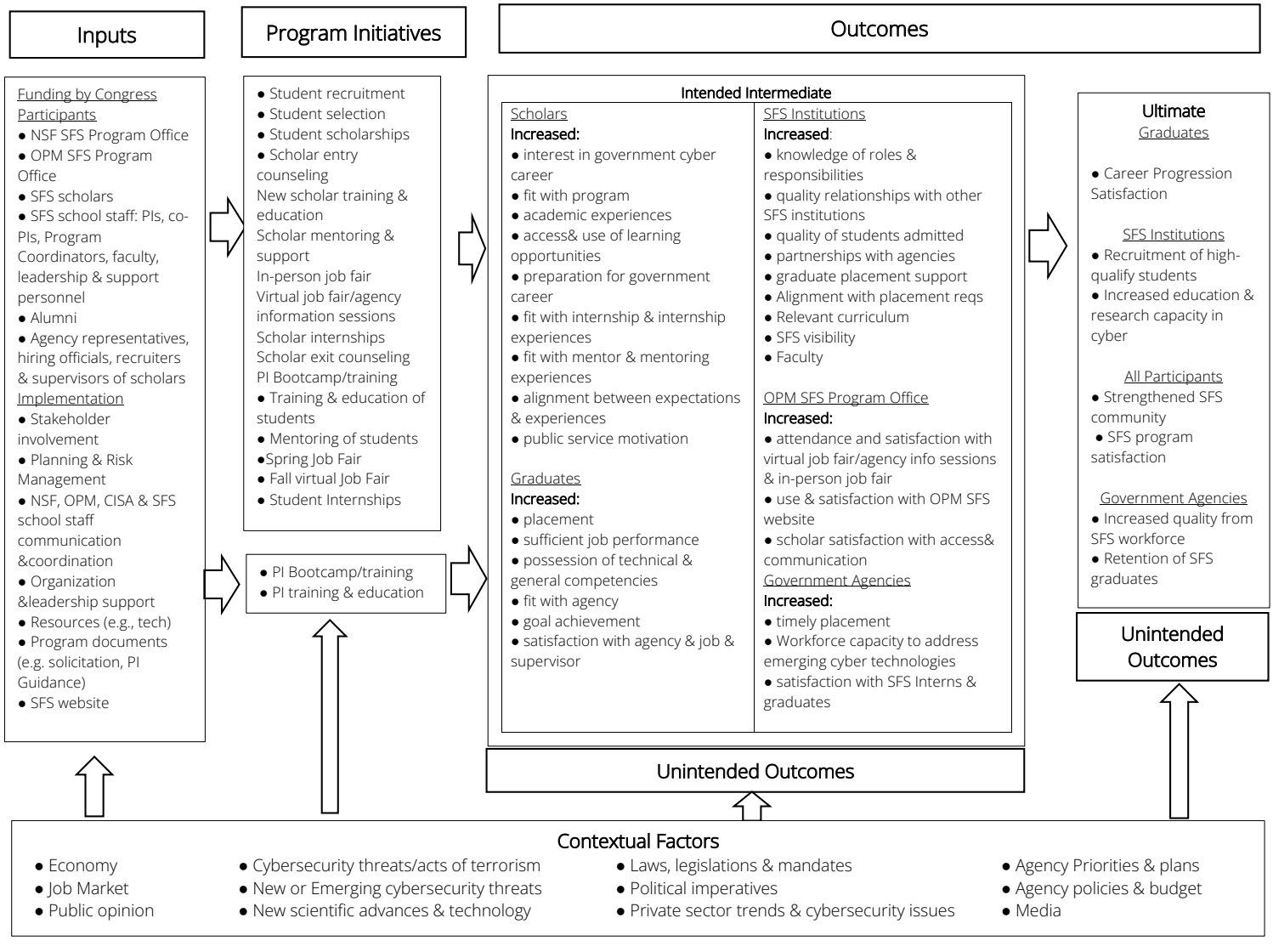

Cyber GS Grades and Executive Pay Plans
5
0.1%
6
0.1%
7
0.8%
0.9%
9
3.1%
3.0%
11
8.7%
8.5%
12
17.1%
16.1%
13
25.9%
21.4%
14
13.7%
14.1%
15
4.4%
4.7%
Other Pay...
25.3%
31.1%
SES
0.6%
0.5%
Fiscal Year
2022
2023
2024
2025
(Top to Bottom)

APPENDIX G: LIST OF SFS SCHOOLS (ACTIVE AS OF 2025)

Alabama (6)	Auburn University Tuskegee University University of Alabama - Tuscaloosa University of Alabama at Birmingham University of Alabama, Huntsville University of South Alabama
Arizona (2)	Arizona State University University of Arizona
Arkansas (1)	University of Arkansas
California (3)	California State Polytechnic University, Pomona California State University - San Bernardino CSU – Sacramento
Colorado (1)	University of Colorado at Colorado Springs
Connecticut (1)	University of New Haven
Delaware (1)	University of Delaware
DC (2)	George Washington University Georgetown University
Florida (7)	Embry-Riddle Aeronautical University Florida Atlantic University Florida State University University of Central Florida University of Florida University of South Florida University of West Florida
Georgia (3)	Augusta University Georgia Institute of Technology Georgia State University
Hawaii (1)	University of Hawaii
Idaho (3)	Boise State University Idaho State University University of Idaho
Illinois (2)	Loyola University of Chicago University of Illinois at Urbana Champaign
Indiana (2)	Indiana University Purdue University
Iowa (1)	Iowa State University
Kansas (3)	Kansas State University University of Kansas Wichita State University
Kentucky (1)	University of Louisville
Louisiana (2)	Louisiana State University Louisiana Tech University
Maryland (6)	Bowie State University Johns Hopkins University Morgan State University Towson University University of Maryland - Baltimore County University of Maryland - College Park
Massachusetts (4)	Northeastern University University of Massachusetts, Amherst University of Massachusetts, Dartmouth Worcester Polytechnic Institute
Michigan (2)	Michigan Technological University Oakland University
Mississippi (1)	Mississippi State University
Missouri (2)	Missouri University of Science and Technology University of Missouri-Columbia
Nevada (2)	University of Nevada, Las Vegas University of Nevada, Reno
New Jersey (1)	New Jersey Institute of Technology
New Mexico (2)	New Mexico Institute of Mining and Technology University of New Mexico
New York (6)	Binghamton University Fordham University New York University Pace University Rochester Institute of Technology University at Buffalo
North Carolina (3)	North Carolina A & T State University North Carolina State University University of North Carolina at Charlotte
Ohio (2)	Ohio State University University of Cincinnati
Oklahoma (1)	University of Tulsa
Oregon (1)	Oregon State University
Pennsylvania (3)	Carnegie Mellon University Pennsylvania State University Robert Morris University
Puerto Rico (1)	Polytechnic University of Puerto Rico
Rhode Island (1)	University of Rhode Island
South Carolina (1)	The Citadel
South Dakota (1)	Dakota State University
Tennessee (3)	Tennessee Tech University University of Memphis University of Tennessee Chattanooga
Texas (5)	Sam Houston State University Texas A&M University University of Texas at Dallas University of Texas at El Paso University of Texas, San Antonio
Utah (1)	Brigham Young University
Vermont (1)	Norwich University
Virginia (6)	George Mason University Hampton University Marymount University Norfolk State University Old Dominion University Virginia Polytechnic Institute & State University
Washington (2)	University of Washington, Tacoma Washington State University
Wisconsin (1)	Marquette University

APPENDIX H: SFS EVALUATION LOGIC MODEL

U.S. National Science Foundation CyberCorps® Scholarship for Service Program Logic Model



APPENDIX I: LIST OF SATC-EDU AWARDS (FY 2024 – 2025)

Title	Year Funded	Institution Name	State	Award Amount	Award Page
Collaborative Research: SaTC: EDU: Enhancing IoT Software and System Security Education with Student-centered Pedagogy and Next Generation Capture-the-Flag Platform	2024	North Carolina Agricultural & Technical State University	NC	$50,000	2329705
Education DCL: EAGER: Teaching Privacy via Stakeholder Modeling	2024	Brown University	RI	$300,000	2335625
Education DCL: EAGER: An Embedded Case Study Approach for Broadening Students' Mindset for Ethical and Responsible Cybersecurity	2024	George Mason University	VA	$299,486	2335636
SaTC: EDU: AI for Cybersecurity Education via an LLM-enabled Security Knowledge Graph	2024	Arizona State University	AZ	$499,999	2335666
SaTC: EDU: Investigating the Role of Storytelling Visualization in Privacy Education	2024	Arizona State University	AZ	$500,000	2350036
SaTC: EDU: Learning Threat Perception through Build-Break-Fix Assignments	2024	University of Wisconsin-Madison	WI	$499,828	2350165
Excellence in Research: Establishing a Research Framework to Foster Digital Capital Among Adolescents for Safe and Secure Online Habitus	2024	Norfolk State University	VA	$516,302	2401831
SaTC: EDU: Collaborative: An Assessment Driven Approach to Self-Directed Learning in Secure Programming (SecTutor)	2024	Worcester Polytechnic Institute	MA	$109,772	2403603
Collaborative Research: SaTC: EDU: A Socially-Distant Cloud-Based Hardware Security Educational Platform	2024	University of Texas at Dallas	TX	$186,000	2413048
Collaborative Research: SaTC: EDU: A Socially-Distant Cloud-Based Hardware Security Educational Platform	2024	North Carolina State University	NC	$213,100	2413049
Collaborative Research: SaTC: EDU: Education on Securing AI System under Adversarial Machine Learning Attacks	2024	Temple University	PA	$146,000	2414365
Collaborative Research: SaTC: EDU: Education on Securing AI System under Adversarial Machine Learning Attacks	2024	New Jersey Institute of Technology	NJ	$127,000	2414366
Collaborative Research: SaTC: EDU: Education on Securing AI System under Adversarial Machine Learning Attacks	2024	Rutgers University New Brunswick	NJ	$127,000	2414367
Collaborative Research: SaTC: EDU: A Lab-based Curriculum for Watermarking AI-Generated Content: Theory, Algorithms and Robustness Testing	2024	Duke University	NC	$210,000	2414406
Collaborative Research: SaTC: EDU: A Lab-based Curriculum for Watermarking AI-Generated Content: Theory, Algorithms and Robustness Testing	2024	Pennsylvania State Univ University Park	PA	$190,000	2414407
SaTC: EDU: Designing Next Generation Training Using VR for Microelectronics Physical Assurance (VR MiPA)	2024	University of Florida	FL	$497,905	2415749
Authentic Learning Modules for DevOps Security Education	2024	University of West Florida	FL	$125,880	2421324
SaTC: EDU: Augmenting Cybersecurity Education in Mobile Health (mHealth) Through Curriculum and Experimental Platform Development	2024	Yeshiva University	NY	$399,999	2428595
Education DCL: EAGER: Developing Sector-specific Cybersecurity Training Programs: What are the Benefits to Students and Employers?	2024	Research Foundation of the City University of New York	NY	$204,171	2447489
Collaborative Research: SaTC: EDU: Dual-track Role-based Learning for Cybersecurity Analysts and Engineers for Effective Defense Operation with Data Analytics	2024	Gonzaga University	WA	$367,447	2502341
Collaborative Research: SaTC-EDU: Integrating Cybersecurity in Computing Curricula: A Software PBL-Driven Approach with Focus on Identity and Access Management (IAM)	2024	Rochester Institute of Tech	NY	$398,370	2513110
Collaborative Research: SaTC: EDU: Enhancing IoT Software and System Security Education with Student-centered Pedagogy and Next Generation Capture-the-Flag Platform	2024	Northeastern University	MA	$450,000	2523436
Collaborative Research: SaTC: EDU: Fire and ICE: Raising Security Awareness through Experiential Learning Activities for Building Trustworthy Deep Learning-based Applications	2025	Miami University	OH	$220,000	2512870
Collaborative Research: SaTC: EDU: A Socially-Distant Cloud-Based Hardware Security Educational Platform	2025	Rensselaer Polytechnic Institute	NY	$186,000	2537759

APPENDIX J: LIST OF CYBERCORPS® FUNDED INSTITUTIONS WITH AI PROGRAMS

The CyberCorps®: Scholarship for Service (SFS) program, funded by the National Science Foundation (NSF), supports students pursuing cybersecurity-related degrees, including those with a focus on AI. Many participating institutions offer interdisciplinary programs that integrate AI into cybersecurity education.

Active and recently made awards are for the following institutions:

Award #	Institution
2438185	University of Maryland Baltimore County
2438580	Dakota State University
2438810	University of Pennsylvania University Park
2438885	Carnegie Mellon University
2439007	University of Hawaii
2336516	George Washington University
2336252	Rochester Institute of Tech
2336490	Washington State University
2336109	University of Arizona
2336545	Boise State University
2336456	Florida Atlantic University
2336444	Norwich University
2336539	University of Nevada Las Vegas
2234911	Tuskegee University
2234910	University of Tennessee Chattanooga
2234868	University of Alabama at Birmingham
2146280	Oakland University
2142229	Fordham University
2146278	Marymount University
2043210	University of North Carolina at Charlotte
2146254	Johns Hopkins University
2146497	Georgia State University
2146466	University of Texas at San Antonio
1922398	University of Texas at Dallas

GLOSSARY

CyberCorps® SFS Scholarship Recipient (scholarship recipient): A student who is selected by an SFS institution for CyberCorps® SFS scholarship and agrees to work after graduation for a federal, state, local, or tribal government organization in a position related to cybersecurity.

DHS: Department of Homeland Security

Deferral: An approved extension of the obligation phase.

Monitoring Phase: A period following the completion of the Obligation Phase during which the recipient must maintain current contact information and complete periodic (usually annual) data collections as requested by the SFS Program Office.

Obligation Phase: A period following the completion, or otherwise cessation of the Scholarship Phase within which the SFS recipient must complete their obligation requirement.

OPM CyberCorps® SFS Program Management Office: This refers specifically to the OPM program management office.

PI: Principal investigator, the individual(s) designated by the proposer and approved by NSF, who will be responsible for the scientific or technical direction of the project.

SaTC: The NSF Secure and Trustworthy Cyberspace (SaTC) program.

SaTC-EDU: The NSF SaTC program features an education designation, called SaTC-EDU.

Scholarship Phase: A period when scholarship recipients are enrolled in an approved SFS academic program in cybersecurity.

SFS: Scholarship for Service, in this document this term refers to the CyberCorps® Scholarship for Service program.

SFS Institution: A higher education institution that receives a CyberCorps® Scholarship for Service grant from the U.S. National Science Foundation to recruit, train and graduate CyberCorps® Scholarship Recipients.

SFS Program Office: An office managing the CyberCorps® SFS program through partnership between the U.S. National Science Foundation (NSF) and the U.S. Office of Personnel Management (OPM).

Solicitation: The term "program solicitation" refers to formal NSF publications that encourage the submission of proposals in specific program areas of interest to NSF.