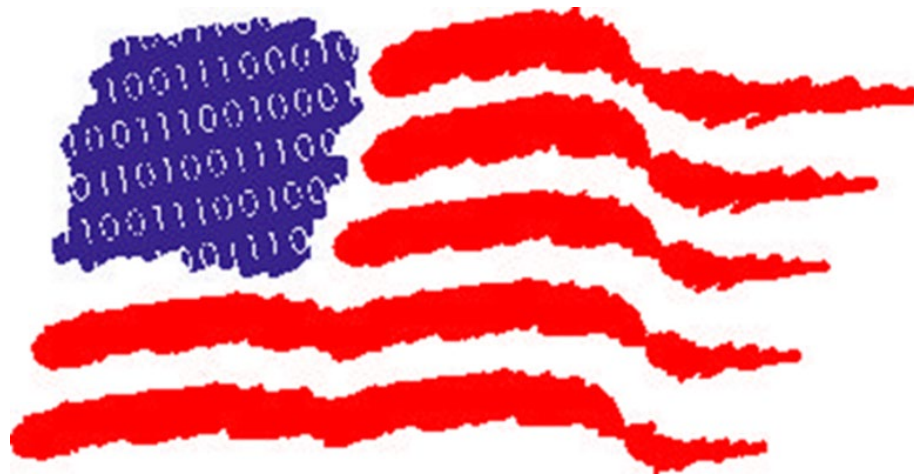


# 2021 BIENNIAL REPORT

CYBERCORPS®: SCHOLARSHIP FOR SERVICE (SFS)



Defending  
America's Cyberspace



Request this document in an accessible format by visiting [nsf.gov/accessibility](https://www.nsf.gov/accessibility)

January 2022

National Science Foundation

## TABLE OF CONTENTS

Letter From Dr. Sylvia Butterfield, Acting Assistant Director, Directorate for Education and Human Resources .....	1
CyberCorps® Program Overview.....	3
Scholarships .....	5
Program Management.....	7
Facilitating Government Hiring.....	11
CyberCorps® Program Monitoring and Evaluation.....	12
Public Information .....	13
A. Post Graduate Placement Rates .....	14
B. Post Graduate Placement by Agency.....	14
C. Salary Ranges 2018-2021 .....	14
D. Average Time from Graduation to Employment .....	14
E. Time Employed by the First Organization After Graduation.....	14
F. Students Released from Obligation .....	16
G. Competency Gap Analysis of Recent SFS Graduates.....	17
H. Disparity in Reporting (2018 – 2021).....	20
I. Federal Cybersecurity Workforce Statistics .....	20
Increasing National Capacity in Cybersecurity Education.....	20
Special Initiative: Cybersecurity Education in the Age of Artificial Intelligence .....	22
K-12 initiatives.....	22
GenCyber - Inspiring the Next Generation of Cyber Stars .....	23
JROTC Cyber Academies.....	25
Advanced placement Computer Science Principles: Cybersecurity .....	27
Community College Initiatives .....	28
Increasing Diversity and Inclusion in the Cybersecurity Workforce.....	30
Women in Cybersecurity.....	32
CyberCorps® SFS Hall of Fame .....	33
Future of the CyberCorps® SFS Program .....	36
Appendix A: Post Graduate Placement Rate by Enrolled Year .....	37
Appendix B: Post Graduate Placement by Agency .....	38
Appendix C: Job Titles .....	41
Appendix D: Sample Job Descriptions.....	51
Appendix E: Students Released from Obligations .....	70
Appendix F: Federal Cybersecurity Workforce Statistics .....	71

Appendix G: List of SFS Schools (ACTIVE AS OF 2021) .....	73
Appendix H: SFS Evaluation Logic Model .....	78
Appendix I: Women in Cybersecurity (WiCyS).....	79
Appendix J: List of SaTC-EDU awards (FY 2018 – 2021).....	80
Appendix K: Cybersecurity Education in the Age of Artificial Intelligence .....	85
Glossary.....	89

LETTER FROM DR. SYLVIA BUTTERFIELD, ACTING ASSISTANT DIRECTOR,  
DIRECTORATE FOR EDUCATION AND HUMAN RESOURCES

Cyberspace has transformed the daily lives of people. Emerging technologies such as high-speed wireless networking and artificial intelligence, promise that cyberspace will continue to offer us exceptional benefits including living environments that promise to be smart and connected communities. However, the more we rely on cyberspace, the greater the potential damage that adversaries can create through ransomware, disruption of essential services and infrastructure, breaches of personal privacy, and other malicious cyber activities. There is also a growing gap in the supply and demand for cybersecurity workers in the United States.

The CyberCorps® Scholarship for Service (SFS) program is a successful and long-running interagency partnership between the National Science Foundation (NSF), the Office of Personnel Management (OPM), and the Department of Homeland Security (DHS). Since the first cohort of 31 students in 2001, the CyberCorps® program has grown to 1,076 students on active scholarships in 2021 and has graduated 3,842 students who have gone on to play critical roles defending our nation's cyberspace by working at federal, state, tribal, and local government organizations.

The CyberCorps® program also supports efforts leading to an increase in the ability of the U.S. higher education enterprise to produce cybersecurity professionals. The complex interactions between the human, social, organizational, economic, and technological factors require more than technical skills alone; they require the ability to engage with all sectors of society and it requires a diverse and inclusive cybersecurity workforce.

Special initiatives supported through CyberCorps® extend the reach beyond the core CyberCorps® SFS program to reach students beginning in K-12 and to support innovation at the frontiers of cybersecurity education, including artificial intelligence and quantum information science. These range from the NSF-wide Secure and Trustworthy Cyberspace program, which includes an education designation (SaTC-EDU) that focuses on fundamental and applied research enabling new approaches, to cybersecurity education and workforce development from the K-12 up to the professional education levels. GenCyber, which hosts camps for K-12 students and teachers, has reached more than 15,000 students across the U.S. since it started in 2014. A new pilot initiative, that involves partnerships with private industry targets students enrolled in Junior Reserve Officers' Training Corps (JROTC) programs. Initiatives also focus on developing and leveraging capacity at community colleges.

I want to congratulate the innovation and tenacity that has been demonstrated by the CyberCorps® students and institutions in the face of the challenges posed by the ongoing pandemic and to thank them for their commitment to protect U.S. cyberspace. I am pleased to introduce this 2021 Biennial CyberCorps® SFS report of the program's accomplishments.

## CYBERCORPS® PROGRAM OVERVIEW

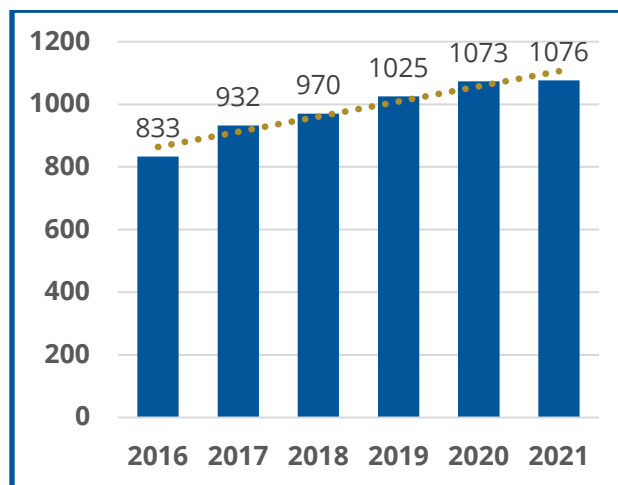
Cybersecurity is arguably one of the most important challenges confronting society in the information age. Addressing this challenge requires an innovative cybersecurity education system that will create an unrivaled cybersecurity workforce critical to US national security, continued economic growth, and future technological innovation in secure cyberspace.

The National Science Foundation (NSF) CyberCorps® Scholarship for Service (SFS) program was established as a result of Presidential Directive 63, dated May 22, 1998. The subsequent National Plan for Information Systems Protection, issued January 8, 2000, was the first attempt by any national government to design a way to protect its cyberspace. The Cybersecurity Enhancement Act of 2014, as amended by the National Defense Authorization Acts for 2018 and 2021, authorized NSF, in coordination with the U.S. Office of Personnel Management (OPM) and the U.S. Department of Homeland Security (DHS), to continue the CyberCorps® scholarship program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for Federal, State, local, and tribal governments.

Until 2017 the CyberCorps® program included two tracks. First is a Scholarship

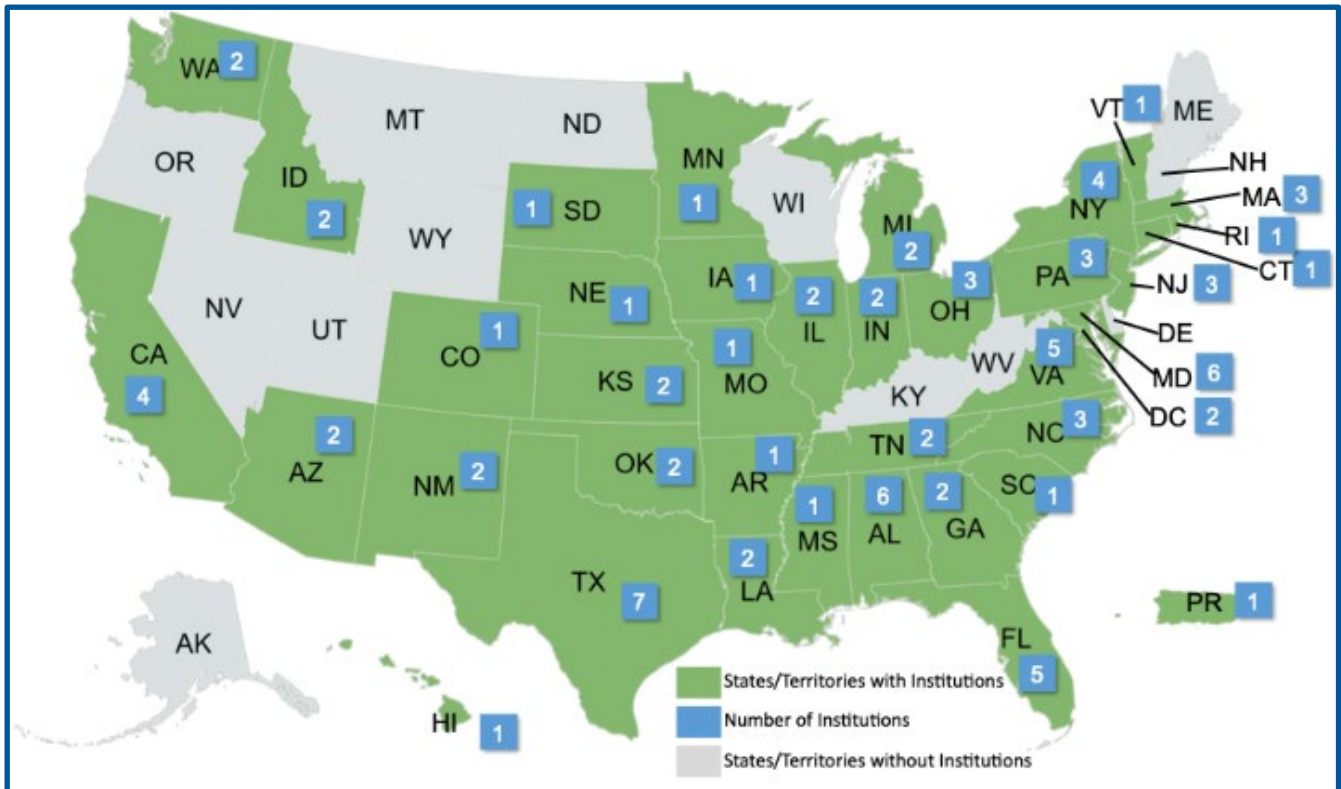
Track providing funding to universities to award scholarships for up to three years to students in undergraduate or graduate degree programs in the area of cybersecurity. All scholarship recipients must work after graduation in an approved organization in a position related to cybersecurity for a period equal to the duration of the scholarship. Second is a Capacity Building Track providing funding to increase the ability of the United States higher education enterprise to produce cybersecurity professionals. In 2018, this track was merged with the Education Designation (EDU) of the cross-agency Secure and Trustworthy Cyberspace (SaTC) program.

### CYBERCORPS® SFS STUDENT ENROLLMENT



The first cohort of 31 CyberCorps® students was enrolled in Fall 2001 and the first nine students graduated the following year. As of December 2021, 3,842 CyberCorps® students have graduated from the program and a total of 4,773 students have been enrolled in the program since its inception. There are 83 institutions of higher education with active

**CYBERCORPS® SFS PARTICIPATING INSTITUTIONS (2021)**



CyberCorps® SFS projects. In addition, there are 28 community colleges that participate as a partner with a CyberCorps® university, and eight community colleges in the CyberCorps® Community College Cyber Pilot (C3P) program (See Appendix G for the complete list).

The goals of the CyberCorps® SFS program are aligned with the 2018 National Cyber Strategy to develop a superior cybersecurity workforce for government organizations. In addition, NSF contributes to the multi-agency efforts convened by the National Initiative for Cybersecurity Education (NICE).

The program’s short-term goal, as defined in the National Defense Authorization Act (NDAA) 2021, is full student placement in

government cybersecurity positions with at least 70% of scholarship recipients securing placement in the executive branch of the Federal government, up to 20% of scholarship recipients securing placement in state, local, and tribal government organizations or Federally-Funded Research and Development Centers (FFRDCs), and up to 10% securing placement as educators at other CyberCorps® SFS institutions.

The long-term goals of the program are to:

- 1) Increase the number of qualified and diverse 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® graduates in Federal Government employment; and
- 4) Strengthen partnerships between institutions of higher education and Federal, state, local, and tribal governments.

Finally, NSF recognizes that cybersecurity education and workforce development are critical elements for a successful implementation and transition to practice of any advances in cybersecurity research and development as outlined in the 2019 Federal Cybersecurity Research and Development Strategic Plan.

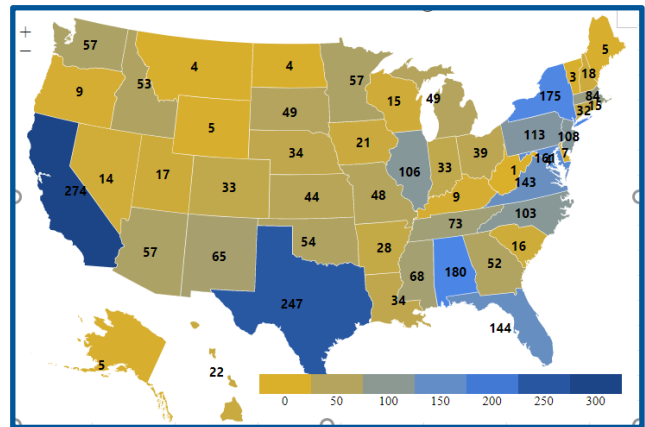
### SCHOLARSHIPS

The CyberCorps® SFS program provides funds to institutions of higher education to award student scholarships in cybersecurity. Each scholarship recipient agrees to work for a period equal to the duration of the scholarship to support the cybersecurity mission of an approved government organization.

To be eligible for consideration for a CyberCorps® SFS scholarship, a student must be a citizen or lawful permanent resident of the United States; and be a full-time student in a coherent formal program that is focused on cybersecurity. Students may range from a sophomore in an associate’s degree program

to one in a research-based doctoral program. CyberCorps® SFS students are enrolled in over 60 different areas of study and the most popular major is Computer Science. The most common degree is a Master’s (53%), followed by a Bachelor’s (39%), Ph.D. (4%), and Associate’s (4%). Overall, CyberCorps® SFS graduates hold high GPAs, with 74% graduating with a GPA of 3.6 or higher.

### CYBERCORPS® STUDENT HOME STATE (BY HIGH SCHOOL ATTENDANCE)



Grantee institutions provide scholarship support to students who are selected in a competitive processes developed by the institution. Internship placements and final job placements in government organizations typically require high-level security clearances, and scholarship recipients are required to undergo the background investigation necessary to obtain such clearances as part of the job and/or internship application process.

The CyberCorps® scholarships provide up to three years of stipends, tuition, and professional development allowances for students in the general area of cybersecurity.



During the scholarship period, students must participate in meaningful summer internships and other CyberCorps® activities such as conferences, workshops, and seminars.

**CYBERCORPS® STUDENT TOP PLACEMENTS  
(2001-2021)<sup>1</sup>**

Post-Graduation Organization	Students
National Security Agency	673
Department of Navy	341
Department of Energy	334
State/Local/Tribal Government	231
Department of the Army	188
Department of Homeland Security	147
Department of Air Force	112
Federal Reserve	101
Department of Justice	100
Applied Physics Laboratory	95
Department of Defense	85
Central Intelligence Agency	71

A CyberCorps® SFS scholarship recipient is financially liable to the United States if the individual fails to maintain an acceptable level of academic standing or fails to fulfill the post-award employment obligation. Such circumstances would result in forfeiture of the scholarship award, which must either be repaid or converted to a student loan.

The CyberCorps® scholarship recipients are responsible for their own job searches in the Executive Branch of the US Federal government. With permission from the SFS

Program Office, a limited number of students, but no more than 20 percent of scholarship recipients, may be placed in a non-executive federal agency; state, local or tribal government organization; National Laboratories; or Federally Funded Research and Development Centers (FFRDCs).

**TOP UNIVERSITIES BY AVERAGE ANNUAL  
COHORT SIZE (2016-2021)**

CyberCorps® SFS Institution	Average Cohort
Dakota State University	40.8
University of Tulsa	32.4
Florida State University	30.4
CSU - San Bernardino	26.4
Naval Postgraduate School	24.8
University of Alabama, Huntsville	24.4
Carnegie Mellon University	23.8
Northeastern University	22.8
University of South Alabama	20.2
University of Texas at Dallas	19.8
Mississippi State University	19.4
University of Illinois (UIUC)	19.2
Rochester Institute of Technology	18.0
Towson University	17.2
University of Texas, San Antonio	17.0

Also, a limited number of students, but no more than 10 percent of scholarship recipients, may be placed as educators in the field of cybersecurity at qualified institutions of higher education that provide CyberCorps® SFS scholarships.

---

<sup>1</sup> Data as of September 21, 2021.

## PROGRAM MANAGEMENT

As specified in the Cybersecurity Enhancement Act of 2014 (15 U.S. Code § 7442), the CyberCorps® SFS program is led and managed by NSF in coordination with the Office of Personnel Management (OPM) and the Department of Homeland Security (DHS). The three agencies have frequent consultations and participate in monthly CyberCorps® SFS Management Board meetings.

### **National Science Foundation**

The NSF CyberCorps® SFS Program Office oversees all aspects of the program, including:

- Program solicitations, merit review process, site visits, grant awards, assessing progress via annual and final reports, managing financial functions, representing the program in interactions with federal agencies and other organizations within the academic/scientific communities;
- Outreach to current and prospective CyberCorps® SFS grantee institutions and principal investigators (PIs);
- Coordination with OPM via an annual reimbursable Inter-Agency Agreement (IAA) for student management;
- Coordination with DHS on connecting students with government agencies via CyberCorps® SFS Job Fairs;
- Implementing contracts for independent continuous program monitoring and program-level evaluation;

- Coordination with the U.S. Treasury and/or Department of Education on collections and repayments for the small number of students who do not fulfill their service obligations; and
- Processing requests for partial or complete releases from the service obligation under appropriate circumstances.

### **Office of Personnel Management**

The OPM CyberCorps® SFS Program Management Office is supported by a reimbursable Interagency Agreement with NSF and manages the operational aspects of CyberCorps® student scholarships including:

- Creating and distributing Student Service Agreements, policy, guidance and other program documents;
- Tracking CyberCorps® SFS students from entry into the program until eight years following the completion of their post-graduation service obligation;
- Facilitating the registration of new CyberCorps® SFS students and monitoring their academic status with participating institutions during the scholarship phase;
- Reviewing and approving student job offers and monitoring the service obligations reported by students;
- Coordinating collection of information for repayments and waiver requests to NSF; and

- Maintaining the CyberCorps® SFS program website (<https://sfs.opm.gov/>) that allows students to access CyberCorps® SFS program information and post their resumes online, so they become available to registered and approved organizations.

### **Department of Homeland Security**

DHS serves as a strategic partner to promote cybersecurity education and workforce development; helps strengthen partnerships between CyberCorps® SFS institutions and Federal, State, local, and tribal governments; serves as a technical advisor; sponsors annual CyberCorps® SFS Job Fairs; and organizes and maintains the CyberCorps® SFS Hall of Fame site. In addition, DHS partners with the National Security Agency on the National Centers of Academic Excellence in Cybersecurity (NCAE) initiative to:

- Establish standards for cybersecurity curricula and academic excellence;
- Include competency development among students and faculty;
- Value community outreach and leadership in professional development;
- Integrate cybersecurity practice within the institution across academic disciplines; and

- Actively engage in solutions to challenges facing cybersecurity education.

### **NSF Merit Review Process**

NSF is a proposal-driven funding agency supporting cutting-edge research and development in STEM and STEM education. Preserving the integrity of NSF’s anonymous peer review process, to ensure that the highest quality proposals are identified for funding, is essential to the success of NSF’s work. NSF’s Merit Review Process is considered the gold standard among funding entities, both public and private. As one of NSF’s many funding programs CyberCorps® uses this process. NSF program officers recruit experts to form review panels whose purpose is to identify and analyze the strengths and weaknesses of all proposals using NSF’s two merit review criteria, Intellectual Merit and Broader Impacts, which have been approved by the National Science Board<sup>2</sup>. In addition to these two review criteria, individual programs at NSF may include additional review criteria to evaluate the quality of submitted proposals. Additional review criteria, specific to CyberCorps® SFS, include:

- A project plan and objective metrics designed to evaluate the success of the proposed project;

---

<sup>2</sup> [https://www.nsf.gov/bfa/dias/policy/merit\\_review/](https://www.nsf.gov/bfa/dias/policy/merit_review/)

- The quality of education and research in cybersecurity at the institution and the extent to which they are integrated. The quality of applied experiences to increase students' understanding of cybersecurity;
- The extent to which cybersecurity faculty members are integrally involved with the scholarship students and working with the students as a cohort;
- Opportunities for undergraduate research experiences; and
- Broadening participation efforts at the institution as well as specific plans for recruitment, mentoring, and retention of CyberCorps® SFS scholars who are members of populations that are underrepresented in their participation in the cybersecurity field, such as racial and ethnic minority groups, women, first-generation/low-income students, persons with disabilities, or veterans.

Individual members of the review panel provide written reviews of each proposal. The whole panel then convenes in a meeting where the individual reviews are deliberated. For each proposal being considered, the panel then provides individual reviews and a panel summary including a recommendation on the suitability of funding to the CyberCorps® SFS program officers. The reviews and panel summary are made available to the submitting organization.

Following the conclusion of the panel review process the NSF CyberCorps® SFS program officers consider appropriate scientific,

programmatic, and technical considerations pertaining to the proposals. The program officers also engage in a portfolio analysis exercise that considers the current set of existing awards and then looks at how well the strongest proposals identified during the merit review process fit into, complement, or otherwise potentially extend the impact of the program's investments.



In addition to the merit review process described above, the CyberCorps® SFS program officers engage with a short list of competitive institutions in the form of a pre-award site visit to gain additional information about the project and institutional environment. The visits normally include meetings with senior leadership at the institution (e.g., President, Provost and the Deans of involved schools or other units at the institution); meetings with the Department chairs; a presentation by the project team; meetings with students; tours of research labs; meetings with the Financial Aid office; and meetings with the Sponsored Research Office. Information obtained during the site

visit is considered by the program officers as key elements of the merit review.

Based on all these considerations, the program officers present a funding recommendation to Division leadership.

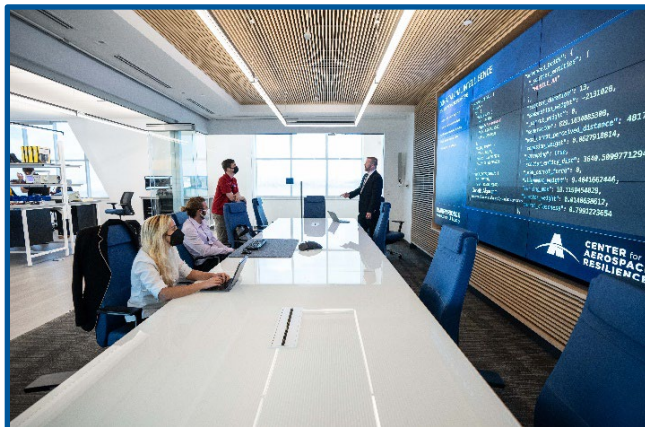
### **CyberCorps® SFS New PI Boot Camp**

New PIs attend a one-day PI boot camp as part of their first year as an CyberCorps® SFS institution. Several experienced CyberCorps® faculty and students make presentations about their respective programs and share their experiences. The purpose of the boot camp is to provide new PIs an overview of the CyberCorps® SFS program, what to expect as a new CyberCorps® SFS institution, and to discuss lessons learned and best practices from the successful projects. In addition, members of the CyberCorps® SFS program staff from NSF, OPM, and DHS provide an overview of program requirements and new developments.

### **Student Boot Camp and Seminars**

Beginning in 2016, an annual two-day CyberCorps® SFS New Scholar Bootcamp has been conducted for about 40 students each summer at Tennessee Tech University. This boot camp experience provides new recipients of the SFS scholarship both the knowledge and skills to become successful CyberCorps® SFS Scholars, including program expectations, federal resume writing, and security clearances. In Fall 2021, due to the impact of COVID-19 and with the intention to

expand this opportunity to more incoming CyberCorps® students, the boot camp was transitioned to the SFS New Scholar Seminar Series. This 14-week online course is now available to all new SFS scholars. The series is designed to help students become successful in the CyberCorps® SFS program with



guidance from the SFS Program Office, experts from around the country, distinguished speakers from government and national labs speaking to the importance and impact of the CyberCorps® SFS program and public service, and activities allowing interactions and relationship building with the CyberCorps® peers and mentors. The students also have in-person “meet-and-greet” opportunities at the annual Winter CyberCorps® SFS Job Fair. The series includes such topics as:

- Requirements, benefits, expectations, and obligations of a CyberCorps® SFS Scholar;
- Q&A with CyberCorps® SFS alums and current scholars;
- Ethics and etiquette in research: Authorship, plagiarism, copyrights, use of human subjects, etc.;



- Technical writing skills: Tips and tricks in effective writing of technical articles;
- Interpersonal skills: Communications and teamwork skills;
- Federal resume writing: Tips and resources;
- Clearance counselling: Do's and Don'ts;
- Job and internships hunting: Planning and execution;
- Presenting self: Face-to-face and online;
- Managing funds: Handling stipend and professional development funds wisely;
- Equitable communication and treatment: Being free from unconscious bias; and
- Staying healthy: In body and mind.

## FACILITATING GOVERNMENT HIRING

Finding cybersecurity talent can be challenging for government organizations. The CyberCorps® SFS Program helps hiring managers by providing scholarships to the finest candidates from institutions with some of the top cybersecurity programs in the country.

Congressional special hiring authorities as authorized by section 302 (e) of the Cybersecurity Enhancement Act of 2014 (P.L. 113-274) allows Federal organizations, without regard to any provision of chapter 33 of Title 5 governing appointments in the competitive service, to noncompetitively appoint SFS graduates. In addition, upon fulfillment of their service term, they may be converted noncompetitively to a term, career-conditional or career appointment. If converted to a term appointment, an agency

may later noncompetitively convert such employee to a career-conditional or career appointment before the term appointment expires.

Agencies may recruit SFS students for internships during their academic term and permanent placement after graduation. Hiring Managers and Human Resources Consultants interested in recruiting from the pool of SFS Scholars can gain access to these talented candidates by registering as an agency official at the OPM SFS Portal to browse the SFS student pool.

Closed hiring events specifically for the SFS students are held twice a year to give agencies an opportunity to interview and even hire SFS students on the spot. The Winter CyberCorps® Job Fair, sponsored jointly by NSF and DHS, is typically held at a hotel in the Washington, DC metro area over a three-day period. Students visit agency booths and interview rooms to speak with representatives about internship and hiring opportunities and to gain a better understanding of what it would be like to work at a particular agency and in government. In 2021 and 2022, the in-person events were held virtually due to the impacts of COVID-19.

The Summer Virtual Job Fair allows SFS students to visit participating agencies' virtual booths to search for possible employers. Each agency booth includes a representative for students to connect with and talk online regarding potential employment during a one-

day period. At each virtual booth, students can view current job postings and submit resumes to apply for jobs.

## CYBERCORPS® PROGRAM MONITORING AND EVALUATION

Since 2002, periodic SFS evaluations have been designed and conducted by OPM's Assessment and Evaluation Branch (AEB) of the Division for Human Resources Solutions (HRS). The most recent two-year evaluation was completed in 2020. This evaluation examined the effectiveness of the SFS program through a rigorous, multi-method approach, including multiple data sources, focus groups, annual surveys, college site visits, agency site visits, interviews, SFS Program Office data, and external data spanning multiple years. The logic model shown in Appendix H is a representation of program inputs, program initiatives, intended intermediate outcomes, ultimate outcomes, unintended outcomes, and contextual factors of the SFS program.

Program monitoring for the SFS program consists of NSF annual reports; core monitoring by OPM's SFS Program Management Office of the progress of SFS scholarship recipients; and a Quality Monitoring System (QMS), which is described below.

### **NSF Annual Reports**

All NSF projects are required to submit annual reports that document progress and findings of the project. These reports enable the SFS

program officers to monitor the progress of projects towards their specific goals. Financial tracking also enables NSF to examine if a project is spending its funds in a timely manner indicating progress. If an SFS project is not progressing as planned, NSF can defer disbursement of annual budget increments.

### **OPM Core Monitoring**

The OPM SFS Program Management Office conducts core monitoring of SFS students including registration of new students, monitoring their academic status, approving their internships and post-graduation placement, and processing annual employment verification until the end of the obligation phase. In addition, in case a student does not fulfill the obligation, necessary information is collected and/or generated to support processing waiver requests, repayment agreements, or collection by the U.S. Treasury.

### **Quality Monitoring System**

Annual surveys were initiated in 2015 as NSF's response to a recommendation included in a report on cybersecurity human capital conducted by the United States Government Accountability Office (GAO). NSF partnered with the AEB to develop and manage a program monitoring system, known as the Quality Monitoring System (QMS), which includes annual surveys to monitor program implementation, outputs and outcomes for the purposes of accountability, program

management and improvement of the SFS program.

The QMS includes monitoring and tracking scholarship recipients beginning with their entry into the SFS program until the end of their reporting requirement as required by the legal agreement that each student signs upon acceptance of the scholarship. The reporting requirements in the monitoring phase conclude 8 years after the Service Commitment end date.

Annually, six types of surveys are administered to new students, continuing students, recent graduates, graduates who recently met their service obligation, graduates past at least one year from their obligation, and SFS academic teams.

The evaluators conduct focus groups with students at the annual Winter CyberCorps® SFS Job Fair including community college (CC) students who plan to transfer to a partnering SFS university; undergraduate students; graduate students; PIs from the SFS institutions; and agency representatives involved in the recruitment and hiring of SFS interns and graduates. Focus group results supplement the survey data.

Interviews with the supervisors of graduates and interns provide an important perspective, including such factors as the job performance, fit with the organization, and special characteristics the SFS scholar brings to the job. Supervisors can also identify areas of growth for the graduate or intern as they

progress through their careers. The evaluators visit several agencies each year, shadowing and interviewing students, interns, and graduates.

## PUBLIC INFORMATION

Pursuant to the requirements of P.L. 116-283, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, is required to create, not less frequently than once every two years, this public report including information on:

- 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

View detailed information in Appendix A.

### B. POST GRADUATE PLACEMENT BY AGENCY

View the information on

- Placement in Appendix B
- Job titles in Appendix C
- Job descriptions in Appendix D

### C. SALARY RANGES 2018-2021

Degree (N)	Salary Range	Average Salary
Bachelor's Degree (207)	\$21,875 - \$124,800	\$68,754
Master's Degree (421)	\$24,552 - \$140,000	\$79,821
Doctoral Degree (30)	\$47,000 - \$150,000	\$91,019
<b>Total, All Degrees (658)</b>	<b>\$21,875 - \$150,000</b>	<b>\$76,850</b>

### D. AVERAGE TIME FROM GRADUATION TO EMPLOYMENT

SFS Scholars have 18 months from their date of graduation to begin completing the service

requirement. Deferrals of the service requirement are considered on a case-by-case basis for scholarship recipients, such as eligibility for coverage under the Family and Medical Leave Act (FMLA) or pursuing further education or professional development in cybersecurity.

### TIME FROM GRADUATION TO EMPLOYMENT<sup>3</sup>

Number of Months	Number of Students	%
0-3	1356	59%
4-6	567	25%
7-9	135	6%
10-12	85	4%
13-15	51	2%
16-18	38	2%
Over 18	67	3%

### E. TIME EMPLOYED BY THE FIRST ORGANIZATION AFTER GRADUATION

Survey data illustrating how long students stay in the *positions* they enter upon graduation are not available but survey data from the Service Obligation Completed (SOC) Survey from 2017-2020 and survey data from the 2019 Graduate Pulse Survey can be used to partially illustrate how long graduates

<sup>3</sup> Graduates from 2012 to October 2021 with a post-graduation commitment reported.

stayed with the same *employer* where they began working after graduation.

The SOC survey is given to graduates who have completed their service obligation within the last year. The SOC survey asks graduates if their current employer is the same organization where they began working upon graduation and how long they have been at their current employer. Respondents who indicated they have left the organization where they began working after graduation are asked how long they worked for that employer.

The survey questions ask about staying with the employer. They do not ask about staying in the same position. Graduates may stay at the same organization they enter upon graduation, yet change positions (i.e., job series) over time. They may also leave the organization they entered upon graduation and hold a job in the same job series elsewhere.

Below are combined SOC survey results from 2017-2020 summarizing the time employed by the organization hired upon graduation.

**TIME EMPLOYED BY THE FIRST ORGANIZATION AFTER GRADUATION FOR GRADUATES STILL AT THE ORGANIZATION AT TIME OF SURVEY (N=272)**

Time	%
Less than 1 year	0.70%
1 year	2.60%
2 years	30.70%
3 years	56.70%
4 years	9.30%

**TIME EMPLOYED BY THE FIRST ORGANIZATION AFTER GRADUATION FOR GRADUATES THAT LEFT THE ORGANIZATION AT THE TIME OF SURVEY (N=89)**

Time	%
Less than 1 year	20.20%
1 year	14.60%
2 years	43.80%
3 years	21.30%
4 years	0.00%

The 2017-2020 SOC Graduate Survey results indicate at the time the survey was administered that 75.3% (272/361) of the respondents were still with the organization they entered upon graduation and 24.7% (89/361) of the respondents had left the organization they entered upon graduation. Among those who stayed, most (56.7%)

reported being with the same agency for three years.

The 2019 Pulse Graduate Survey includes the same questions related to staying with the employer as the SOC Graduate Survey. Graduates who were between one to nine years beyond their service obligation received the 2019 Graduate Pulse Survey.

Below are 2019 Pulse Graduate Survey results summarizing the time employed by the organization hired upon graduation.

**TIME EMPLOYED BY THE FIRST ORGANIZATION AFTER GRADUATION FOR GRADUATES STILL AT THE ORGANIZATION AT THE TIME OF SURVEY (N=153)**

Time	%
Less than 1 year	0%
1 year	0%
2 years	0%
3 years	7.8%
4 years	22.2%
5 years	19.6%
6 years	11.1%
7 years	15.0%
8 years	7.8%
9 years	4.6%
10 years	7.8%
11 years	2.0%
12 years or more	2.1%

**TIME EMPLOYED BY THE FIRST ORGANIZATION AFTER GRADUATION FOR GRADUATES THAT LEFT THE ORGANIZATION AT THE TIME OF SURVEY (N=175)**

Time	%
Less than 1 year	3.4%
1 year	4.6%
2 years	33.7%
3 years	26.3%
4 years	16.0%
5 years	7.4%
6 years	3.4%
7 years	1.1%
8 years	1.7%
9 years	1.1%
10 years	0.6%
11 years	0%
12 years or more	0.6%

The 2019 Pulse Graduate Survey results indicate at the time the survey was administered that 46.6% (153/328) stayed with the organization they entered upon graduation and 53.4% (175/328) left the organization they entered upon graduation. Among those who stayed, most (67.9%) had been with the same agency for four to seven years.

---

**F. STUDENTS RELEASED FROM OBLIGATION**

From 2012 to 2021, there were 10 partial or full releases from obligation. This includes 4 releases during the academic phase; and 3 partial and 3 full releases during the employment phase. In addition, there are 6 pending requests for release. The complete data is in Appendix E.

---

## G. COMPETENCY GAP ANALYSIS OF RECENT SFS GRADUATES

Because of the high level of academic achievement of SFS graduates at schools that have also distinguished themselves by earning special designation as Centers of Academic Excellence in Cybersecurity, the available data do not include remedial training needs. However, the SFS does conduct a gap analysis of students' levels of proficiency on general and technical cybersecurity competencies.

The competency gap analysis for recent graduates of the SFS program was conducted by OPM's Assessment and Evaluation Branch (AEB) in August and September of 2019. It focused on a set of competencies identified as important for successful performance in numerous cybersecurity positions across various institutions (i.e., Federal, state, local, and tribal government, FFRDCs, and other SFS-approved organizations). These competencies are based on the NICE Workforce Framework. However, the results were collected in 2019, prior to the most recent update to the NICE Workforce Framework which occurred in November 2020.

AEB invited 591 scholarship recipients who graduated between December 2016 and June 2019 to complete the *Survey for Recent Program Graduates* and 434 first-line supervisors of the pool of recent graduates to complete the *Survey for Supervisors of Recent Program Graduates*. Of the 591 invitations distributed to recent graduates, AEB received 370 submitted responses containing data, representing a response rate of 62.6%. Of the 434 invitations distributed to supervisors, AEB received 165 submitted responses containing data, representing a response rate of 38.0%.

Graduates participating in the survey were asked to rate their level of proficiency on each competency when first entering their position. Supervisors were asked to rate the level of proficiency on each competency required to successfully perform the duties. Both graduates and supervisors used a proficiency rating scale ranging from None to Expert.

- **Level 0 (None)** - No experience with or knowledge of the competency.
- **Level 1 (Awareness)** - Applied the competency in the simplest situations; Required close and extensive guidance; Demonstrated awareness of concepts and processes.
- **Level 2 (Basic)** - Applied the competency in somewhat difficult situations; Required frequent guidance; Demonstrated familiarity with concepts and processes.
- **Level 3 (Intermediate)** - Applied the competency in difficult situations; Required occasional guidance;

Demonstrated understanding of concepts and processes.

- **Level 4 (Advanced)** - Applied the competency in considerably difficult situations; Generally required little or no guidance; Demonstrated broad understanding of concepts and processes.
- **Level 5 (Expert)** - Applied the competency in exceptionally difficult situations; Served as a key resource and advised others; Demonstrated comprehensive, expert understanding of concepts and processes.

AEB aggregated data from supervisors, calculated averages, and rounded to a whole number that became a required proficiency level for a specific competency.

The competencies shown below are grouped into a general category of competencies and seven technical categories as defined by the NICE Workforce Framework. Each table includes the following columns

- Competency name
- Level of proficiency required (Lev)
- Average of SFS graduates self-report ratings of their proficiency level (Ave)
- Percentage of SFS graduates who self-reported that their proficiency level in a competency is below the required proficiency level (%)

## GENERAL COMPETENCIES

Competency	Lev	Ave	%
Accountability	3	3.9	<b>3.9%</b>
Attention to Detail	3	3.9	<b>3.3%</b>
Computer Skills	3	4	<b>4.5%</b>
Creative Thinking	3	3.6	<b>12.5%</b>
Decision Making	3	3.5	<b>10.9%</b>
External Awareness	2	2.9	<b>14.3%</b>
Flexibility	3	3.7	<b>8.1%</b>
Integrity/ Honesty	4	4.4	<b>12.5%</b>
Interpersonal skills	3	3.9	<b>9.4%</b>
Leadership	2	3.2	<b>4.8%</b>
Learning	3	4	<b>3.2%</b>
Oral Communication	3	3.6	<b>8.6%</b>
Organizational Awareness	2	3.1	<b>8.0%</b>
Reading	3	4.1	<b>2.9%</b>
Reasoning	3	3.9	<b>5.4%</b>
Resilience	3	3.7	<b>9.0%</b>
Self-Management	3	3.8	<b>8.0%</b>
Strategic Thinking	2	3.3	<b>6.9%</b>
Stress Tolerance	3	3.6	<b>12.4%</b>
Teamwork	3	3.9	<b>4.9%</b>
Writing	3	3.9	<b>7.5%</b>

### NICE - SECURELY PROVISION

Competency	Lev	Ave	%
Compliance	2	2.7	16.5%
Computer Network Defense	3	3	27.0%
Configuration Management	2	2.8	15.9%
Distributed Systems	2	2.7	15.0%
Embedded Computers	2	2.2	35.7%
Enterprise Architecture	2	2.7	17.8%
Information Assurance	3	3	32.1%
Infrastructure Design	2	2.8	13.9%
IT Architecture	2	2.7	14.4%
Logical Systems Design	2	2.5	21.0%
Requirements Analysis	2	2.8	13.7%
Systems Life Cycle	2	2.7	14.3%
Vulnerabilities Assessment	3	3.1	26.6%

### NICE - OPERATE AND MAINTAIN

Competency	Lev	Ave	%
Computer Network Defense	2	3	10.0%
Configuration Management	2	2.8	15.7%
Data Analysis	2	2.6	18.5%
Distributed Systems	2	2.6	14.4%
Enterprise Architecture	2	2.7	15.7%
IT Architecture	2	2.7	14.2%
Network Management	2	2.9	9.0%
Operating Systems	3	3.3	18.4%
Process Control	2	2.6	17.6%
Product Evaluation	2	2.7	20.4%
Risk Management	2	2.8	12.2%

### NICE - PROTECT AND DEFEND

Competency	Lev	Ave	%
Computer Network Defense	3	3	28.9%
Data Management	2	2.7	14.2%
Incident Management	2	2.6	19.0%
Information Systems/ Network Security	3	3.1	28.0%
IT Architecture	2	2.7	17.1%
Operating Systems	3	3.3	18.7%
Risk Management	2	2.8	16.2%
Security	3	3	30.1%
Software Engineering	2	3	15.9%
Threat Intelligence	2	2.7	16.4%
Vulnerabilities Assessment	3	3.1	30.5%

### NICE - OVERSEE AND GOVERN

Competency	Lev	Ave	%
Capital Planning and Investment Assessment	2	2	39.4%
Compliance	2	2.7	15.3%
Information Systems Security Certification	2	2.5	21.7%
Information Systems/ Network Security	3	3.1	25.2%
Internal Controls	2	2.5	20.3%
Operational Technology	2	2.6	18.9%
Project Management	2	2.8	14.0%
Risk Management	2	2.9	13.2%
Vulnerabilities Assessment	3	3.1	28.2%

**NICE - ANALYZE**

Competency	Lev	Ave	%
Computer Network Defense	3	3.1	<b>30.4%</b>
Data Analysis	3	2.9	<b>34.1%</b>
Data Management	3	2.8	<b>35.3%</b>
Information Systems/ Network Security	3	3.1	<b>25.2%</b>
IT Architecture	3	2.9	<b>31.3%</b>
Knowledge Management	2	3	<b>9.0%</b>
Modeling and Simulation	2	2.3	<b>30.4%</b>
Vulnerabilities Assessment	3	3.1	<b>29.0%</b>
Web Technology	3	3	<b>29.0%</b>

**NICE - COLLECT AND OPERATE**

Competency	Lev	Ave	%
Computer Network Defense	3	3.2	<b>25.8%</b>
Data Analysis	3	2.8	<b>43.3%</b>
Data Management	3	2.9	<b>38.2%</b>
Information Systems/ Network Security	3	3.2	<b>24.4%</b>
IT Architecture	3	2.9	<b>36.7%</b>

**NICE - INVESTIGATE**

Competency	Lev	Ave	%
Computer Forensics	3	2.7	<b>39.3%</b>
Computer Network Defense	3	3.1	<b>23.6%</b>
Criminal Investigation	2	2	<b>41.6%</b>
Data Analysis	3	2.8	<b>38.6%</b>
Forensics	2	2.4	<b>31.5%</b>
Information Systems/ Network Security	3	3.1	<b>29.2%</b>
Operating Systems	3	3.3	<b>21.6%</b>
Surveillance	2	2.2	<b>37.5%</b>

**H. DISPARITY IN REPORTING (2018 - 2021)**

There have been no known instances of the disparity in reporting between scholarship recipients and their respective institutions of higher education.

**I. FEDERAL CYBERSECURITY WORKFORCE STATISTICS**

OPM has provided a limited set of data from the OPM’s Enterprise Human Resources Integration (EHRI). EHRI contains Government-wide personnel data on Executive Branch agencies, excluding agencies within the Intelligence Community. More detailed information on the composition of the Federal Cybersecurity workforce is considered Controlled Unclassified Information by OPM and is not included in this report. The available data is in Appendix F.

**INCREASING NATIONAL CAPACITY IN CYBERSECURITY EDUCATION**

The CyberCorps® SFS program supports efforts to increase the ability of the United States higher education enterprise to produce cybersecurity professionals. Proposals may be submitted in response to the solicitation from the NSF-wide Secure and Trustworthy Cyberspace (SaTC) program which includes an education designation (EDU).



The EDU designation is interested in inquiry into and the development of evidence-based and evidence-generating approaches that will improve cybersecurity education and workforce development at the K-12, undergraduate, graduate, and professional education levels. EDU supports projects that: improve cybersecurity learning and learning environments, conduct education research; develop new educational materials and methods of instruction; develop new assessment tools to measure student learning, promote teacher recruitment and training in the field of cybersecurity; and improve the diversity of the cybersecurity workforce. In addition to innovative work at the frontier of cybersecurity education, the program also encourages replications of research studies at different types of institutions and with different student bodies to produce deeper knowledge about the effectiveness and transferability of findings. This may include, but is not limited to, the following efforts:

- Conduct research that advances improvements in teaching and student learning in cybersecurity;



- Based on the results of basic research in cybersecurity, define a cybersecurity body of knowledge and establish curricular activities for new courses, degree programs, and educational pathways leading to wide dissemination and adoption;
- Investigate approaches to make cybersecurity education and workforce development broadly diverse and inclusive, including the effects of instructional strategies on the culture of the STEM classroom;
- Design and implement graduate programs to produce future faculty and cybersecurity professionals with research expertise in critical areas, such as the secure use of AI, quantum computing, advanced manufacturing, and emerging wireless technologies;
- Improve teaching methods for delivering cybersecurity content to K-12 students that promote correct and safe online behavior, and understanding of the foundational principles of cybersecurity;
- Develop and implement activities to help K-12 teachers integrate cybersecurity into formal and informal learning settings;
- Support institutional collaborations between community colleges and four-year colleges and universities;
- Develop educational approaches or pathways to foster industry-relevant skills for cybersecurity jobs of the future;
- Develop effective evidence-based co-curricular activities for students studying



cybersecurity at the K-12, undergraduate, or graduate level; and

- Evaluate the effectiveness of cybersecurity competitions and other engagement, outreach, and retention activities.

The complete list of funded projects in FY 2018-2021 is in the Appendix J.

#### SPECIAL INITIATIVE: CYBERSECURITY EDUCATION IN THE AGE OF ARTIFICIAL INTELLIGENCE

One of the priority areas of the 2019 Federal Cybersecurity Research and Development Strategic Plan is Artificial Intelligence (AI) that enables autonomous systems to perform tasks that are traditionally considered to require human decision-making abilities. The plan highlights the mutual needs and benefits of AI and cybersecurity. In April 2020, NSF published a Dear Colleague Letter (DCL) (NSF 20-072 “Cybersecurity Education in the Age of Artificial Intelligence”) sponsored by the CyberCorps® SFS and SaTC programs and focusing on: the interplay between Artificial Intelligence (AI), Machine Learning (ML), and cybersecurity; partnerships between AI researchers, cybersecurity researchers, and education researchers in order to inspire novel education and outreach efforts; a workforce with integrated AI and cybersecurity competencies; and an informed public that understands the privacy, confidentiality, ethics, safety, and security implications of AI. The DCL received an enormous response of more than 400 concept papers and 34 teams of researchers

were invited to submit NSF proposals. SFS will continue supporting these efforts and use a similar approach to explore new collaborations at the intersection of cybersecurity and other priority areas such as quantum information science and next generation wireless networks.

The complete list of funded proposals submitted in response to the DCL is in the Appendix K.

#### K-12 INITIATIVES

The National Defense Authorization Acts of 2018 and 2021 modified the SFS statute (15 U.S. Code § 7442) and stated that SFS “shall provide awards to improve cybersecurity education, including by seeking to provide awards in coordination with other relevant agencies for summer cybersecurity camps or other experiences, including teacher training, in each of the 50 States, at the kindergarten through grade 12 level: (A) to increase interest in cybersecurity careers; (B) to help students practice correct and safe online behavior and understand the foundational principles of cybersecurity; (C) to improve teaching methods for delivering cybersecurity content for kindergarten through grade 12 computer science curricula; and (D) to promote teacher recruitment in the field of cybersecurity.” In response to this legislation, CyberCorps® supports investments in K-12 education with the aim of growing interest in cybersecurity careers; promoting foundational cybersecurity principles and safe online behavior; improving teaching methods to help

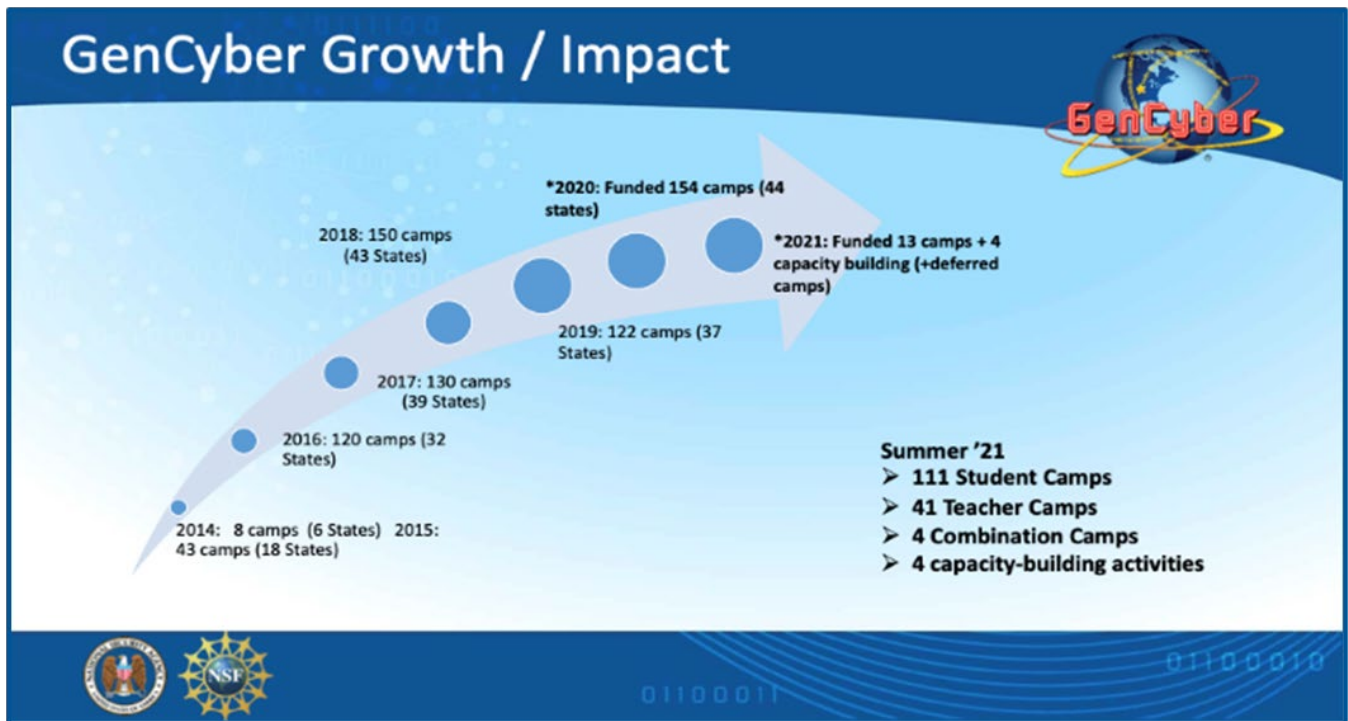


K-12 teachers integrate cybersecurity into formal and informal learning settings; and promoting teacher recruitment in the field of cybersecurity. Some key initiatives focused on K-12 students and teachers are described below.

### GENCYBER - INSPIRING THE NEXT GENERATION OF CYBER STARS

Since 2014, CyberCorps® has collaborated with the National Security Agency (NSA) to establish and offer the Inspiring the Next Generation of Cyber Stars (GenCyber) program. The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the K-12 level. The goals of the program are to help all students understand correct and safe on-line behavior, increase diversity and interest in cybersecurity

and careers in the cybersecurity workforce of the Nation, and improve teaching methods for delivering cybersecurity content in K-12 computer science curricula. The camps focus on engaging learners with sound cybersecurity principles and teaching techniques. In Summer 2019, the last pre-COVID year, the GenCyber program supported 123 camps, including 89 student camps and 34 teacher camps, held in 38 states, the District of Columbia, and Puerto Rico. These camps were developed and hosted by 76 academic institutions and attended by 3,035 students and 778 teachers; 53% of the students and 68% of the teachers were female, and 46% of the students and 26% of the teachers were underrepresented minorities. The COVID-19 pandemic necessitated 2020-2021 camps to be postponed or transitioned to virtual offerings.



In 2022, some camps will be held in person while a majority will still be virtual offerings.

GenCyber as an out-of-school time (OST) activity has become an important component of the K-12 cybersecurity ecosystem. It is accomplishing many of its goals, although in different ways and at varying degrees depending on the local context and educational/workforce ecosystem within which the camps reside. For student camps, GenCyber is a spark – an initial introduction to cybersecurity that excites students to pursue future opportunities if they exist in the ecosystem – or in the case of students who have had other exposure to cybersecurity topics, GenCyber functions to further students’ interests in an ecosystem with other opportunities. While the camps themselves provide the ‘spark’, a five-year evaluation of

the program (2015-2019) recommended that the camps be augmented with some form of follow-up activities. Responding to this recommendation, the most recent iteration of the GenCyber request for proposals (RFP) awards grants to cover an 18-month period, allowing host institutions to plan activities before as well as after the camps. While these activities will not be as intensive as the camps themselves, they are expected to enable students and teachers to sustain the spark long enough to identify other in-school activities that support cybersecurity interest.

Over the last eight years, the program has demonstrated the potential for scale and sustainability. Over 15,000 students have been directly impacted by the camps and several thousands more will be indirectly impacted by the teachers who have been





curriculum program in Computer Science and Cybersecurity. For example, does the JROTC-CS program lead to an increase in: the number of courses in computer science and cybersecurity that are offered, awareness of inequities in these courses, additional professional development experiences for teachers, or additional students at the schools who are engaged in computer science and cybersecurity? Aligning the current JROTC-CS demonstration project with research on multiple and confounding factors will provide evidence for ensuring a high-quality improvement science model that improves implementation of the project as it scales.



In the Summer of 2021, the pilot Cyber Academy program was expanded to reach a target of 100 Air Force JROTC cadets. With NSF funding from SFS, five Cyber Academies were hosted at five different SFS institutions: Cal Poly Pomona, Dakota State University,

Norwich University, Tennessee Tech University, University of Colorado at Colorado Springs. All of these institutions have robust cybersecurity education programs (evidenced by their existing SFS programs) as well as experience offering GenCyber camps in the past. A total of 96 Air Force JROTC cadets participated in the program in Summer 2021. In addition to the curriculum provided by Whatcom Community College, the students also had access to research and project opportunities provided by each of the host institutions. Students were provided the option of earning 3 college credits at the host institution; 85 out of the 96 cadets successfully completed all the work required and earned college credit. Students were also prepared to earn the CompTIA IT Fundamentals+ certification.

The SFS program is continuing to work with this broad coalition to further expand the pilot in Summer 2022. The goal is to increase the number of Academy sites to 10. Recruitment and institutional site identification is ongoing at the time of this writing. Out of the 10 Academy sites, the plan is to hold one academy as a residential program, one as a hybrid program, and the remaining eight as virtual programs. This combination approach will provide important lessons for future planning for this effort. The 2022 Cyber Academies will reach a total of 250 cadets. Another key dimension for expansion is the addition of a second service. The Marine Corps JROTC will also be participating in the 2022 Cyber Academies in addition the Air

Force. Similar to the 2021 Cyber Academies, the 2022 iteration will feature cybersecurity curriculum provided by the NCyTE Center in addition to project and research experiences at host institutions.

---

## ADVANCED PLACEMENT COMPUTER SCIENCE PRINCIPLES: CYBERSECURITY

A CyberCorps® SFS Capacity Building project entitled Catalyzing Computing and Cybersecurity in Community Colleges (C5) has been awarded to Whatcom Community College for the period 2015-2022. One of this project's two goals is to create and disseminate "CSP-Cybersecurity," a cybersecurity-themed version of the Advanced Placement course Computer Science Principles (CSP), which is being finalized by a team of computer science educators organized by the College Board and NSF.

According to the College Board, the non-profit organization that administers the SAT® and AP program for high schools, more than 950 colleges and universities offer credit, advanced placement, or both for qualifying scores on the AP CSP exam, thus allowing students to progress more rapidly in their chosen program of study by earning college credit while still in high school. In 2020, over 116,000 students took the AP CSP exam—more than double the number of exam takers in the course's first year, and a 21% increase over the previous year. There are many flavors

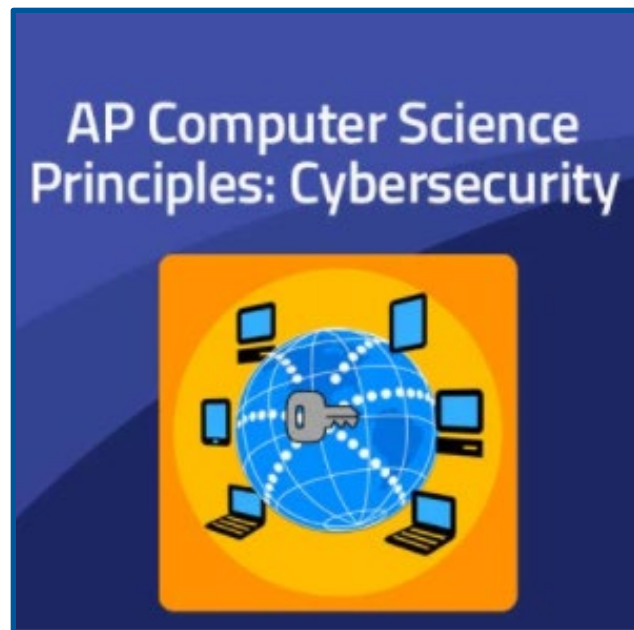
of CSP courses, but the course developed by the SFS C5 project, AP CSP: Cybersecurity, is the only one that has a cybersecurity theme and is officially endorsed by College Board.

AP CSP: Cybersecurity is offered by College Board authorized provider CodeHS and is free of charge to high school teachers. The available materials include a pre-approved syllabus, lesson plans, instructional supports, and professional development to help prepare teachers to teach the course. The C5 project (at Whatcom Community College) also created a collection of individual online educational units, supplemental materials and activities. The 13 lessons are designed to be an easy way to integrate cybersecurity concepts into the existing AP CSP course. In this initial set, all programming is in JavaScript; a variation in Python is being developed and will be released this year.

## COMMUNITY COLLEGE INITIATIVES

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. In recognition of this role, NSF supports skilled technical workforce programs at community colleges to develop skills necessary for the Nation's cybersecurity missions.

The 2014 Cybersecurity Enhancement Act included several important and lasting changes to the SFS program including



addition of community colleges. Subsequently, community college students were included in the CyberCorps® SFS program via a Community College (CC) Pathways where second-year students at community colleges became eligible for one year of support if there is a formal agreement between their community college and a four-year CyberCorps® institution. The student then transfers to the four-year institution to complete a bachelor's degree. At the four-year institution, the student is eligible for two more years of CyberCorps® support (total of three years). Currently there are 28 community colleges participating in the CC Pathways.

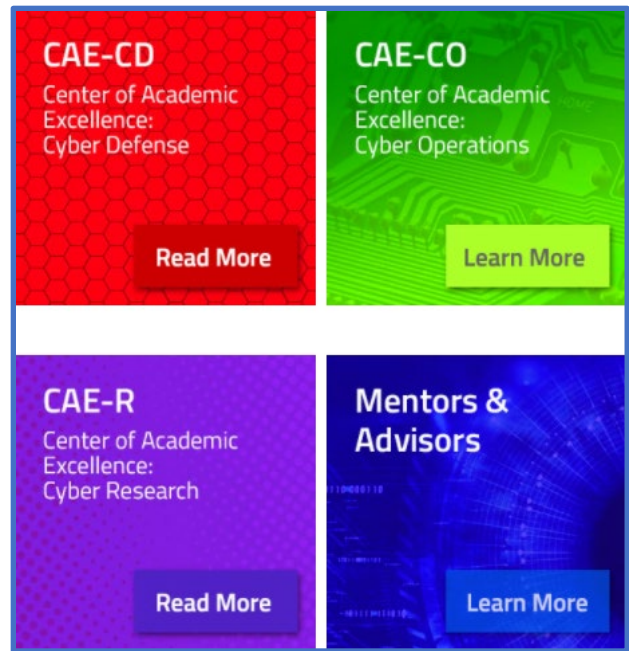
In addition, section 1649A of the National Defense Authorization Act for Fiscal Year 2018 authorized the National Science Foundation, in coordination with the Office of Personnel Management, to develop and implement a Community College Cyber Pilot (C3P) program

as part of NSF's CyberCorps® SFS program. Specifically, it authorized scholarships for eligible students who:

1. are pursuing associate degrees or specialized program certifications in the field of cybersecurity; and
2. have bachelor's degrees or are veterans of the Armed Forces.

In response to the NDAA 2018, NSF accepted proposals to develop, implement, support, and evaluate C3P projects in this pilot effort. This new category of CyberCorps® SFS scholars satisfies criteria and receives the benefits consistent with the CyberCorps® SFS program requirements. NSF encouraged projects that generate new knowledge about effective cybersecurity education, reskilling workers to meet cybersecurity needs, preparing nontraditional students to re-enter the educational system, increasing the diversity of the cybersecurity workforce, using applied research experiences to build skills and competencies for real-world scenarios, and building effective collaborations between educational institutions, business, industry, and government. Investigating some of these issues in conjunction with a novel educational program for the scholars may enhance the impact of the pilot projects.

The C3P Pilot consists of eight community colleges that in September 2018 received grants for a three-year period. However, due to the impact of the ongoing COVID-19 pandemic, the pilot has been extended to the



fourth year and will conclude in September 2022. It is expected that the final evaluation of the pilot outcomes and future recommendations will be available by January 2023.

The second goal of the CyberCorps® C5 project described in the previous section was to double the number of community colleges holding the "National Center of Academic Excellence in Information Assurance 2-Year Education" (CAE2Y) designation sponsored by the National Security Agency (NSA) and the Department of Homeland Security (DHS). In 2015 at the C5 program's inception, 32 community colleges had the CAE2Y designation. By the end of 2018, the number increased to 83, an increase of 51 CAE2Y designations or 159%. With C5 assistance, Alabama, Florida, Georgia, Idaho, Indiana, Kansas, Michigan, Minnesota, Missouri, Montana, Nebraska, Nevada, New Jersey,



North Dakota, Pennsylvania, Rhode Island, Tennessee, and Wisconsin had the first community college CAE in their state. The project exceeded its goals and the SFS program, in collaboration with NSA, has continued its funding and expanded the target from community colleges to all institutions of higher education.

As of July 2021, 522 educational institutions have been assisted from the beginning of the C5 grant with support from C5 funding. This includes 93 community colleges and 45 universities that have earned the CAE. In collaboration with the NSA and other government agencies, the C5 project plans to continue to use C5 funds to provide mentee support to colleges and universities through February 2022, for those that want to validate programs of study and/or achieve the CAE designation, improving the overall defense posture of the U.S. by significantly enhancing cybersecurity curriculum at educational institutions across the nation.

**INCREASING DIVERSITY AND INCLUSION IN THE CYBERSECURITY WORKFORCE.**

The underrepresentation of many groups in cybersecurity and computing, including women, Blacks and African Americans, Hispanic Americans, American Indians, Alaska Natives, Native Hawaiians, Native Pacific Islanders, and persons with disabilities, deprives large segments of the population of the opportunity to be cybersecurity professionals or researchers and importantly

deprives the nation from benefitting from the talent and potential of a large segment of the United States' population. Ending underrepresentation is aligned with SFS programmatic goals and critical to economic and national security. Addressing this matter will require a range of measures, including institutional programs and activities as well as culture change across colleges, departments, classes, and research groups.

Proposals submitted to the CyberCorps® SFS program are evaluated with careful attention to the following review criterion: "Broadening participation efforts at the institution as well as specific plans for recruitment, mentoring, and retention of CyberCorps® scholars who are members of underrepresented racial and ethnic minority groups, women, first-generation/low-income students, persons with disabilities, or veterans."

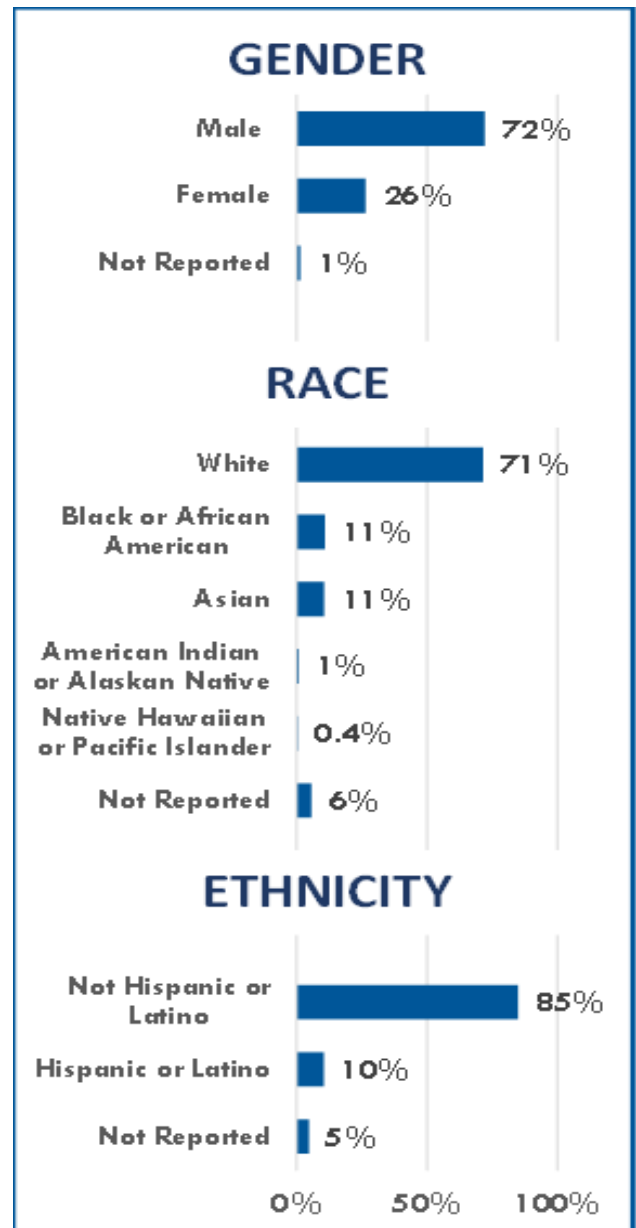
While the diversity efforts are on-going, CyberCorps® SFS students are still overwhelmingly White (71%) and male (72%). Therefore, with the aim of increasing the participation of populations traditionally underrepresented in the cybersecurity workforce, CyberCorps® SFS is planning long-term investments to understand barriers to diversity, equity, and inclusion at CyberCorps® institutions; and to implement best practices to address such barriers.

The following Minority Serving Institutions<sup>4</sup> are currently in the CyberCorps® program:

- Hampton University – HBCU
- Norfolk State University – HBCU
- North Carolina A&T State University – HBCU
- Arizona State University – HSI
- University of Arizona – HSI
- California State Polytechnic University, Pomona – HSI
- California State University, Sacramento – HSI & AANAPISI
- California State University, San Bernardino – HSI
- Florida International University – HSI
- New Mexico Institute of Mining and Technology – HSI
- University of New Mexico – HSI
- Polytechnic University of Puerto Rico – HSI
- Texas A&M University – HSI
- University of Texas at El Paso – HSI
- University of Texas at San Antonio – HSI
- University of Houston – HSI
- University of Hawaii – ANNHI & AANAPISI
- University of Central Florida – HSI

Collection of student demographic data began in 2015 and is voluntary.

## CYBERCORPS® RECIPIENT DEMOGRAPHICS<sup>5</sup>



<sup>4</sup> Minority Serving Institution (MSI) Abbreviations used include: HBCU: Historical Black Colleges and Universities; HSI: Hispanic Serving Institute; AANAPISI: Asian American Native American Pacific Islander Serving Institute; ANNHI: Alaskan Native or Native Hawaiian Serving Institute

<sup>5</sup> Data on CyberCorps® recipients' data from 2015 through June 2021

## WOMEN IN CYBERSECURITY

In 2013, SFS program awarded \$244,160 to a Tennessee Tech project (DUE-1303441) focused on broadening participation of women in cybersecurity. This effort created the first national event for women in cybersecurity and, over the 5-year period of this NSF grant, almost 3,500 participants have attended five Women in Cybersecurity (WiCyS) conferences. In 2018, when NSF support ended, WiCyS converted to a non-profit organization that currently has more than 5,200 members in more than 70 countries; over 140 student chapters; 42 professional affiliates; and more than \$4,400,000 in industry support. The WiCyS conference remains the flagship conference for women in cybersecurity and regardless of gender, is the only cybersecurity conference that has a comparable representation of students and professionals. It had 7,700 attendees, issued 3,876 student scholarships, honored 372 faculty grants, and 79 veteran fellowship awards. The nonprofit receives year-round support for its initiatives from 50 strategic partners including AWS, Bloomberg, Carnegie Mellon University Software Engineering Institute, Cisco, Facebook, Google, Lockheed Martin, Microsoft, Optum, and more.

WiCyS has 21 special interest groups such as neurodiversity in cybersecurity, data privacy, cybersecurity law, military spouses in cybersecurity, and more. WiCyS bridges the gap for job seekers with employers through the Job Board that has currently 47 employers

and 900 resumes. WiCyS also offers virtual and in-person career fairs, leadership summits, leadership series (to lead with equity, allyship and inclusion), senior leader networking luncheon workshops, ongoing strategic partner global webinar series (over 14,000 subscribers), affiliate and student chapter events, and much more.

### WICYS CONFERENCE 2021



In 2019, the SFS program supported WiCyS project to investigate a concerted effort to increase personal engagement through a series of “cyber encounters” offered to a mass population of teacher-student cohorts. It impacted more than 1000 students through instructional materials, cybersecurity challenges and the Girls-Go-CyberStart competition organized in collaboration with the SANS Institute. Additional efforts with support from Google, Bloomberg and Facebook were implemented in 2021 where 600 participants participated in a beginners Capture-The-Flag competition and 250 advanced to play the CyberStart game. After additional CyberTalent assessment, 40 finalist received scholarships to take advanced SANS security training and certification exams.

The Mentor/Mentee Program was developed to upskill and up-level women as they prepare for advancement at all levels of their cybersecurity career. WiCyS created a curriculum so that 191 mentors and 775 mentees can develop a deeper relationship in a shared cohort setting, reducing barriers and diving into meaningful conversations about career advancement.

Through the history of WiCyS, starting as a conference, WiCyS has showcased what diversity in the workforce looks like through gender and other lenses of representation. It continues to lead its mission to recruit, retain and advance women in cybersecurity through equity, allyship and inclusion, and ensures the power of community is cultivated throughout. When this project started in 2013, women participation in the cybersecurity profession in U.S. was at 11%, and today it is at 24% thanks to many efforts, including work done by WiCyS.

### CYBERCORPS® SFS HALL OF FAME

Each year, the CyberCorps® SFS program inducts one outstanding alumni 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 six alumni have earned this distinction.

**Josiah Dykstra**, author of "Essential Cybersecurity Science," a 2016 guide for using



the scientific method to build, test, and evaluate systems. In 2017, he received both the Presidential Early Career Award for Scientists and Engineers (PECASE)

and the Hope College Young Alumni Award. In 2013, he received the Director of National Intelligence's Galileo Award and the U.S. Department of Defense's David O. Cooke Excellence in Public Administration Award. Ever motivated to share and apply his extensive knowledge, Dykstra mentors university students and junior National Security Agency (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** graduated from a joint SFS program at Marymount University and

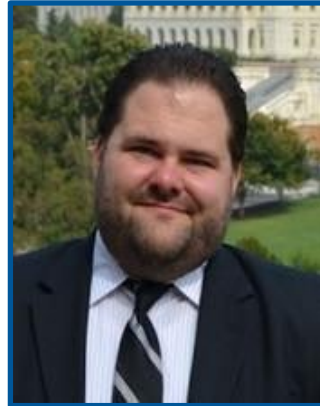


George Washington University in 2005, receiving a master's degree in computer science with an emphasis in information assurance. While serving as the

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 Department of Homeland Security's 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 the public-sector security solutions, strategies, technologies and policy.

**Steven Hernandez** has held information assurance positions at the U.S. Department of Education, the U.S. Department of Agriculture and an NSA National Security Administration Center of Academic Excellence Research

Institute in Idaho. In 2010, he joined the Department of Health of 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, and a bachelor's degree in computer information systems and an associate degree in electronic systems from the same institution.

**Patrick Kelly** has a master's degree in public policy from the SFS program at George

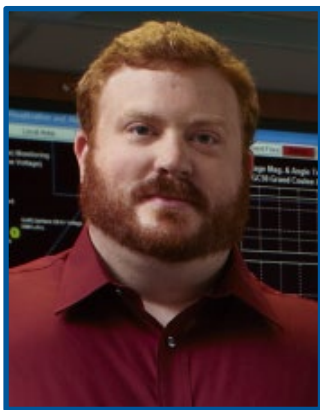


Washington University. Patrick began to serve his country after graduation at the Federal Reserve and at the Department of Health and Human Services where he served as



Senior Official for Privacy and the Information Security Branch Chief at 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 the 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 students.

**David Manz** is currently a Chief Cyber Security 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 a M.S. and 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 cyber security, control system security, and cryptographic key management.

**Dan Guido** 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 NYC. 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.”

## FUTURE OF THE CYBERCORPS® SFS PROGRAM

In support of the 2019 Federal Cybersecurity Research and Development Strategic Plan, NSF will continue its focus on cybersecurity education, with the aims of (i) building and sustaining an unrivaled cybersecurity workforce; (ii) promoting the development and maintenance of inclusive learning settings to improve diversity in cybersecurity; and (iii) raising cybersecurity awareness across the general population.

CyberCorps® SFS will address a critical shortage of cybersecurity educators and researchers by preparing up to 10% of SFS scholars to fulfil their service obligation as cybersecurity faculty members; continuing support of collaborative efforts among the AI, cybersecurity, and education research communities to foster a robust workforce with integrated AI and cybersecurity competencies; and exploring new collaborations at the intersection of cybersecurity and privacy, and other priority areas such as quantum

information science and engineering as well as next-generation wireless networks.

CyberCorps®: SFS will accelerate investments in K-12 as well as post-secondary education with the aim of growing interest in cybersecurity careers and their intersection with other key areas of national interest such as data science and AI; promoting foundational cybersecurity principles and safe online behavior; developing curriculum materials and improving teaching methods to help K-12 teachers as well as college professors integrate cybersecurity and privacy into formal and informal learning settings; developing new knowledge on how people learn the concepts, practices, and ways of thinking in cybersecurity; and promoting teacher recruitment in the field of cybersecurity. With the aim of increasing the participation of populations traditionally underrepresented in the cybersecurity workforce, CyberCorps®: SFS will make investments to (a) understand barriers to diversity, equity, and inclusion at SFS institutions; and (b) implement best practices to address such barriers.

## APPENDIX A: POST GRADUATE PLACEMENT RATE BY ENROLLED YEAR

Source: SFS Master Roster and Placement Log as of 10/20/2021

Enrolled Year	Placed	In Process	Still Looking	Released	Repayment	Total	Graduate Placement Rate <sup>6</sup>	Still Looking within 18 Months	Still in School	Non Grad Release	Non Grad Repayment	Total Awarded SFS
2001	25	0	0	6	0	31	81%	0	0	0	0	31
2002	95	0	0	16	1	112	85%	0	0	2	1	115
2003	196	0	0	16	2	214	92%	0	0	1	4	219
2004	171	0	0	3	2	176	97%	0	0	0	9	185
2005	166	0	1	2	4	173	96%	0	0	4	5	182
2006	124	0	0	0	3	127	98%	0	0	1	5	133
2007	100	0	0	0	5	105	95%	0	0	1	5	111
2008	93	0	0	0	0	93	100%	0	0	0	1	94
2009	117	0	0	1	8	126	93%	0	0	4	3	133
2010	169	0	0	1	6	176	96%	0	0	2	3	181
2011	179	0	2	2	6	189	95%	0	0	2	4	195
2012	173	0	1	0	5	179	97%	0	0	2	5	186
2013	244	1	1	1	7	254	96%	0	0	1	13	268
2014	254	1	1	3	8	267	96%	0	0	0	10	277
2015	258	1	1	0	9	269	96%	2	0	0	6	277
2016	279	5	1	2	4	291	98%	11	4	1	6	313
2017	313	11	3	0	5	332	98%	11	6	2	6	357
2018	255	25	0	0	2	282	99%	35	17	2	3	339
2019	188	24	0	0	1	213	100%	74	88	2	7	384
2020	31	6	0	0	0	37	100%	19	315	0	4	375
2021	0	0	0	0	0	0	0%	0	351	0	1	352
<b>Total</b>	<b>3430</b>	<b>74</b>	<b>11</b>	<b>53</b>	<b>78</b>	<b>3646</b>	<b>96%</b>	<b>152</b>	<b>781</b>	<b>27</b>	<b>101</b>	<b>4707</b>

<sup>6</sup> Graduate placement rate is calculated as the percentage of scholarship recipients that have graduated and that are in a *still looking*, *in process*, or *placed* status.



## APPENDIX B: POST GRADUATE PLACEMENT BY AGENCY

Source: SFS Master Roster and Placement Log as of 10/20/2021<sup>7</sup>

Post Graduate Agency	Total
<b>Total</b>	<b>3426</b>
<b>Department of</b>	
Agriculture	11
Commerce	56
Defense	115
Education	6
Energy	11
Health & Human Service	12
Homeland Security	148
Housing and Urban Development	4
Interior	14
Justice	101
Labor	8
State	32
Transportation	6
Treasury	44
Veterans Affairs	13
<b>Defense</b>	
Air Force	116
Army	189
National Security Agency	678
Navy	345
<b>Energy Labs</b>	
Ames Laboratory	2
Argonne National Laboratory	7
Brookhaven National Laboratory	1
Idaho National Laboratory	40
Lawrence Livermore National Laboratory	32
Los Alamos National Laboratory	37
National Renewable Energy Laboratory	5
Oak Ridge National Laboratory	20
Pacific Northwest National Laboratory	41

<sup>7</sup> The total number of placements (3426) on this report differs from the total number of placements on the Post Graduate Placement Rate by enrolled year (3430) because this report does not include start dates occurring in 2022 and the report was pulled at different times during the day so other changes could have occurred.

Sandia National Laboratories	153
<b>FFRDC</b>	
Aerospace Federally Funded Research and Development Center	21
Carnegie Mellon University - Defense Advanced Research Projects Agency (DARPA)	1
Center for Internet Security	9
Center for Naval Analyses	2
Homeland Security Systems Engineering and Development Institute	6
Institute for Defense Analyses (IDA)	7
Jet Propulsion Laboratory (NASA)	9
Massachusetts Institute of Technology (MIT) - Lincoln Laboratory	66
MITRE Corporation	235
MITRE Corporation - Center for Advanced Aviation System Development	1
MITRE Corporation - Center for Enterprise Modernization	3
MITRE Corporation - National Cybersecurity Center of Excellence	24
MITRE Corporation - National Security Engineering Center	22
National Defense Research Institute/RAND Corp.	1
North American Electric Reliability Corporation (NERC)	1
Software Engineering Institute (SEI)- Carnegie Mellon University	62
Southwest Research Institute	1
Stanford Linear Accelerator Center (SLAC)	1
Agency for International Development	4
Board of Governors of the Federal Reserve System	59
Central Intelligence Agency (CIA)	71
Contractor/Private-Approved	13
Environmental Protection Agency	2
Executive Office of the President	2
Federal Communication Commission	2
Federal Deposit Insurance Corporation (FDIC)	19
Federal Reserve Banks (Banks and NRIT)	54
Federal Retirement Thrift Investment Board	1
Federal Trade Commission	2
Freddie Mac	1
General Services Administration	4
Government Accountability Office (GAO)	46
Judicial Branch	4
National Aeronautics and Space Administration (NASA)	9
National Science Foundation (NSF)	7
Nuclear Regulatory Commission (NRC)	6
Office of Personnel Management (OPM)	6
Privacy & Civil Liberties Oversight Board (PCLOB)	1

Railroad Retirement Board (RRB)	6
Securities and Exchange Commission (SEC)	4
Small Business Administration (SBA)	2
Smithsonian Institution/Smithsonian Libraries	2
Social Security Administration (SSA)	9
State/Local/Tribal Government	235
U.S. Agency for Global Media	2
U.S. Government	21
U.S. Postal Service (USPS)	9
U.S. Senate	5
UARC/John Hopkins University - Applied Physics Laboratory	98
US Global Change Research Program	1

## APPENDIX C: JOB TITLES

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

Access Manager	Associate Embedded Security Engineer
Adjunct Faculty	Associate Engineer
Adjunct Instructor and Research Fellow	Associate Information Security Analyst
Adjunct Professor	Associate Information Systems Analyst
Advanced Developer	Information Security
AF Palace Acquire Intern	Associate Member of the Technical Staff
Analyst	Associate Network and Security Engineer
Analyst, Cybersecurity Hunt and Incident Response Team	Associate Network Intelligence Analyst
Analytic Methodologist	Associate Networking and Security Engineer
Application Developer	Associate Operations Research Analyst
Application Security Analyst	Associate Penetration Tester
Application security Engineer	Associate Professional Staff I
Application Sys Analyst and Programmer II	Associate Professional Staff I Cyber Control Systems QNC
Applications Administrator II	Associate Research Staff
Applications Programmer	Associate Security Engineer
Applied Cybersecurity Engineer	Associate Security Researcher
Applied Research Mathematician	Associate Senior Cyber Security Researcher
Architect Support	Associate Software Developer
Assistant Network Defense Analyst	Associate Software Engineer
Assistant Professor	Associate Software Security Engineer
Assistant Professor - Cyber Security Instructor	Associate Staff - Cyber Systems and Technology Group
Assistant Professor of Mgmt Science and Information System	Associate Staff - Engineering
Assistant Researcher	Associate System Security Engineer
Assistant Security Researcher	Associate Systems Software Specialist
Assistant Software Engineer	Associate Technical Staff
Assistant Staff - Cyber Security Researcher	Attorney
Assistant Staff Engineer	Attorney Advisor
Assistant Staff Engineer	Auditor
Assistant Staff for Cyber System Assessments Group	Availability Specialist
Assistant Technical Staff	Business Intern - Application Support Group
Associate Adjunct Professor	Business Systems Analyst
Associate Computer Scientist	Business Technology Strategist Junior Analyst
Associate Computer Security Staff	Capabilities Development Specialist
Associate Cyber Researcher	Cellular Cyber Research Engineer
Associate Cyber Security Engineer	CERT Analyst
Associate Cybersecurity Software Engineer	CERT Technical Staff
Associate Data Scientist	Chief Cyber Security Officer
	Chief Scientific Officer

CIO/G6 Army Knowledge Leadership Internship Program  
Clinical Assistant Professor of Cybersecurity  
Clinical Informatics Analyst I  
Clinical Quality Specialist  
Committee Professional Staff Member  
Communications Analyst  
Communications Network Analyst  
Communications Network Specialist  
Compliance Analyst  
Computer & Network Security Scientist  
Computer Analyst  
Computer Application Analyst  
Computer Applications Programmer  
Computer Associate Operations  
Computer Detection Network Analyst  
Computer Engineer  
Computer Engineer Intern  
Computer Forensics Examiner  
Computer Forensics Specialist  
Computer Information Security Spec  
Computer Network Analyst  
Computer Network Defense  
Computer Network Defense Analyst  
Computer Network Defense Service Provider  
Computer Network Operations Development Program  
Computer Network Operator  
Computer Operator I  
Computer Programmer  
Computer Science  
Computer Science - Cybersecurity  
Computer Science Analyst  
Computer Science and Cyber Security Advisor  
Computer Science and Security Engineer  
Computer Science Engineer  
Computer Science Incident Response Team  
Computer Science Instructor  
Computer Science Intern  
Computer Science Research and Developer  
Computer Science Senior  
Computer Science Staff  
Computer Scientist  
Computer Scientist - Field Ops  
Computer Scientist - Naval Research Lab

Computer Scientist - Pathways Recent Graduate  
Computer Scientist - Security  
Computer Scientist (Cyber)  
Computer Scientist (Intern)  
Computer Scientist (ND-1550)  
Computer Scientist (Red Team)  
Computer Scientist I  
Computer Scientist Intern  
Computer Scientist/Math Programmer  
Computer Security Manager  
Computer Security Researcher  
Computer Security Specialist  
Computer Software Research/Development  
Computer Specialist  
Computer Support Specialist  
Computer Systems Analysis  
Computer Systems Analyst/Programmer  
Computer Systems Architect at the Technology Directorate  
Computer Systems Researcher  
Computer Systems Security Manager  
Computer Systems Specialist  
Computer Technician  
Computer/Research Scientist  
Counter Threat Automation Developer  
Counter Threat Automation Engineer -Developer  
Criminal Investigator - Computer Crimes Unit  
Criminal Investigator (Cyber)  
Critical Infrastructure Analyst  
Critical Infrastructure Modeler  
Critical Skills Master's Program  
Cryptanalyst - Computer Network Operations Developer  
Cryptic Analytic Computer Scientist  
Cryptographer  
Cryptographic Computer Scientist  
Cryptographic Vulnerability Analyst  
Cryptologic Computer Scientist  
Cryptologic Linguist  
Cryptologic Vulnerability Analyst  
CTN-Cryptologic Technician Networks  
Cyber Adversarial Engineer  
Cyber Analyst  
Cyber and IT Risk Associate  
Cyber Assessor

Cyber Audit Analyst with NYC Cyber Command  
 Cyber Cellular Research Engineer  
 Cyber Concepts Developer  
 Cyber Defense Development Program  
 Cyber Defense Infrastructure Support Specialist  
 Cyber Defense Network Analyst  
 Cyber Defense Solutions Engineer  
 Cyber Defensive Operator  
 Cyber Engineer  
 Cyber Engineering Group Associate Professional Staff I  
 Cyber Exploitation Corps Development Program Participant  
 Cyber Exploitation Officer  
 Cyber Forensics Investigator  
 Cyber Infrastructure Cyber Protection Vulnerability Analyst  
 Cyber Network Professional  
 Cyber Network Security Research Engineer  
 Cyber New Professional  
 Cyber Officer  
 Cyber Operating Systems Research Engineer  
 Cyber Operations Analyst  
 Cyber Operations Officer  
 Cyber Operations Research  
 Cyber Operations Specialist  
 Cyber Physical Systems Engineer  
 Cyber Physical Systems Security Researcher  
 Cyber Platform Engineer  
 Cyber Professor  
 Cyber Research Engineer  
 Cyber Research Staff  
 Cyber Response Investigator  
 Cyber Security Analyst  
 Cyber Security Application Developer  
 Cyber Security Associate  
 Cyber Security Engineer  
 Cyber Security Engineer - Exercise Developer  
 Cyber Security Engineer - Insider Threat  
 Cyber Security Engineer - Penetration Test  
 Cyber Security Engineer - Staff  
 Cyber Security Engineer Associate  
 Cyber Security Engineer I  
 Cyber Security Engineer Lead  
 Cyber Security Exercise Developer and Trainer  
 Cyber Security IT Specialist  
 Cyber Security Member  
 Cyber security network research engineer  
 Cyber Security Officer  
 Cyber Security Operations  
 Cyber Security Research and Support Engineer  
 Cyber Security Research Engineer  
 Cyber Security Research Scientist  
 Cyber Security Research Scientists II  
 Cyber Security Researcher  
 Cyber Security Researcher and Developer  
 Cyber Security Researcher Associate Senior  
 Cyber Security Scientist  
 Cyber Security Software Engineer  
 Cyber Security Specialist  
 Cyber Security Staff  
 Cyber Security Technical Analyst  
 Cyber Security Technical Professional  
 Cyber Security Technical Staff  
 Cyber Security Trainer and Exercise Developer  
 Cyber Software Engineer  
 Cyber Systems Exploitation Researcher  
 Cyber Systems Security Engineer  
 Cyber Test and Evaluation Engineer  
 Cyber Threat Analyst  
 Cyber Threat Engineer  
 Cyber Threat Intelligence Analyst  
 Cyber Warfare Developer  
 Cyber Workforce Development Intern  
 Cyber Workforce Engineer Scientist  
 Cybersecurity Automation Engineer (Information Services IV)  
 Cybersecurity Engineer  
 Cybersecurity Engineer- Exercise Developer  
 Cybersecurity Engineer I  
 Cybersecurity Instructor  
 Cybersecurity Intelligence Specialist  
 Cybersecurity Management Analyst  
 Cybersecurity Management Officer  
 Cybersecurity Member of Technical Staff  
 Cybersecurity Research and Development  
 Cybersecurity Research and Development Senior Scientist  
 Cybersecurity Research and Development Software Engineer



Cybersecurity Research Engineer  
 Cybersecurity Researcher  
 Cybersecurity Risk Analysis Associate  
 Cybersecurity Risk Analyst  
 Cybersecurity Risk Management Framework Analyst  
 Cybersecurity Scientist and Engineer  
 Cybersecurity Senior Engineer  
 Cybersecurity Software Engineer  
 Cybersecurity Specialist  
 Cybersecurity Staff  
 Cybersecurity Standards Specialist  
 Cybersecurity Teacher  
 Cybersecurity Technical Analyst  
 Cybersecurity Technical Professional  
 Cybersecurity Technical Staff  
 Cybersecurity Technical Staff I  
 Cybersecurity Technical Staff II  
 Cybersecurity Technology Developer  
 Cybersecurity Test and Evaluation Specialist  
 Cybersecurity Test Engineer  
 Cyberspace Operations Specialist  
 Cyberthreat Intel Analyst  
 Data Analyst  
 Data Engineer Cyber and Machine Learning  
 Data Processing Programmer  
 Data Scientist  
 Data Systems Engineer  
 Defense Network Exploitation Analyst  
 Defensive Cyber Engineer  
 Deputy District Attorney  
 Deputy Information Security Officer  
 Developer  
 DHS Emerging Leader Fellowship  
 Digital Engineer  
 Digital Evidence Analyst  
 Digital Investigative Analyst  
 Digital Network Exploitation Analyst  
 Digital Service Expert  
 Durational Technology Security Specialist  
 Electrical Engineer  
 Electrical Engineering Intern  
 Electronics Engineer  
 Embedded Security Engineer  
 Embedded Software Engineer  
 Emergency Management Planner  
 Emerging Technology Institute Specialist  
 Endpoint Exploitation Analyst  
 Energy Industry Analyst  
 Engineer  
 Engineer/Scientist 2  
 Engineering and Physical Sciences Researcher  
 Engineering Applications Software Engineer  
 Engineering Applications Software Engineer I  
 Engineering Applications Software Engineer II-  
 Cyber Defense  
 Engineering Intern  
 Engineering Leader  
 Engineering Scientist  
 Engineering Scientist Associate  
 Enterprise Information Assurance Officer  
 Entry Level Cyber Security or System Security  
 Engineer  
 Entry Level Engineer  
 Entry Level Technical Developer  
 Exploitation Analyst  
 Financial Systems Analyst  
 Foreign Service Specialist  
 Foreign Services Officer  
 Forensic Analyst  
 Forensic Examiner  
 Forensic Examiner Trainee  
 Forensic Investigator  
 Forensic IT Specialist  
 Forensic Systems Analyst  
 Forensics Specialist Engineer  
 GAO Entry Level Information Technology Auditor  
 General Attorney  
 General Security Assistant  
 Geographer  
 Geospatial Analyst  
 Global Development Program  
 Global Network Exploitation and Vulnerability  
 Analyst  
 Global Network Operations Vulnerability Analyst  
 Graduate Development Program  
 Hardware-Software Analysis Engineer  
 Hardware-Software Design Engineer  
 Hardware-Software Engineer  
 Hardware-Software Project Manager

HPC Cyber Security Engineer  
 HPC System Administrator and Security Engineer  
 Identity and Access Analyst Assistant  
 Imagery Analyst  
 Incident Handler  
 Incident Response Team Member  
 Incident Response/Forensics Specialist  
 Industrial Control Systems Analyst  
 Industrial Engineer  
 Information Assurance Analyst  
 Information Assurance Compliance Officer  
 Information Assurance Engineer  
 Information Assurance Intern  
 Information Assurance Management Officer  
 Information Assurance Manager  
 Information Assurance Officer  
 Information Assurance Security Professional  
 Information Assurance Specialist  
 Information Assurance Staff  
 Information Assurance Technical Officer  
 Information Management Specialist  
 Information Management Technical Specialist  
 Information Security Administrator  
 Information Security Analyst  
 Information Security Analyst - Incident Detection  
 Information Security Analyst EGRC  
 Information Security Analyst I  
 Information Security Analyst II  
 Information Security Analyst III  
 Information Security Associate  
 Information Security Associate Sr  
 Information Security Compliance Specialist  
 Information Security Engineer  
 Information Security Engineer Assistant  
 Information Security Engineer Scientist  
 Information Security Engineer/Scientist  
 Information Security Integrator  
 Information Security Intelligence Analyst  
 Information Security Intern/Scientist  
 Information Security Officer  
 Information Security Operations Center  
 Technician II  
 Information Security Risk Analyst  
 Information Security Scientist  
 Information Security Scientist/Engineer  
 Information Security Specialist  
 Information Security Sr Analyst B  
 Information Security Student Worker  
 Information Specialist Operations  
 Information System Analyst  
 Information System Engineer  
 Information Systems & Computer Systems  
 Software  
 Information Systems Engineering Project  
 Manager  
 Information Systems Scientist/Engineer  
 Information Systems Security Analyst  
 Information Systems Security Designer  
 Information Systems Security Engineer  
 Information Systems Security Engineer ISSE  
 Information Systems Security Manager  
 Information Systems Security Officer  
 Information Technology and Cyber Risk Analyst  
 Information Technology and Cyber Risk  
 Management Analyst  
 Information Technology Associate  
 Information Technology Auditor  
 Information Technology Auditor (Cybersecurity)  
 Information Technology Compliance Analyst II  
 Information Technology Cyber Risk Management  
 Analyst  
 Information Technology Cybersecurity Analyst  
 Information Technology Cybersecurity Engineer  
 Information Technology Cybersecurity Specialist  
 Information Technology Cybersecurity Specialist  
 (INFOSEC)  
 Information Technology Enterprise Architect  
 IT Examination Analyst Disaster Recovery and  
 Continuity  
 Information Technology II  
 Information Technology Management Specialist  
 Information Technology Manager  
 Information Technology Network Team Lead  
 Information Technology Officer  
 Information Technology Program Analyst  
 Information Technology Project Specialist  
 Information Technology Risk Analyst  
 Information Technology Risk Examiner  
 Information Technology Security Analyst  
 Information Technology Security Specialist

Information Technology Specialist	Information Technology Systems Administrator Senior
Information Technology Specialist - (PLCYPLN)	Information Technology Systems Analyst
Information Technology Specialist - Cybersecurity	Information Technology Technical Support Analyst Senior
Information Technology Specialist - Forensic Examiner	Information Technology Technician I
Information Technology Specialist (APPSW)	Information Technology User Support Technician II
Information Technology Specialist (Co-Op Conversion)	Information Technology Volunteer
Information Technology Specialist (CUSTSPT)	Infosec Engineer/Scientist
Information Technology Specialist (CUSTSPT) (NETWORK)	InfoSec Operations Analyst
Information Technology Specialist (INET APPSW)	Instructional Design Specialist
Information Technology Specialist (IA Specialist)	Instructional Faculty Member
Information Technology Specialist (INFOSEC)	Instructor of Computer and Cyber Sciences
Information Technology Specialist (Network Services)	Instructor of Computer Science
Information Technology Specialist (Security)	Instructor-Arizona State University
Information Technology Specialist (Student Trainee)	Integrated Warfare Systems Test and Evaluation Engineer
Information Technology Specialist (System Admin)	Intelligence Analyst
Information Technology Specialist (Systems Analysis)	Intelligence Officer
Information Technology Specialist Customer Support	Intelligence Officer - Computer Network Operations
Information Technology Specialist Cybersecurity	Intelligence Operations Specialist
Information Technology Specialist Forensic Examiner	Intelligence Specialist
Information Technology Specialist Functional Analyst	Intelligence Specialist (Operations)
Information Technology Specialist III Enterprise Security Eng	Intelligence Specialist Operations
Information Technology Specialist Information Security	Interactive Operator
Information Technology Specialist Information Security Mgmt	Intermediate Cyber Operations Engineer
Information Technology Specialist Policy Planning	Internet and Technology Analyst
Information Technology Specialist Supervisory INFOSEC	Intrusion Analyst Skill Development Program Investigator
Information Technology Specialist-Forensic Examiner	IO (Computer Network Operations)
Information Technology Staff Auditor	Joint Intelligence Navy Reserve Officer
Information Technology Support Analyst	Judicial Law Clerk
	Junior Information Systems Security Analyst
	Junior Insider Threat Researcher
	Junior IT Specialist
	Junior Network Security Analyst
	Junior Network Security Metric Analyst
	Junior Site Reliability Engineer
	Lab Systems Engineer
	Lead Embedded Security Engineer
	Lecturer of Computer Information Systems
	Linux Administrator
	Logistics Management Specialist

Malware analyst	Network Security Professional II
Malware and Cyber Security Research Engineer	Network Security Software Developer
Management Analyst Cyber Security	Network Security Test Engineer
Management and Program Analyst	Network Services Support Technician
Manager Information Technology Security	Network Systems Engineer
Mathematician	Network Technician
Mechanical Engineer - Cyber SME	Open Stack Administration and Software
Member of Computer & Network Securities	Development
Team	Operational Support Technician
Member of Engineering Staff - Associate Level	Operations Research Analyst
Member of Information Assurance Division	Operations Specialist
Member of Technical Staff (Cybersecurity)	Operations Support Officer
Member of the Technical Staff	Palace Acquire Intern
Member of the Technical Staff - Info. Sys.	Palace Acquire Intern - Computer Scientist
Security Analyst	Patent Examiner (Computer Science/ Information
Member of the Technical Staff (Computer	Security)
Science R&D)	Platform Engineer Cyber Security Analyst L II
Member Technical Staff	Policy Analyst
Military Analyst	Policy Lead
Mission Strategy	Presidential Management Fellow
Mobile Cyber Security Engineer	Privacy Analyst
Multi-discipline Language Analyst	Privacy and Security Analyst
Multi-Discipline Systems Engineer	Probation Parole Officer
National Geospatial Intelligence Agency Intern	Production Operator
National Graduate Fellowship Program Fellow	Professional Associate Staff
National Incident Response Team Intern	Professional Associate Staff I
National Security Specialist	Professional Staff
Naval Special Warfare Officer Program	Professional Staff I
Navy Scientist	Program Coordinator - Networking
Network Administrator	Program Risk Management and Monitoring
Network Administrator I	Team Member
Network Analyst	Programmer
Network and Intelligence Analyst	Programmer Analyst
Network and Systems Administrator	Programmer Analyst I
Network Data Analyst	Project Director
Network Defense Analyst	Public Affairs Specialist
Network Engineer	Public Health Informatics Fellow
Network Engineer I	Quality Assurance Analyst
Network Evaluator	R&D S&E Microwave and Sensor Engineering
Network Intrusion Analyst	Radio Frequency Design Engineer
Network Research Engineer	Red Team Operator
Network Security Analyst	Research and Development Analyst
Network Security Engineer	Research and Development Computer Engineer
Network Security Professional	Research and Development Computer Science
Network Security Professional I	Member Level

Research and Development Computer Scientist  
Research and Development Cyber Security Team  
Member  
Research and Development Cybersecurity  
Research and Development Cybersecurity  
Engineer  
Research and Development Cybersecurity  
Incident Response  
Research and Development Cybersecurity  
Member Level  
Research and Development Cybersecurity  
Researcher  
Research and Development Scientist  
Research and Development Scientist and  
Engineer  
Research and Development SE Computer  
Science  
Research Assistant  
Research Assistant for the Center for Cyberspace  
Research  
Research Assistant II  
Research Associate  
Research Associate I  
Research Associate II  
Research Associate IV  
Research Computer Engineer  
Research Computer Scientist  
Research Development Software Engineer  
Cybersecurity  
Research Engineer  
Research Engineer I  
Research Engineer II  
Research Engineer III  
Research Fellow  
Research Programmer  
Research Scientist  
Research Scientist I  
Research Scientist III  
Research System Administrator  
Research Systems Analyst  
Researcher  
Researcher and Developer  
Researcher II  
Researcher II - Cyber Security and Resilience

Researcher II Network and Security Research  
Engineer  
Reverse Engineer  
Reverse Malware Analyst  
RF Design Engineer  
Risk Analyst  
SCEP Student IT Trainee  
Science & Weapons Analyst  
Science and Engineering Cybersecurity  
Science, Technology, and Weapons Analyst  
Science, Weapons, and technology Analyst  
Scientist  
Scientist (IA Team)  
Scientist / Engineer II  
Scientist 1  
Scientist Engineer  
Scientist II  
Scientist--Software Assurance Manager  
Security Administrator  
Security Analyst  
Security Analyst II  
Security Designer  
Security Engineer  
Security Operation Center Analyst  
Security Operations Analyst III  
Security Operations Associate  
Security Operations Center Analyst  
Security Operations Engineer  
Security Research Analyst  
Security Research and Education  
Security Researcher  
Security Senior Analyst A  
Security Software Developer  
Security Specialist  
Security Systems Engineer  
Senior Analyst  
Senior Applications Developer  
Senior Auditor I  
Senior Computer Science Engineer  
Senior Computer Scientist  
Senior Computer Vision Software Engineer  
Senior Cyber Cloud and Network Engineer with  
Dept Security  
Senior Cybersecurity Engineer

Senior Cybersecurity Research and Development Staff  
Senior Electrical Engineer  
Senior Information Security Engineer/Scientist  
Senior Information Security Services Specialist  
Senior Information Systems Engineer  
Senior Investigative Analyst - Programmer/DBA  
Senior Law Clerk  
Senior Member of Technical Staff  
Senior Mobile Cybersecurity Engineer  
Senior Network and Systems Administrator  
Senior Network Engineer  
Senior Network Security Engineer  
Senior Network Systems and Distributed Systems Engineer  
Senior Professional Staff I  
Senior Security Analyst  
Senior Sensor Systems Engineer  
Senior Software Engineer  
Senior Software Systems Engineer  
Senior System Administrator  
Senior Systems Engineer  
Signals Analyst  
Software and Computing Systems Student  
Software Application Developer  
Software Computer System Graduate Student Intern  
Software Configuration Management Specialist  
Software Developer  
Software Developer - Computing Directorate Global Security  
Software Developer Analyst  
Software Developer Data Analytics  
Software Developer I  
Software Development Specialist  
Software Engineer  
Software Engineer - Information Security Team  
Software Engineer I  
Software Engineer II  
Software Implementation and Integration Engineer  
Software Systems Engineer  
Software Systems Engineer II  
Software Systems Engineer, Senior  
Software Vulnerability Analyst

Software/Computer Security Engineer  
Special Agent  
Special Agent (Criminal Investigator)  
Special Investigations Officer  
SQL Server DBA  
Sr Cyber Security Researcher  
Sr Malware and Cyber Security Research Engineer  
Sr Multi-Discipline Systems Engineer  
Sr Professional Staff I  
Sr. Multiple Discipline Systems Engineer  
Sr. Technologist (Windows System Administrator)  
Staff Cyber Engineer  
Staff Cybersecurity Engineer  
Staff Officer  
Staff Operations Specialist  
Staff Programmer Analyst  
Student Cooperative Administrative Band on Comp Crime  
Student Intern  
Student Trainee  
Student Trainee (Information Technology Specialist)  
Student Trainee (Intelligence)  
Student Trainee Computer IT Security  
Student Trainee Engineering  
Student Trainee Information Technology Management  
Supervisory Development Associate in Cyber and IT Risk  
Surface Warfare Officer  
Systems Administrator  
Systems Analyst  
Systems Analyst/Developer  
Systems Consultant II  
Systems Design Engineer  
Systems Engineer  
Systems Integration Engineer  
Systems Integrator  
Systems Programmer II  
Systems Security Designer  
Systems Security Engineer  
Systems Security Researcher  
Systems Software Engineer  
Systems Support Specialist




Systems Support Specialist III  
Systems Vulnerability Analyst  
Systems Vulnerability Analyst  
Target Analyst  
Technical Analyst  
Technical Associate Staff  
Technical Information Security Officer  
Technical Intelligence Officer  
Technical Leader  
Technical Policy Fellow  
Technical Professional Staff  
Technical Program Management Officer  
Technical Project Manager  
Technical Specialist  
Technical Staff  
Technical Staff PDT Forensics  
Technology Analyst  
Technology Engineer

Technology Information Security Analyst  
Technology Security Designer  
Technology Vulnerability Analyst  
Telecommunications Specialist  
Test and Evaluation Specialist  
Threat Analyst  
Tier I Technician  
United States Air Force, Developmental Engineer,  
Project  
United States Navy Cryptologic Warfare Officer  
Vulnerability Analyst  
Vulnerability Management Assessment  
vulnerability researcher  
Vulnerability Specialist  
Vulnerability Team Member  
Wireless Communications Security Engineer  
Wireless Security Researcher

APPENDIX D: SAMPLE JOB DESCRIPTIONS

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.

 <h2 style="margin: 0;">ARMY POSITION DESCRIPTION</h2>		
<b>PD#:</b> DZ496020	<b>Sequence#:</b> 4149670	<b>Replaces PD#:</b>
<b>IT SPECIALIST (INFOSEC/NETWORK)</b> <b>GS-2210-07</b>		
<b>POSITION LOCATION:</b>  <b>Servicing CPAC:</b> FORT GORDON, GA <b>Agency:</b> ARMY <b>Installation:</b> DZ2AW6ZBAAA <b>Army Command:</b> US ARMY NETCOM HEADQUARTERS CYBER PROTECTION BRIGADE COMMAND SECTION FORT GORDON, GA 30905 A DZ2AW6ZBAAA  <b>Region:</b> SOUTH CENTRAL <b>Command Code:</b> 2A UNITED STATES ARMY CYBER COMMAND (ARCYBER)		
<b>POSITION CLASSIFICATION STANDARDS USED IN CLASSIFYING/GRADING POSITION:</b>  <b>Citation 1:</b> OPM JFS FOR ADMIN WORK IN INFOR TECH GRP, GS-2200, OCT 2018		
<b>Supervisory Certification:</b> <i>I certify that this is an accurate statement of the major duties and responsibilities of this position and its organizational relationships, and that the position is necessary to carry out Government functions for which I am responsible. This certification is made with the knowledge that this information is to be used for statutory purposes relating to appointment and payment of public funds, and that false or misleading statements may constitute violations of such statutes or their implementing regulations.</i>  <b>Supervisor's Name:</b> [REDACTED] <b>Date Certified:</b> 11/16/2017		
<b>Classification Review:</b> <i>This position has been classified/graded as required by Title 5, U.S. Code in conformance with standard published by the U.S. Office of Personnel Management or if no published standards apply directly, consistently with the most applicable published standards.</i>  <b>Classified By:</b> [REDACTED] <b>Date Classified:</b> 11/16/2017		
<b>Position Cursory Review:</b> <i>This position description (PD) has been reviewed and it is determined that: the major duties equal 100%; the statement Performs other duties as assigned (PODAA) is present; where applicable, the factors, levels, and points are identified</i>		

directly under PODAA, add up correctly, and the Point Range for the grade is present; and, the Conditions of Employment are properly identified in the Conditions of Employment & Notes section and at a minimum include Temporary Duty Travel (TDY) 25% or more (may be less if requested by management). The PD is in the format of the classification standard of record, and the standard(s) is/are cited properly, and the title/series/grade are properly determined based on the standard. The FLSA is correct and when it is determined that the position is Exempt, a complete explanation is provided, and all outdated/obsolete forms are removed. (All position descriptions require a cursory review upon initial verification in FASCLASS and may be reviewed again every 5 years thereafter, or before if OPM issues a new classification standard or guide).

**Reviewed By:**

**Date Reviewed:**

<p><b>POSITION INFORMATION:</b>  <b>Cyber Workforce:</b></p> <ul style="list-style-type: none"> <li>• <b>Primary Work Role:</b> 521</li> <li>• <b>Additional Work Role 1:</b></li> <li>• <b>Additional Work Role 2:</b></li> </ul> <p><b>FLSA:</b> NON-EXEMPT  <b>FLSA Worksheet:</b> NON EXEMPT  <b>FLSA Appeal:</b> NO  <b>Bus Code:</b> 8888  <b>DCIPS PD:</b> NO</p> <ul style="list-style-type: none"> <li>• <b>Mission Category:</b></li> <li>• <b>Work Category:</b></li> <li>• <b>Work Level:</b></li> </ul> <p><b>Acquisition Position:</b> NO</p> <ul style="list-style-type: none"> <li>• <b>CAP:</b></li> <li>• <b>Career Category:</b></li> <li>• <b>Career Level:</b></li> </ul> <p><b>Functional Code:</b> 00  <b>Interdisciplinary:</b> NO  <b>Supervisor Status:</b> Non-Supervisory  <b>PD Status:</b> VERIFIED  <b>DCA Override:</b> NO</p>	<p><b>CONDITION OF EMPLOYMENT:</b></p> <p><b>Drug Test Required:</b> POSN MAINTAINS TOP SECRET CLEAR REQUIRING DRUG TEST</p> <p><b>Financial Management Certification:</b></p> <p><b>Position Designation:</b> Tier 5 – Special Sensitive, Critical Sensitive, Noncritical Sensitive, High Risk</p> <p><b>Position Sensitivity:</b> SPECIAL SENSITIVE (SS) NATIONAL SECURITY RISK</p> <p><b>Security Access:</b></p> <p><b>Emergency Essential:</b> No [N: Position Not Designated Emergency-Essential Or Key]</p> <p><b>Requires Access to Firearms:</b> NO</p> <p><b>Personnel Reliability Position:</b> Not Valid PRP Code</p> <p><b>Information Assurance:</b> N</p> <p><b>Influenza Vaccination:</b></p> <p><b>Financial Disclosure:</b> NO</p> <p><b>Enterprise Position:</b></p>	<p><b>POSITION ASSIGNMENT:</b></p> <p><b>Competitive Area:</b> A1  <b>Competitive Level:</b> 0015  <b>Career Program:</b> 71  <b>Career Ladder PD:</b> YES  <b>Target Grade/FPL:</b> 12  <b>Career Pos 1:</b> <a href="#">DZ496019</a> GS-2210-05  <b>Career Pos 2:</b>  <b>Career Pos 3:</b> <a href="#">DZ496021</a> GS-2210-09  <b>Career Pos 4:</b> <a href="#">DZ496022</a> GS-2210-11  <b>Career Pos 5:</b> <a href="#">DZ475150</a> GS-2210-12  <b>Career Pos 6:</b> <a href="#">DZ475153</a> GS-2210-12</p>
--	---	---

**POSITION DUTIES:**

\*\*\*THIS IS A PATHWAYS POSITION\*\*\*

This position meets three or more CP-71 career program criteria as outlined by the Cyberspace Effects Career Management Office.

**STATEMENT OF DIFFERENCES**

This is a developmental position leading to either of the target positions, IT Specialist (INFOSEC/NETWORK), GS-2210-12 (SME), PD# DZ475153 or IT Specialist



(NETWORK/INFOSEC), GS-2210-12, PD# DZ475150. The next training level PD at the GS-2210-09 grade level is PD# DZ 496021 and the GS-2210-11 PD# is DZ 496022. The duties described within this document at the GS-07 grade level are similar to those of the target PDs, except that the incumbent does not have the requisite experience to perform all of the duties of the position without a greater degree of supervisory assistance and review as identified in the full performance GS-12 PDs. The incumbent may be promoted non-competitively to the next performance level in the progression to the target GS-12 PD provided: the work is at the higher level, the work continues to exist, the incumbent has demonstrated the ability to perform it, and the qualifications and other administrative requirements are met. The differences from the full performance GS-12 level are as follows.

US Army Cyber Protection Teams (CPTs) are new cyber units focused on Defensive Cyberspace Operations (DCO). The CPTs are divided into four mission areas: National, Department of Defense (DOD) Information Networks (DODIN), Combatant Command (CCMD) support, and Service support. All CPT units are focused on cyber actions internal to the defended network, which will be primarily within the DODIN unless they are separately authorized to defend non-DOD networks.

Serves as an Information Technology (IT) Specialist for a US Army Cyber Protection Team in the US Army Cyber Protection Brigade. May be assigned to a National, DoD Information Networks (DODIN), Combatant Command (CCMD) or Service team and may be rotated across any of several Cyber functions, including: inspection, operations support, threat mitigation, counter-infiltration, and cyber threat emulation. May perform a range of cyber tasks in support of the organization's mission, including support for military personnel engaged in network infrastructure activities, cyber operations planning, cyber operations execution, cyber threat analysis, and incident response.

#### MAJOR DUTIES:

1. Analyzes computer/network incidents following prescribed standard operating procedures relating to discovery/detection, isolation, recovery/remediation, and root cause analysis. Detects intrusions across multiple platforms to determine root cause and anticipate effects. Conducts research and apply new techniques to identify unanticipated threats. Identifies trends, establishes baselines, and detects anomalies in network and host data; often through novel approaches. Assists system technicians, managers, and other stake-holders for incident response actions. Monitors enterprise tools for indications of potential intrusions or violations of existing joint, Service specific, or Department of Defense (DoD) policies. 40%
2. Tests and maintains network infrastructure including software and hardware devices. Performs network monitoring and intrusion detection system tuning to identify and mitigate malware and threats; ensures sensors are optimized and functioning properly according to the operating environment. Employs programming and scripting as needed for scale and efficiency. Creates, edits, and manages changes to network and host access control lists (ACLs) on specialized Cyberspace Defense (CD) systems such as firewalls and intrusion prevention systems. Assists in identifying and evaluating network traffic baselines to facilitate the discovery of adverse network trends, anomalies, and malicious threats. Monitors and analyzes real time embedded sensors or unit provided packet captures, network traffic, connectivity, and performance. 40%
3. Installs, configures, troubleshoots, supports, and operates cyber security tools including but not limited to sensors and analysis tools such as Security Onion, McAfee Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), and Security Information and Event Management (SIEM), etc. Researches state-of-the-art capabilities for potential use in the defensive environment, including the option of developing custom



## JOB DESCRIPTION

*To perform this job successfully, an individual must be able to perform the essential job functions satisfactorily. Reasonable accommodations may be made to enable individuals with disabilities to perform the primary job functions herein described. Since every duty associated with this position may not be described herein, employees may be required to perform duties not specifically spelled out in the job description, but which may be reasonably considered to be incidental in the performing of their duties just as though they were actually written out in this job description.*

### IT SECURITY ANALYST

**Department/Division:** Fiscal and Administrative Services/Information Technology

**Pay Grade:** 117

**FLSA Status:** Exempt

**Telework Eligible:** Yes

**Reports To:** Information Security Officer

**Supervises:** None

#### JOB SUMMARY

Supports the development and deployment of enterprise-wide computing and information security requirements, policies, standards, guidelines, plans and procedures to ensure security of County systems. Works with the Information Security Officer to identify security solutions and implement a multi-layered defense to protect County networks. Monitors County networks, systems and data and responds to intrusions. Overall goals are set and the worker determines the specific tasks and assignments to be performed, independently handling new and unusual problems and deviations encountered in the work.

#### ESSENTIAL JOB FUNCTIONS

- Supports the planning, design, implementation, and testing of information security controls protecting County information systems from attacks.
- Configures, manages, maintains, and troubleshoots information security technology controls.
- Monitors County information systems for vulnerabilities and security breaches.
- Performs incident response activities for information system intrusions and other data breaches.
- Consults with vendors and service providers regarding information security technology solutions; evaluates and recommends solutions.
- Maintains current knowledge of cyber threats, security issues and security requirements.
- Supports the risk assessment and evaluation of County information systems.

- Participates in security policy assessments and audits.
- Trains County and other agency employees on IT security related issues to increase awareness of the growing threat to system security with the goal being to keep County systems and data secure.
- Works closely with Information Security Officer in identifying security issues and implementing solutions.
- Performs related work as required.

### QUALIFICATIONS

#### **Education and Experience:**

Bachelor's degree in IT, Cyber Security, or related field. Seven (4) years of networking systems or cyber security, or an equivalent combination of education, experience, and training.

#### **Licenses or Certifications:**

CompTIA Security Plus Certification

#### **Special Requirements/Qualifications:**

Work is subject to frequent interruptions and occasional work beyond the normal scheduled hours of operation.

#### **Knowledge, Skills and Abilities:**

- Knowledge of Information Security concepts, best practices, and threats
- Knowledge of Information Security controls
- Knowledge of legal issues, privacy, and ethics as it relates to IT Security
- Knowledge of a wide range of computer systems and security tools
- Knowledge of network infrastructure
- Ability to maintain knowledge of current information security best practices and threats
- Ability to install, maintain, and troubleshoot IT security appliances such as firewalls, email and web filters, and VPN appliances
- Ability to understand and secure wireless, telework, and BYOD networking infrastructure
- Ability to manage training programs related to information security awareness efforts
- Ability to collect, manage, and generate reports from data related to risk or vulnerability assessments
- Ability to create scripts or simple programs to automate repetitive or reoccurring tasks
- Ability to communicate effectively orally and in writing
- Ability to establish and maintain effective working relationships with others encountered in the workplace

### PHYSICAL DEMANDS

The work is mostly sedentary with frequent periods of walking and standing. Typical positions require workers to lift and carry up to 30 pounds; climb stairs; bend and crouch; reach, hold, grasp, and turn objects; and use fingers to operate computer or typewriter keyboards. The work requires the ability to speak normally, to use normal or aided vision and hearing and to detect odors.



**CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY  
IT SPECIALIST (INFOSEC)  
GS-2210-09**

## **I. INTRODUCTION**

This position is located in various Department of Homeland Security (DHS Cybersecurity and Infrastructure Security Agency (CISA). CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating with industry to build more secure and resilient infrastructure for the future. CISA works with partners across industry and government to understand and manage risk to our critical infrastructure from a constantly evolving range of cyber and physical threats. CISA accomplishes its mission through five key functions:

- National Risk Management
- Infrastructure and Cybersecurity Operations
- Critical Infrastructure Resilience
- Federal Information Security
- Interoperable Emergency Communications

## **II. MAJOR DUTIES and RESPONSIBILITIES**

Implements security requirements such as those resulting from laws, regulations or Presidential directives. Integrates security programs across disciplines; defines the scope and level of detail for security plans and policies; applicable to the security program. Assess new systems design methodologies to improve software quality; implementation activities. Ensure awareness and compliance. Identifies need for changes based on new security technologies or threats. **(45%)**

Conducts risk and vulnerability assessments of planned and installed information systems and the broader IT industry to identify vulnerability, risks and protection needs of activities. **(45%)**

Promotes Departmental awareness of security issues and ensures sound security principles and policies are reflected in organizational goals and objectives. Provides technical advice and guidance to Department managers and other technical specialists on significant information security problems and issues. Ensures integration of security programs with other IT programs and services in DHS. **(10%)**

**Performs other duties as assigned.**

## Position Description

AC#: 1000000010243

Preparation Date: 05/03/2021

Incumbent Name: [REDACTED]

FLSA: Exempt

Career Path: ZP

Series: 1550

Band: 03

Title: Computer Scientist

Function: 11 Research

Cybersecurity:

111 All-Source Analyst - All-Source Analysis

### Principal Objective:

Participate in development of Lightweight Cryptography standards. Conduct research in cryptography applications and cybersecurity. Participate in industry and international standards activities. Develop NIST guidelines in network and wireless security.

### Series Definition:

Performs professional research or development work to develop new methods and techniques to store, manipulate, transform, or present information by means of digital computer systems; includes work in the development of new fields of computer science research or on problems arising from use of digital computers. Requires professional competence in the theoretical foundations of computer science, computer design and applications, mathematics, and statistics.

### General Duties and Responsibilities:

Plans and carries out difficult and complex assignments in a scientific, engineering, mathematics or information technology discipline with limited supervision. Develops new methods, approaches, and procedures usually in cooperation with coworkers or advisors. Works with peers and others to develop resolutions to complex or challenging issues and provide recommendations for improvements in order to meet program objectives. Completed work is expected to have a sound overall approach and effectively meet stated requirements. Work impacts the technical planning, completion, and direction of major scientific, mathematical, engineering, or information technology projects.

### Knowledge, Skills, and Abilities:

Advance knowledge and skill in applying theories, principles, and methods of a technical professional field (in science, engineering, information technology, or mathematics) and of a specialty within that field. Ability to define problems, perform background research, develop and execute a project plan, organize and evaluate results, and prepare reports of findings. Ability to consider precedents and use judgment to research, select, interpret, modify, adapt, and apply available guidelines to specific problems or issues. Ability to present ideas and results in a clear, compelling and persuasive manner.

**Incumbent's Supervisory Responsibilities:**

No supervisory responsibilities

**Specialty Descriptor:**

055075 Computer Science - Cryptography

Conducts research and development of new and advanced methods and techniques for implementing cryptographic security functions and protocols, including secret key and public key cryptographic algorithms, cryptographic modes of operation, cryptographic key management techniques, and network (and LAN) security techniques and protocols.

055080 Computer Science - Cryptology

Performs research in the application of cryptography for the protection of computer systems, including development, application, analysis, and testing of cryptographic systems that prevent unauthorized disclosure of data, detect unauthorized modification of data, and control access to computer systems; provides for electronic certification of data; implements cryptography in communications protocols; develops cryptographic security standards for government and commercial use; instructs others on the proper application of cryptographic techniques.

**Position-Specific Key Phrases:**

Cryptography, Network security, Standards

**Position Requirements:**

- This position is telework eligible.

**Position Sensitivity:**

This is a Low Risk - ADP position.



## Summary

Identifies, assesses, neutralizes, exploits, detects, and/or defends against of cyber system vulnerabilities, risks, and resulting physical or mission impacts. Contributes to creating intelligence, analysis, or operational products and performing cyber analysis necessary to increase understanding of computer network operations, programs, and capabilities. Incorporates technical knowledge of classic and contemporary cyber threats and vulnerabilities into system engineering, analytics, or operations. Collaborates with other cyber security and information technology experts throughout the Department of Energy complex and intelligence communities across the United States.

## Job Duties

1. Safety and security are a primary responsibility for all Laboratory employees. Maintains required safety and security training, assures safety and security compliance, and makes safety and security an integral part of every task, including taking the necessary steps to stop work if continuing the job is unsafe or compromises security.
2. Performs identification, monitoring, detection, analysis, exploitation and/or mitigation of moderately complex computer and network security vulnerabilities, incidents, and suspicious activity.
3. Evaluates new tools, researches exploitation methods and techniques, and proposes effective solutions to cyber security issues.
4. Develops and implements metrics, analyzes data for new and unusual features, and manipulates raw data when needed to gather information.
5. Contributes to the design, development, modification, and debugging of cyber protection and/or analysis software tools in an effective manner, using judgement and creativity in applying defined practices and procedures that leads to technical decisions including selections and adaptations of technical alternatives, for assigned work.
6. Contributes to automating the implementation, configuration and maintenance of NIST related standards and controls for networks and systems.
7. Works on complex issues requiring analysis of situations, alternatives, or data. Exercises sound judgement in selecting methods, techniques and evaluation criteria for obtaining results.
8. Contributes to the development and presentation of technical reports and briefings on moderately complex system vulnerabilities to convey risks, impacts and recommendations to senior management and/or external personnel.
9. Contributes to resolving typical cyber issues, providing guidance as appropriate to other cyber security personnel.
10. Contributes to establishing direction and milestones for well-defined tasks involving more than one person. Scopes tasks within a project and defines deliverables at a task level within the approved scope, schedule, and budget. Small to moderate projects may involve more than one capability and organization.
11. Researches, assembles, and/or evaluates information or data regarding industry practices or applicable regulatory changes affecting *cyber security* policies or programs; recommends sound, practical solutions to complex issues.
12. Understands and adheres to all Laboratory and industry regulatory guidance and governance specific to *cyber security*.
13. Ensures all results, processes, and final products meet quality specifications and are completed according to established requirements.
14. Fosters a mutually respectful work environment that is free from discrimination and harassment.

Dakota State University invites applicants at all levels for multiple full-time openings as a Research Engineer.

These positions are 12 month, full-time, and benefit-eligible. The positions will report to the lab director. Upper level placements will supervise teams of 8-10 in addition to student researchers.

### **Responsibilities**

- Review, isolate, analyze, and reverse engineer software programs.
- Document the specific capabilities of the specimen (code, virus, etc.) and understand the concept of exploitation scenario.
- Create a detailed technical report including proof-of-concept exploit code.
- Stay on top of the "vulnerability landscape" and be up-to-date on current attacks or potential attacks and prepare counter-measures (if possible) to thwart those attacks.
- Analyze common network services and software applications in order to discover new and potential vulnerabilities.
- Strong understanding of low-level computer fundamentals, assembler and processor architecture, and experience with C, C++ and assembly programming.
- Relevant experience involving WinDbg or OllyDbg, BinDiff, IDA Pro, and Ghidra.
- In-depth knowledge of TCP/IP.
- Desire to perform cyber security research on real-world software.
- Activities will include vulnerability assessment (source code auditing, fuzzing, etc), reverse engineering (static and dynamic analysis) and exploit development. Malware analysis will also be covered.

### **Minimum Qualification**

- Bachelor's degree in a technical field such as cyber operations, computer science, network security, computer engineering or similar field with demonstrated technical acumen and interest.
- Ability to obtain and maintain TS/SCI FS+ clearance. Preference will be given to candidates that currently hold this clearance.

### **Preferred Qualifications**

- Master's degree in a technical field such as cyber operations, computer science, network security, computer engineering

### **These positions are contingent on grant funding**

DSU accepts applications through an on-line employment site. To apply, visit <https://yourfuture.sdbor.edu>. The employment site will allow the attachment of a cover letter, resume, transcripts, and a minimum of three supporting references which include email addresses and telephone numbers.

For questions concerning the position, send emails [REDACTED] Review of applications will begin immediately and will continue until the positions are filled.

## Vacancy Position

### Vacancy Information

Vacancy Announcement: 2019-HQRG-B0362

Position Title: Information Technology Cyber Risk Management Analyst, CG-2210-07

Series: 2210

Grade: 07

Location(s): Salt Lake City, UT, US

### Job Summary

These positions are located in the Division of Risk Management Supervision of the Federal Deposit Insurance Corporation at various field offices and will perform administrative, technical, and analytical support to the examination staff conducting the IT portion of risk-based bank examination, or IT examinations of Bank service providers. Additional selections may be made from this vacancy announcement to fill identical vacancies that occur subsequent to this announcement.

### Major Duties of ITCA in FDIC

Information Technology Cyber Risk Management Analysts perform developmental assignments and receive on-the-job training to perform progressively more difficult analysis and examination duties to include the following:

- Evaluates and assesses an institution's processes to assure that existing and new IT systems meet the institution's cybersecurity and operational risk requirements.
- Identifies and reports unusual transactions, irregularities, weaknesses or deficiencies to the senior specialists, analysts, or examiners.
- Presents findings and recommendations to higher graded analysts and examiners, and to institution management.
- Makes adjustments and recommendations as necessary.
- Conducts meetings with financial institution management to recommend corrective action for deficiencies.
- Performs work assignments and completes projects in a team environment.



## JOB DESCRIPTION

### Cyber Security Researcher - (15519)

#### Description

Does a career focused on changing the world's energy future intrigue you? If so, we might have just the opportunity you're looking for!

Idaho National Laboratory's (INL) Cybercore group is seeking forward-thinking professionals interested in exploring a technical career as a Cyber Security Researcher.

The Cyber Security Researcher will support the National and Homeland Security Directorate with engineering, reverse engineering, development and maintenance of custom code used to analyze security vulnerabilities/network traffic in specialized systems and proprietary protocols.

#### Responsibilities Include:

- Participates in support of operations and personnel at government and WFO locations, conducts research, monitoring and analysis of current and emerging threats directed at network infrastructure targets from both internal and external sources. Understands and documents topologies for intricate security relationships, and makes security architecture recommendations that will improve security programs/posture.
- Develops attack and defense methodology and code on high risk computer networks.
- Develops technical solutions for information operations and analysis related to national security topics, intrusion analysis, systems and vulnerabilities, network security, advanced analytic tools and data visualization techniques. Works with peers and mentors/develops as a junior engineer to identify security issues of existing platforms and applications.
- Develops algorithms and methods for detecting and preventing network attacks. Develops and maintains code to find weaknesses in systems and to verify patch effectiveness. Assists and/or conducts penetration testing and vulnerability assessments. Performs analysis and/or reverse engineering of suspect source code. Writes scripts and develops software utilities to automate security analysis efforts.
- Works with customers as part of a team to develop requirements, produce/test code, and provide necessary documentation. Participates in project teams to produce proposals for new work including joint projects with industry. Provides a positive and effective customer interface. Effective communication skills (verbal, written) are also required.
- Participates in the development of significant new concepts or novel approaches to Cyber Security.

#### Minimum Requirements:

- **LEVEL 1: BACHELOR'S DEGREE**
- Must be a US citizen and have the ability and willingness to obtain and maintain a "Q" clearance with appropriate sigmas and SCI clearance.

#### Preferred Requirements:

- Outstanding C programming skills with an ability to code in assembly as necessary.
- Strong understanding of Linux, Solaris, and Windows based operating systems and development tool-sets.
- Strong background in searching and sorting algorithms, decision trees, and/or memory management.
- Familiarity with Zero Day exploits.
- Familiarity with packet level programming.
- Strong personal (hobby) interest in computers, computer and system security and programming as well as academic training.

#### Job Information

- Salary Grade: 210
- Multi-Level: This is a multi-level posting and the selected candidate will be placed at the appropriate level dependent on depth and breadth of proven experience and skills

#### INL Overview:

INL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's mission in nuclear energy research, science, and national defense. With more than 5,000 scientists, researchers, and support staff, the laboratory works with national and international governments, universities and industry partners to discover new science and development technologies that underpin the nation's nuclear and renewable energy, national security, and environmental missions.

#### INL Mission:

Our mission is to discover, demonstrate and secure innovative nuclear energy solutions, other clean energy options and critical infrastructure.

#### INL Vision:

Our vision is to change the world's energy future and secure our nation's critical infrastructure.

#### Selective Service Requirements:

To be eligible for employment at INL males born after December 31, 1959 must have registered with the Selective Service System (SSS). For more information see [www.sss.gov](http://www.sss.gov).

#### Equal Employment Opportunity:

Idaho National Laboratory (INL) is an Equal Employment Opportunity (EEO) employer. It is the policy of INL to provide equal employment opportunities to all qualified applicants without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, protected veteran or disabled status, or genetic information. Women and People of Color are strongly encouraged to apply.

#### Other Information:



**Qualifications**

**Primary Location** United States  
**Job** Computer Information Technology  
**Organization** National & Homeland Security (Dxxx)  
**Schedule** Full-time  
**Employee Status** Regular  
**Posting Date** Jan 7, 2021  
**Unposting Date** Ongoing



INL is operated for the Department of Energy by Battelle Energy Alliance

[DOE OFFICE OF NUCLEAR ENERGY](#)  
[DOE IDAHO OFFICE](#)  
[BATTELLE](#)

1955 N. Fremont Ave. Idaho Falls, ID 83415  
Idaho National Laboratory

866-495-7440

[EQUAL OPPORTUNITY](#)  
[EMPLOYER PRIVACY/ACCESSIBILITY](#)

**RESEARCH AREAS**

Nuclear Energy  
Energy & Environment  
National & Homeland Security

**ABOUT US**

General Information  
Capabilities of Idaho National Laboratory  
Center for Advanced Energy Studies (CAES)  
Environment, Safety, Health  
Visitors  
Contact Info  
Bus Operations

**PARTNER WITH INL**

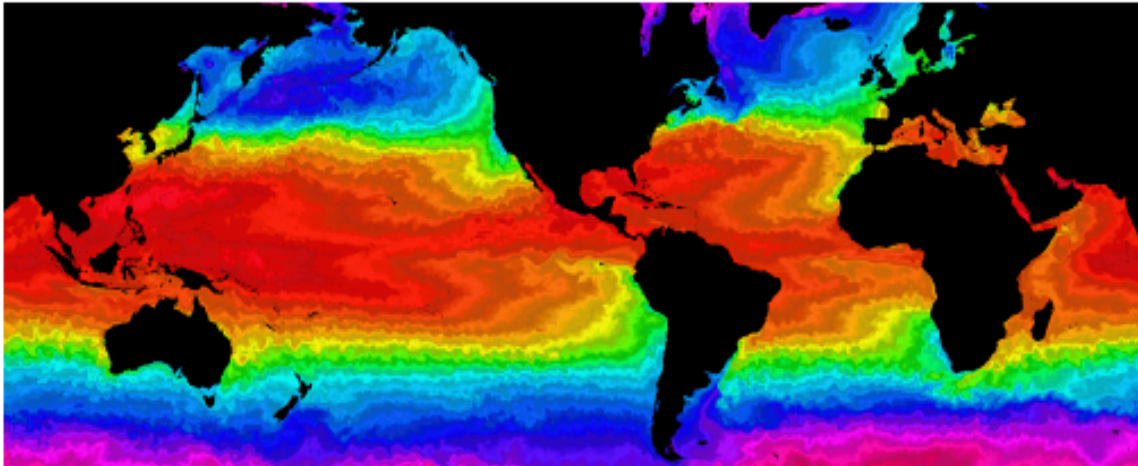
University Partnerships  
User Facilities  
Community & Education Outreach  
Industry & Tech Deployment  
Economic & Workforce Development  
Initiating Business with INL

**CAREERS**

Retirees

**NEWSROOM**

News  
Fact Sheets  
INL Publications



## DEPARTMENT OF NAVY CAREER OPPORTUNITIES

### Solicitation of Applicants for Positions in Cybersecurity Flyer #20-002

*How to apply:* The Naval Oceanographic Office will accept resumes through June 30<sup>th</sup>, 2020 to fill multiple vacancies for entry-level positions involving cybersecurity including positions in the Information Technology, Computer Scientist, and Telecommunications fields. Resumes and transcripts should be submitted by email to [NAVO\\_STNS\\_JOBS@navy.mil](mailto:NAVO_STNS_JOBS@navy.mil) and reference the Flyer # above in the Subject Line of the email. Unofficial versions of transcripts are acceptable provided they list all coursework, credit hours completed, and the student's name. Cover letters are not required, but are encouraged. Highly qualified applicants will be contacted via email to schedule a job interview.

**Salary Range:** \$34,916 to \$77,111 per Annum  
**Job Location:** Stennis Space Center, MS

*About the Job:* Successful candidates will be employed by either the Naval Oceanographic Office (NAVOCEANO) or the Fleet Survey Team (FST) stationed at Stennis Space Center, MS. NAVOCEANO is the Navy's premiere center for operational oceanography. FST conducts hydrographic surveys and related environmental assessments to enable safe and effective maritime navigation and access to the littoral for Naval and Joint Forces.

These positions offer abundant opportunities for professional growth while you work as part of a highly skilled team in applying a wide range of expertise to secure, defend, and preserve data, networks, netcentric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defensive actions in support of the Naval Meteorology and Oceanography Community and Naval operations.

Highly qualified candidates will demonstrate a strong ability to perform the following required tasks:

- Skills and abilities in systems administration including the installation, configuration, security, and reliable operations of operating systems such as Microsoft Windows and Red Hat Enterprise Linux (RHEL) servers and desktops.
- Skills and abilities in cyber security to plan, coordinate, synchronize, and conduct activities to defend information networks, including but not limited to, vulnerability management, compliance, and customer support.
- Skills and abilities in database administration including physical database design, security, and performance of databases such as Oracle and PostgreSQL.
- Skills and abilities in middleware administration including installation, configuration, security and reliable operations of applications such as JBoss Enterprise Application Platform (EAP), Apache HTTP, ESRI ArcGIS Enterprise, and Microsoft IIS.
- Skills and abilities in configuration management including establishing and maintaining the consistency of systems and software performance, functionality, and physical attributes with requirements, design, and operational information.

- Skills and abilities to conduct DoD cryptographic support operations and management (COMSEC) and / or provide customer service supporting telecommunications, server-based information distribution, and telephony, satellite requirements through contracts.
- Skills and abilities in network services and operations including LAN/WAN switching and routing technologies, firewalls, and other cyber security appliances.
- Skills and abilities in software development to plan, design, develop, test, configure, integrate, document and maintain quality software solutions that are cybersecure and satisfy organization software requirements.

**Basic Requirements:** Appointments to Federal positions will be made at the GS-05, GS-07, or GS-09 level and have a full performance level of GS-11. Opportunities are available for applicants who meet the basic qualification requirements outlined below in the following fields:

- **Information Technology (2210)** – Bachelor’s degree in any field or experience demonstrated by paid or unpaid experience and/or completion of specific, intensive training (for example, certification), as appropriate. In addition, individuals must demonstrate they have experience in each of the following four competencies (not necessarily IT-related; 1) Attention to detail, 2) Customer Service, 3) Oral Communication, and 4) Problem Solving
- **Computer Scientist (1550)** - Degree in computer science or bachelor’s degree with at least 30 semester hours in mathematics, statistics, and computer science. At least 15 of the 30 semester hours must have included any combination of statistics and mathematics that included differential and integral calculus.
- **Telecommunications (0391)** - Undergraduate and Graduate Education: Major study -- electrical or electronic engineering, mathematics, physics, public utilities, statistics, computer science, telecommunications management, information systems management, business administration, industrial management, or other fields related to the position to be filled; or

Other Education: Communications/electronics or automatic data processing training in technical institutes or business schools above the high school level or in Armed Forces schools that included advanced instruction in addition to basic courses, may be substituted for general experience on a month-for-month basis; or

Experience that provided a basic knowledge of telecommunications functions, problems, and/or solutions; or

Specialized Experience in evaluating, analyzing, developing, managing, or improving communications systems, procedures, and requirements that demonstrated knowledge of current developments and trends in communications concepts and technology.

**General and Career Information:** Starting salaries are commensurate with education and experience, plus full benefits. Applicants must be U.S. citizens. Males born after December 31, 1959 are required to be registered with the Selective Service System. All positions are subject to satisfactory completion of a security investigation, successful completion of a pre-employment physical, and/or drug test.

Visit our Facebook pages for more information on NAVOCEANO and FST.



**THE DEPARTMENT OF NAVY IS AN EQUAL OPPORTUNITY EMPLOYER.**



NSA Cybersecurity mission is to prevent and eradicate threats to National Security Systems and critical infrastructure, with a focus on the Defense Industrial Base. This diverse team of problem solvers collaborate across industry and government to expose foreign cyber espionage, patch critical vulnerabilities, modernize encryption, and issue unique, timely, and actionable cybersecurity guidance. Here, you will have unique access to classified and unclassified data to solve hard problems and secure critical systems. If you enjoy creatively mission outcomes, cybersecurity at NSA is the place for you.

Information System Security Professionals play a vital role in enabling security solutions by utilizing systems engineering and systems security engineering principles in:

- defining information system security requirements and functionality
- designing system architectures
- developing security designs
- assessing the effectiveness of security solutions against present and projected threats
- producing formal and informal reports, briefings, and direct input to the customer regarding security and functionality requirements, system architecture and security designs

Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program.

The Cybersecurity Engineering Development Program is a 3 year program. To meet the Agency's evolving mission, NSA's core discipline of Information System Security and Cryptographic Engineering must remain strong and agile. Information System Security and Cryptographic Engineering integrates computer science, engineering and mathematics along with Information Assurance/Cybersecurity Analysis skills, so that the Agency can define the standards for high-assurance as the trusted authority for National Security System (NSS) communications. Our nation's security will be determined by NSA's ability to develop experts in these skills, in order to keep pace with the complex and powerful threats introduced by our adversaries. No academic course of study or university program provides the necessary depth of skills and practical hands-on experience required by the Agency, thus the Cybersecurity Engineering Development Program is the only program in the US government designed to develop and advance the core skillset essential to protecting the US's national security systems.

**Agency:** Diplomatic Security Service, Department of State

**Position:** Special Agent (Criminal Investigator). FS 2501/CS 1811 (Foreign Service pay scale is equivalent to the Civil Service/General Schedule pay scale)

**Summary of duties:**

- Conducting investigations, to include criminal investigations, criminal investigations with a cyber component, counterintelligence and counterterrorism inquiries, and investigative work preparing for court appearances, and testifying in court and other legal proceedings.
- For investigations with a cyber component, investigating complex leads on internet-based visa and passport fraud scams, email threats, and performing internet-based cyber investigations.
- Working with law enforcement and Intelligence Community partners on joint criminal investigations regarding threats (to include cyber) against the Department of States.
- Conducting protective security services for the Secretary of State, other U.S. government officials, and visiting foreign dignitaries (similarly to United States Secret Service Special Agents).
- When posted overseas, managing the Bureau of Diplomatic Security's many local security programs, to include cyber security, electronic countermeasures and surveillance, and acting as a point of contact between the Embassy and HQ.
- Conducting and implementing programs involved with safeguarding classified and sensitive information and materials (to include policies to protect the Department of State's cyber and Information Technology resources), as derived from Presidential Directives or Executive Orders.
- Assessing physical security and cyber threats against U.S. interests, properties, Information Technology systems, and other diplomatic installations and personnel abroad, as well as investigating actual or potential hostile intelligence attempts to subvert U.S. personnel and interests overseas.

## JOB SPECIFICATIONS

[Back to Job Specifications List \(https://humanresources.vermont.gov/classification-position-management/classification/job-specifications?jobcode=&letter=&paygrade=&keyword=Security+Analyst&result=Search\)](https://humanresources.vermont.gov/classification-position-management/classification/job-specifications?jobcode=&letter=&paygrade=&keyword=Security+Analyst&result=Search)

### Information Security Analyst I

**Job Code:** 630300

**Pay Plan:** Classified

**Pay Grade:** 24

**Occupational Category:** Information Technology & Statistics

**Effective Date:** 11/24/2014

#### Class Definition:

Incumbents in this class are responsible for technical, compliance, and governance work in one or more areas of information security. Works in collaboration with more experienced staff members as well as Information Technology (IT) and business decision makers to coordinate, plan, design, integrate and audit security capabilities and optimize security of information systems and services for the State of Vermont.

#### Examples of Work:

Analyze and respond to security events/incidents, threats, vulnerabilities, and risks; technical troubleshooting; technical operation of security infrastructure; Response, tracking, and remediation of audits; security posture reviews; security governance; technical tool operation; disaster recovery (DR) and business continuity (BC); oversight of technical/compliance infrastructure; on-call and off- hours management of security infrastructure and create associated documentation. Perform related

duties as required.

**Environmental Factors:**

Work is performed in a standard office setting, but some travel may be required for which private means of transportation should be available. Work outside of regular business hours is expected.

**Knowledge, Skills and Abilities:**

Ability to consume technical details quickly and accurately.

Knowledge of industry accepted (best practice) information security principles and practices.

Advanced understanding in at least one domain of security. Domains listed for reference: Access Control, Telecommunications and Network Security, Information Security Governance and Risk Management, Software Development Security, Cryptography, Security Architecture and Design, Operations Security, Business Continuity and Disaster Recovery, Legal/Regulations/Investigations/Compliance, and Physical (Environmental Security).

A background in one or more areas of IT operations, security, or other auditing/compliance related field.

A basic understanding of how regulations impact data protection mechanisms/schemes and general understanding of security controls that can be applied to help mitigate risks to the environment.

Foundational knowledge of security standards and regulations (including but not limited to NIST security standards, HIPAA/HITECH, and IRS 1075).

Strong oral and written communication skills as well as negotiation and conflict management abilities.

Must communicate effectively with technical and non-technical staff, consultants and vendors.

Ability to establish and maintain effective working relationships.

**Minimum Qualifications** Bachelor's degree in computer science, programming, or engineering



## APPENDIX E: STUDENTS RELEASED FROM OBLIGATIONS

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

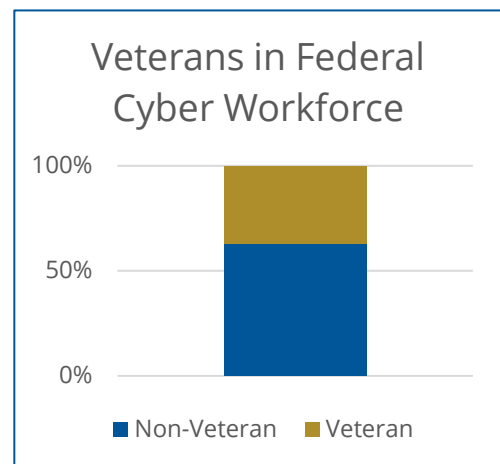
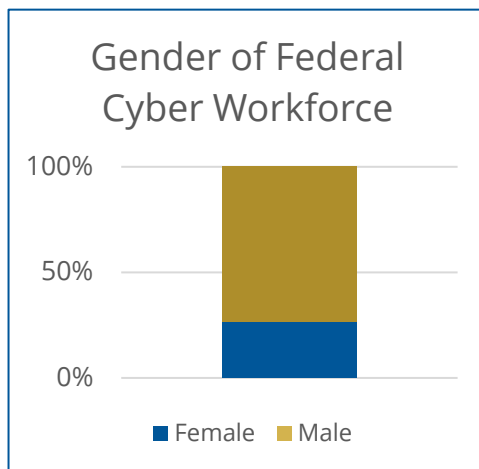
Source: SFS Master Roster and Placement Log as of 11/1/2021

Year	Scholarships Awarded	Full Waiver: Academic Phase	Partial Waiver: Academic Phase	Full Waiver: Employment Phase	Partial Waiver: Employment Phase	Waiver Request Pending Decision	Total Waivers
2001	31	0	0	6	0	0	<b>6</b>
2002	115	2	0	16	0	0	<b>18</b>
2003	219	1	0	16	0	0	<b>17</b>
2004	185	0	0	3	0	0	<b>3</b>
2005	182	4	0	2	0	0	<b>6</b>
2006	133	1	0	0	0	0	<b>1</b>
2007	111	1	0	0	0	0	<b>1</b>
2008	94	0	0	0	0	0	<b>0</b>
2009	133	4	0	1	0	0	<b>5</b>
2010	181	2	0	1	0	0	<b>3</b>
2011	195	2	0	1	0	1	<b>4</b>
2012	186	2	0	0	0	0	<b>2</b>
2013	268	1	0	1	0	0	<b>2</b>
2014	277	0	0	2	0	1	<b>3</b>
2015	277	0	0	0	0	0	<b>0</b>
2016	313	0	0	0	0	3	<b>3</b>
2017	357	0	0	0	2	0	<b>2</b>
2018	339	0	0	0	1	1	<b>2</b>
2019	384	1	0	0	0	1	<b>2</b>
2020	375	0	0	0	0	0	<b>0</b>
2021	354	0	0	0	0	0	<b>0</b>
<b>Total</b>	<b>4709</b>	<b>21</b>	<b>0</b>	<b>49</b>	<b>3</b>	<b>7</b>	<b>80</b>

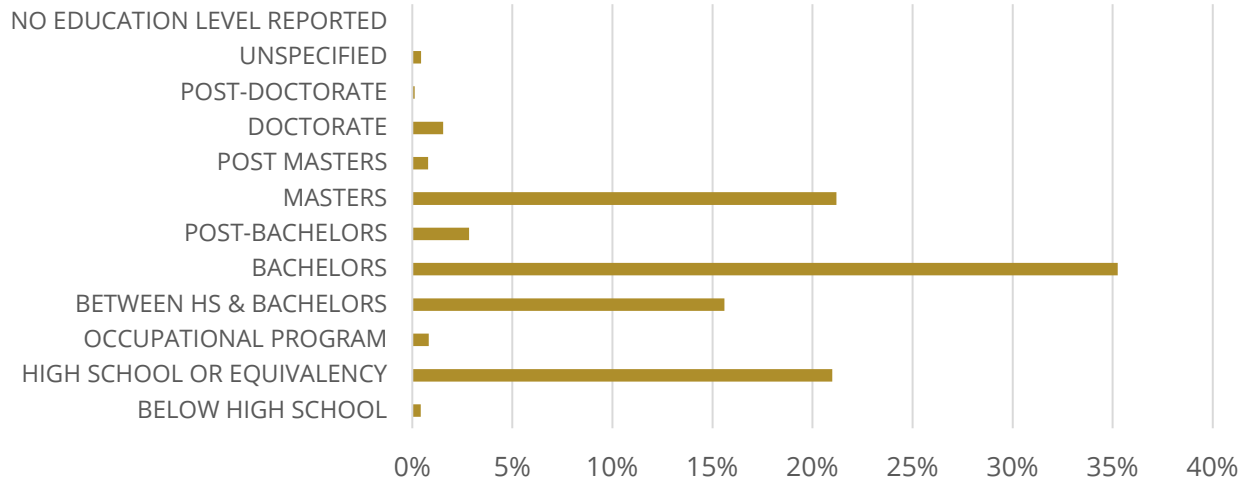
## APPENDIX F: FEDERAL CYBERSECURITY WORKFORCE STATISTICS

OPM's Enterprise Human Resources Integration (EHRI) system is the source of the following data. EHRI contains Government-wide personnel data on Executive Branch agencies, excluding agencies within the Intelligence Community.

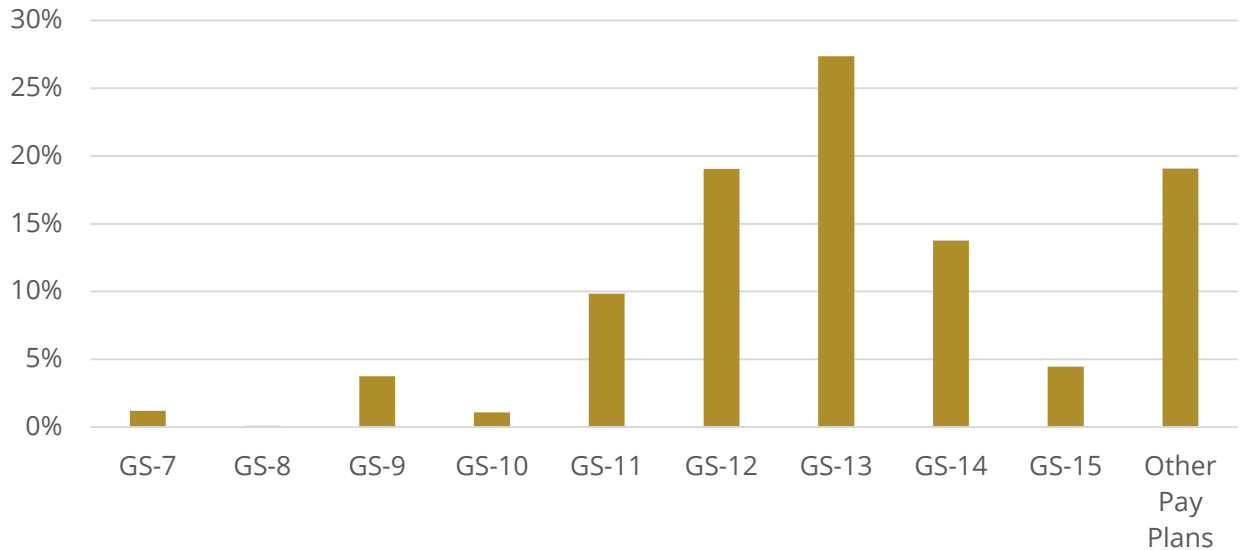
Federal Cyber Workforce (as of June 2021)	
<b>Average Salary</b>	\$112,677 per annum
<b>Average Age</b>	48.4 years of age
<b>Average Length of Service</b>	13.9 years of service



## Education Level of Federal Cyber Workforce



## Grade Levels of Federal Cyber Workforce



**Alabama**

Auburn University  
 Tuskegee University  
 University of Alabama - Tuscaloosa  
 University of Alabama at Birmingham (UAB)  
 University of Alabama in Huntsville  
 University of South Alabama

**Arizona**

Arizona State University  
 University of Arizona

**Arkansas**

University of Arkansas

**California**

Cal Poly Pomona  
 California State University - Sacramento  
 California State University - San Bernardino  
 Naval Postgraduate School

**Colorado**

University of Colorado - Colorado Springs

**Connecticut**

University of New Haven

**District of Columbia**

George Washington University  
 Georgetown University

**Florida**

Florida International University  
 Florida State University  
 University of Central Florida  
 University of Florida  
 University of West Florida

**Georgia**

Augusta University  
Georgia Institute of Technology

**Hawaii**

University of Hawaii at Manoa

**Idaho**

Idaho State University  
University of Idaho

**Illinois**

Moraine Valley Community College \*  
University of Illinois at Urbana Champaign

**Indiana**

Indiana University  
Purdue University Northwest

**Iowa**

Iowa State University

**Kansas**

Kansas State University  
University of Kansas

**Louisiana**

Louisiana State University  
Louisiana Tech University

**Maryland**

Anne Arundel Community College  
Johns Hopkins University  
Morgan State University  
Towson University  
University of Maryland, Baltimore County (UMBC)  
University of Maryland, College Park

**Massachusetts**

Northeastern University  
University of Massachusetts Amherst  
Worcester Polytechnic Institute

**Michigan**

Davenport University  
Michigan Technological University

**Minnesota**

St. Cloud State University

**Mississippi**

Mississippi State University

**Missouri**

University of Missouri-Columbia/Missouri University  
of S&T

**Nebraska**

University of Nebraska at Omaha

**New Jersey**

Brookdale Community College  
New Jersey Institute of Technology  
Stevens Institute of Technology

**New Mexico**

New Mexico Institute of Mining and Technology  
University of New Mexico

**New York**

New York University  
Pace University  
Rochester Institute of Technology  
University at Buffalo, SUNY

**North Carolina**

North Carolina Agriculture and Technical State  
University  
North Carolina State University  
University of North Carolina at Charlotte

**Ohio**

Clark State Community College  
Sinclair Community College  
University of Cincinnati

**Oklahoma**

Oklahoma City Community College  
University of Tulsa

**Pennsylvania**

Carnegie Mellon  
Drexel University  
Pennsylvania State University

**Puerto Rico**

Polytechnic University of Puerto Rico

**Rhode Island**

University of Rhode Island

**South Carolina**

Citadel

**South Dakota**

Dakota State University

**Tennessee**

Tennessee Tech University  
University of Tennessee at Chattanooga

**Texas**

San Antonio College  
Texas A&M University  
University of Houston  
University of North Texas  
University of Texas at Dallas  
University of Texas at El Paso  
University of Texas at San Antonio

**Vermont**

Norwich University

**Virginia**

Hampton University  
Marymount University  
Norfolk State University



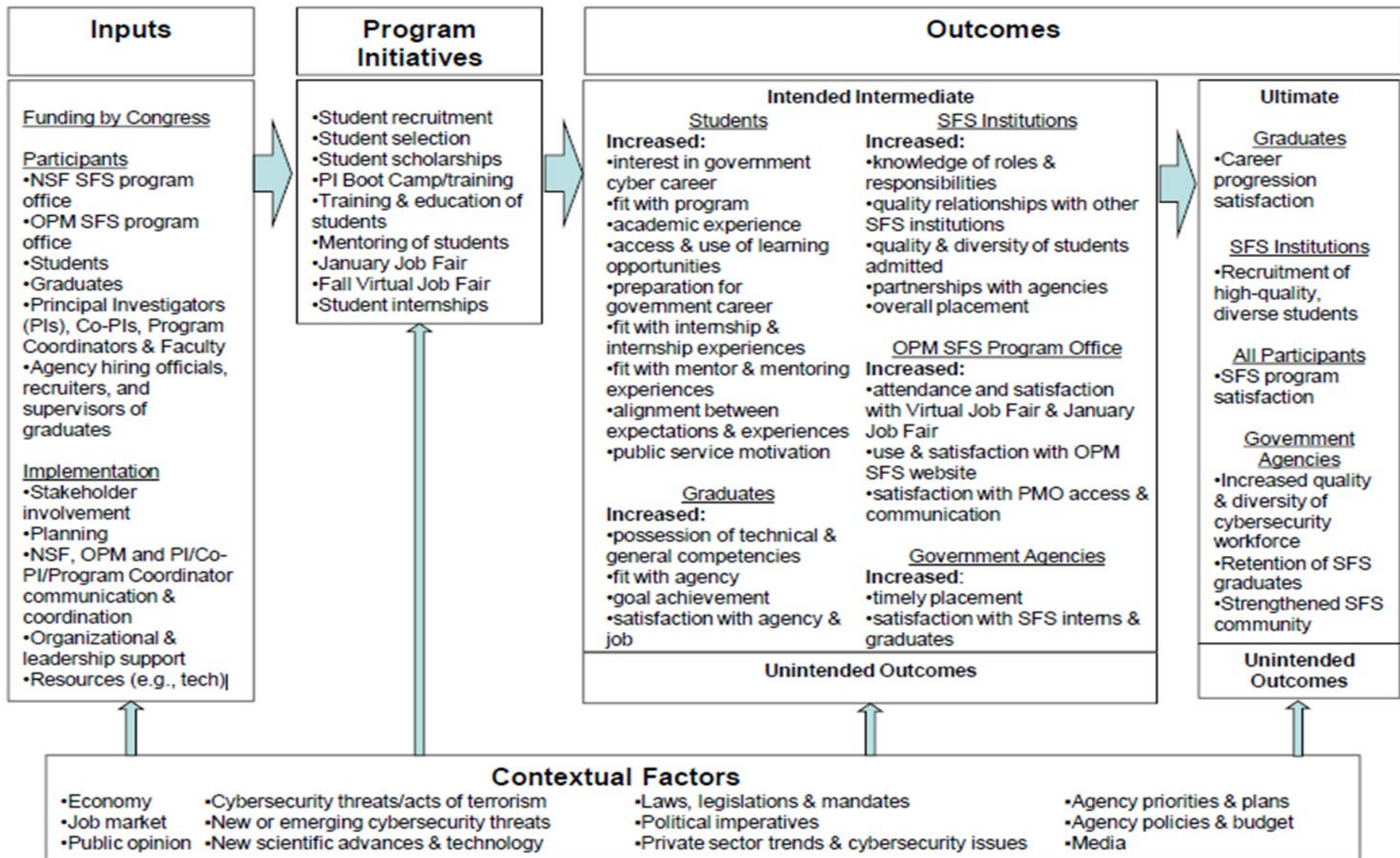
Old Dominion University

Virginia Polytechnic Institute and State University

**Washington**

University of Washington - Tacoma

Whatcom Community College



# WiCyS Professional Affiliates

## United States:

- WiCyS Austin
- WiCyS Central Texas
- WiCyS Central Alabama
- WiCyS Chicago
- WiCyS Colorado
- WiCyS Dallas Fort Worth
- WiCyS Delaware Valley
- WiCyS Florida
- WiCyS Georgia
- WiCyS Houston
- WiCyS Metro NY
- WiCyS Mid-Atlantic
- WiCyS Minnesota
- WiCyS Mississippi
- WiCyS NE Ohio
- WiCyS New England
- WiCyS North Carolina
- WiCyS Northern Alabama
- WiCyS Oregon
- WiCyS Phoenix AZ
- WiCyS San Antonio
- WiCyS San Diego
- WiCyS Silicon Valley
- WiCyS South Dakota
- WiCyS Tennessee
- WiCyS Utah
- WiCyS Western Washington

## WiCyS Corporate Affiliates:

- WiCyS Lockheed Martin
- WiCyS MITRE

## WiCyS Specialty Affiliates:

- WiCyS Artificial Intelligence (AI)
- WiCyS BISO
- WiCyS Critical Infrastructure (CI)
- WiCyS Military

## Africa:

- WiCyS East Africa
- WiCyS Southern Africa

## Asia:

- WiCyS India
- WiCyS Pakistan

## Australia:

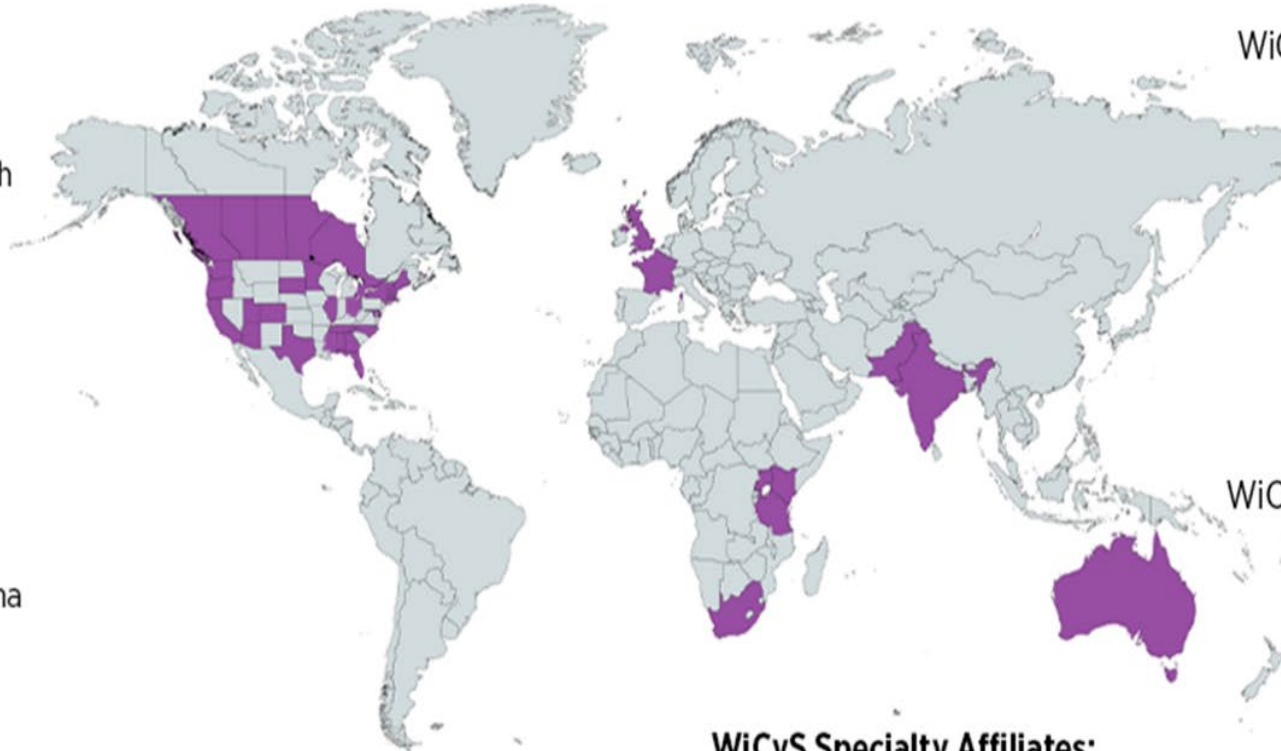
- WiCyS Australia

## Canada:

- WiCyS Ontario
- WiCyS Western Canada

## Europe:

- WiCyS France
- WiCyS UK



APPENDIX J: LIST OF SATC-EDU AWARDS (FY 2018 – 2021)

Title	Year Funded	State	Organization	Award Amount	Award Page
SaTC: EDU: Collaborative: Connecting Contexts: Building Foundational Digital Privacy and Security Skills for Elementary School Children, Teachers, and Parents	2020	MD	University of Maryland, College Park	\$ 334,399	<a href="#">1951688</a>
SaTC: EDU: A Formal Approach to Digital Forensics and Incident Response Investigations	2018	LA	University of New Orleans	\$ 299,998	<a href="#">1821829</a>
SaTC: EDU: Collaborative: Incorporating Sociotechnical Cybersecurity Learning Within Undergraduate Capstone Courses	2018	CA	University of California-Irvine	\$ 64,038	<a href="#">1821822</a>
SaTC: EDU: Collaborative: Connecting Contexts: Building Foundational Digital Privacy and Security Skills for Elementary School Children, Teachers, and Parents	2020	IL	University of Chicago	\$ 199,259	<a href="#">1951311</a>
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2020	FL	Embry-Riddle Aeronautical University	\$ 336,000	<a href="#">1956193</a>
SaTC: EDU: Integrating Cybersecurity Education with Cloud Computing	2018	DE	University of Delaware	\$ 300,000	<a href="#">1821744</a>
SaTC: EDU: Collaborative: Advancing Cybersecurity Learning Through Inquiry-based Laboratories on a Container-based Virtualization Platform	2019	GA	Georgia State University Research Foundation, Inc.	\$ 331,360	<a href="#">1912753</a>
SaTC: EDU: Collaborative: Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students (CyberMiSTS)	2018	NY	SUNY at Stony Brook	\$ 199,131	<a href="#">1821753</a>
SaTC: EDU: Collaborative: Advancing Cybersecurity Learning Through Inquiry-based Laboratories on a Container-based Virtualization Platform	2019	TX	Texas Christian University	\$ 150,000	<a href="#">1912755</a>
SaTC: EDU: Collaborative: An Assessment Driven Approach to Self-Directed Learning in Secure Programming (SecTutor)	2019	IN	Purdue University	\$ 238,127	<a href="#">1934269</a>
SaTC: EDU: Collaborative: INteractive VISualization and PracTice basEd Cybersecurity Curriculum and Training (InviteCyber) Framework for Developing Next-gen Cyber-Aware Workforce	2019	IN	Purdue University	\$ 231,422	<a href="#">1903423</a>



SaTC: EDU: JROTC-CS Project Impact Study	2021	NY	The New York City Foundation for Computer Science Education	\$ 399,203	<a href="#">2028426</a>
SaTC: EDU: Curricula and CTF Exercises for Teaching Smart Fuzzing and Symbolic Execution	2018	OR	Portland State University	\$ 279,448	<a href="#">1821841</a>
SaTC: EDU: Microlessons to Build Readiness in the Cybersecurity Workforce	2018	CA	SRI International	\$ 300,000	<a href="#">1821666</a>
SaTC: EDU: Collaborative: An Educational Initiative on Cybersecurity in Additive Manufacturing	2019	NY	New York University	\$ 496,034	<a href="#">1931724</a>
SaTC: EDU: Collaborative: Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students (CyberMISTS)	2018	NY	Applied Visions, Inc.	\$ 100,804	<a href="#">1821757</a>
SaTC: EDU: Creating Cybersecurity Pathways Between Community Colleges and Universities	2019	VA	Old Dominion University Research Foundation	\$ 497,356	<a href="#">1914613</a>
SaTC:EDU: Enhancing Security Education in Hybrid Mobile and Internet of Things Firmware through Inclusive, Engaging, Learning Modules (E-SHIELD)	2019	NC	University of North Carolina at Charlotte	\$ 444,665	<a href="#">1947295</a>
Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2020	NC	University of North Carolina at Wilmington	\$ 105,790	<a href="#">2025685</a>
Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2021	NC	North Carolina Agricultural & Technical State University	\$ 97,320	<a href="#">2150297</a>
Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2020	NY	Manhattan College	\$ 129,947	<a href="#">2025686</a>
SATC: EDU: Curriculum Development for Secure Blockchain Technologies	2020	TX	University of Texas at Dallas	\$ 499,595	<a href="#">1931800</a>
SaTC: EDU: A Curriculum for Quantum Security and Trust	2021	PA	Pennsylvania State Univ University Park	\$ 215,000	<a href="#">2113839</a>
SaTC: EDU: CyCAD: A Virtual Platform for Cybersecurity Curriculum on Analog Design	2018	PA	Pennsylvania State Univ University Park	\$ 294,280	<a href="#">1821766</a>
SaTC: EDU: Improving Student Learning and Engagement in Digital Forensics through Collaborative Investigation of Cyber Security Incidents and Simulated Capture-the-Flag Exercises	2018	TX	Texas Tech University	\$ 299,999	<a href="#">1821560</a>

Collaborative Research: SaTC: EDU: Hardware Security Education for All Through Seamless Extension of Existing Curricula	2021	FL	Florida International University	\$ 146,675	<a href="#">2114200</a>
SaTC: EDU: Collaborative: An Assessment Driven Approach to Self-Directed Learning in Secure Programming (SecTutor)	2019	CA	University of California-Davis	\$ 151,008	<a href="#">1934279</a>
SaTC: EDU: Collaborative: Building a Low-cost and State-of-the-art IoT Security Hands-on Laboratory	2019	FL	The University of Central Florida Board of Trustees	\$ 372,175	<a href="#">1915780</a>
SaTC: EDU: Game-Based Cyber Security Education on Anonymous Communication	2018	OH	Cleveland State University	\$ 299,977	<a href="#">1821775</a>
SaTC: EDU: Collaborative: Building a Low-cost and State-of-the-art IoT Security Hands-on Laboratory	2019	FL	University of Florida	\$ 150,000	<a href="#">1916175</a>
SaTC: EDU: Collaborative: An Assessment Driven Approach to Self-Directed Learning in Secure Programming (SecTutor)	2019	CA	University Enterprises, Incorporated	\$ 109,772	<a href="#">1934285</a>
SaTC EDU: Assessment Resources for Cybersecurity	2021	IN	Dark Enterprises Inc	\$ 492,892	<a href="#">2117073</a>
SaTC: EDU: Cybersecurity Education Using Interactive Storytelling with Social Robots	2018	DE	University of Delaware	\$ 299,998	<a href="#">1821794</a>
SaTC: EDU: RUI: Enabling a New Generation of Experts by Finding and Fixing Students' Persistent Misconceptions	2018	MN	University of Minnesota Duluth	\$ 315,984	<a href="#">1821788</a>
SaTC: EDU: Collaborative: Incorporating Sociotechnical Cybersecurity Learning Within Undergraduate Capstone Courses	2018	IN	Indiana University	\$ 299,961	<a href="#">1821782</a>
Collaborative Research: SaTC: EDU: Developing Instructional Laboratories for Blockchain Security Applications	2021	NY	Syracuse University	\$ 359,993	<a href="#">2104532</a>
Collaborative Research: SaTC: EDU: Hardware Security Education for All Through Seamless Extension of Existing Curricula	2021	FL	University of Florida	\$ 89,999	<a href="#">2114165</a>
Collaborative Research: SaTC: EDU: Hardware Security Education for All Through Seamless Extension of Existing Curricula	2021	KS	University of Kansas Center for Research Inc	\$ 163,000	<a href="#">2114157</a>
SaTC: EDU: Transdisciplinary Cybersecurity Education for Law and Engineering Students	2021	OH	Cleveland State University	\$ 397,826	<a href="#">2028397</a>
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2020	MA	Northeastern University	\$ 179,999	<a href="#">2043183</a>
SaTC: EDU: LIGERLabs: Educational Modules for (Anti-)Reverse Engineering	2020	AZ	University of Arizona	\$ 400,000	<a href="#">2029632</a>



Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2020	TN	Tennessee Technological University	\$ 196,263	<a href="#">2025682</a>
Collaborative Research: SaTC: EDU: Building an Electronic Voting Technology Inspired Interactive Teaching and Learning Framework for Cybersecurity Education	2020	IN	Indiana University	\$ 237,999	<a href="#">2011117</a>
SaTC: EDU: Improving Student Learning through Competitive Embedded System Security Challenges	2020	FL	University of South Florida	\$ 499,145	<a href="#">1954259</a>
Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2021	MS	Mississippi State University	\$ 105,566	<a href="#">2133190</a>
SaTC: EDU: Secure and Private Artificial Intelligence	2021	GA	Georgia State University Research Foundation, Inc.	\$ 113,025	<a href="#">2054968</a>
Collaborative Research: SaTC: EDU: Building an Electronic Voting Technology Inspired Interactive Teaching and Learning Framework for Cybersecurity Education	2020	CA	University of California-Davis	\$ 178,000	<a href="#">2011175</a>
SaTC: EDU: Preparing cybersecurity advanced professionals for teaching next generation of cybersecurity workforce	2019	VA	Marymount University	\$ 481,761	<a href="#">1927550</a>
SaTC: EDU: Collaborative: INteractive VSualization and PracTice basEd Cybersecurity Curriculum and Training (InviteCyber) Framework for Developing Next-gen Cyber-Aware Workforce	2019	OH	University of Toledo	\$ 267,742	<a href="#">1903419</a>
SATC: EDU: Network Design for Security using Protocol Trust Boundary Observations	2019	TX	University of Houston	\$ 320,446	<a href="#">1907537</a>
SaTC: EDU: Expanding Digital Forensics Education with Artifact Curation and Scalable, Accessible Artifact Exercises	2019	CT	University of New Haven	\$ 300,000	<a href="#">1900210</a>
SaTC: EDU: Collaborative: Personalized Cybersecurity Education and Training	2019	IL	Loyola University of Chicago	\$ 234,654	<a href="#">1919004</a>
SaTC: EDU: Collaborative: Personalized Cybersecurity Education and Training	2019	OK	Oklahoma State University	\$ 306,870	<a href="#">1918591</a>
SaTC: EDU: Advancing Cybersecurity and Privacy of Educational Technologies Used in K-12 schools	2021	NC	University of North Carolina at Charlotte	\$ 499,971	<a href="#">2122416</a>
Collaborative Research: SaTC: EDU: Developing Instructional Laboratories for Blockchain Security Applications	2021	FL	Florida Agricultural and Mechanical University	\$ 39,993	<a href="#">2104519</a>

SaTC: EDU: Developing Ready-to-Use Hands-on Labs with Portable Operating Environments for Digital Forensics Education	2021	CA	University Enterprises, Incorporated	\$ 391,012	<a href="#">2105801</a>
EDU: Collaborative: Using Virtual Machine Introspection for Deep Cyber Security Education	2018	VA	Virginia Commonwealth University	\$ 139,802	<a href="#">1844136</a>
SaTC: EDU: Vertically-Aligned Hands-on Cybersecurity Curriculum Based on Adversarial Thinking	2021	ID	Boise State University	\$ 400,000	<a href="#">2037658</a>
SaTC-EDU: PHIKS - PHysical Inspection and attacks on electronicS	2018	FL	University of Florida	\$ 308,000	<a href="#">1821780</a>
SaTC: EDU: Digital Safety Immersion for Elementary School Students	2020	NC	University of North Carolina at Charlotte	\$ 399,999	<a href="#">2015554</a>
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2020	IL	University of Illinois at Chicago	\$ 179,999	<a href="#">1955337</a>
SaTC: EDU: Collaborative: An Educational Initiative on Cybersecurity in Additive Manufacturing	2019	NY	CUNY New York City College of Technology	\$ 35,966	<a href="#">1932185</a>
EDU: Collaborative: Integrating Embedded Systems Security into Computer Engineering and Science Curricula	2018	IL	Roosevelt University	\$ 32,940	<a href="#">1854494</a>
EDU: Collaborative: Using Virtual Machine Introspection for Deep Cyber Security Education	2018	OH	Ohio State University	\$ 110,883	<a href="#">1834214</a>
SaTC: EDU: Labtainers Framework Extensions	2019	CA	Naval Postgraduate School	\$ 300,000	<a href="#">1932950</a>

APPENDIX K: CYBERSECURITY EDUCATION IN THE AGE OF ARTIFICIAL INTELLIGENCE

Title	Year Funded	State	Organization	Award Amount	Award Page
EAGER: SaTC-EDU: Multi-Level Attack and Defense Simulation Environment for Artificial Intelligence Education and Research	2020	CA	University of California-Irvine	\$300,000.00	<a href="#">2039634</a>
EAGER: SaTC-EDU: A transdisciplinary program for pre-college youth to prepare the future workforce for FATE in AI	2020	CA	University of California-Berkeley	\$299,987.00	<a href="#">2039637</a>
Collaborative Research: EAGER SaTC-EDU: Artificial Intelligence and Cybersecurity: From Research to the Classroom	2021	MD	University of Maryland Baltimore County	\$219,993.00	<a href="#">2114892</a>
EAGER: SaTC-EDU: Exploring Visualized and Explainable Artificial Intelligence to Improve Students' Learning Experience in Digital Forensics Education	2021	MO	University of Missouri-Kansas City	\$90,000.00	<a href="#">2039288</a>
EAGER: SaTC-EDU: Exploring Visualized and Explainable Artificial Intelligence to Improve Students' Learning Experience in Digital Forensics Education	2021	MD	University of Baltimore	\$145,000.00	<a href="#">2039289</a>
EAGER: SaTC-EDU: Exploring Visualized and Explainable Artificial Intelligence to Improve Students' Learning Experience in Digital Forensics Education	2021	MD	Bowie State University	\$64,990.00	<a href="#">2039287</a>
EAGER: SaTC-EDU: Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm	2021	IN	Purdue University	\$299,934.00	<a href="#">2114974</a>
EAGER: SaTC-EDU: AI-based Humor-Integrated Social Engineering Training	2020	IN	Purdue University	\$299,566.00	<a href="#">2039605</a>
Collaborative Research: EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity	2021	SC	Clemson University	\$130,000.00	<a href="#">2114920</a>
EAGER: SaTC-EDU: A Life-Cycle Approach for Artificial Intelligence-Based Cybersecurity Education	2021	IN	Purdue University	\$298,214.00	<a href="#">2114680</a>
EAGER: SaTC-EDU: Mathematically-grounded metaphors to teach AI-related cybersecurity	2020	SC	Clemson University	\$335,982.00	<a href="#">2039616</a>

Collaborative Research: EAGER: SaTC-EDU: Dynamic Adaptive Machine Learning for Teaching Hardware Security (DYNAMITES)	2020	TX	Texas A&M Engineering Experiment Station	\$150,000.00	<a href="#">2039610</a>
EAGER: SaTC AI-Cybersecurity: Opening Doors for Cybersecurity & AI: An Interdisciplinary Approach to Engaging Middle School Students	2021	MA	University of Massachusetts, Dartmouth	\$299,481.00	<a href="#">2114981</a>
EAGER: SaTC-EDU: Designing and Evaluating Curricular Modules for Inclusive Integration of Artificial Intelligence into Cybersecurity	2020	FL	Florida International University	\$308,000.00	<a href="#">2039606</a>
EAGER: SaTC-EDU: Advancing Cybersecurity Education to Human-Level Artificial Intelligence	2020	GA	Georgia Tech Research Corporation	\$299,777.00	<a href="#">2041788</a>
EAGER: SaTC-EDU: A Framework for Developing Attributable Cybersecurity Case Studies	2021	PA	Pennsylvania State Univ University Park	\$312,568.00	<a href="#">2114824</a>
Collaborative Research: EAGER: SaTC-EDU: Safeguarding STEM Education and Scientific Knowledge in the Age of Hyper-Realistic Data Generated Using Artificial Intelligence	2020	CA	Rand Corporation	\$99,923.00	<a href="#">2039612</a>
Collaborative Research: EAGER: SaTC-EDU: Safeguarding STEM Education and Scientific Knowledge in the Age of Hyper-Realistic Data Generated Using Artificial Intelligence	2020	PA	Carnegie-Mellon University	\$100,000.00	<a href="#">2039613</a>
EAGER: SaTC-EDU: Instilling a Mindset of Adversarial Thinking into Computer Science Courses Early and Often	2020	RI	Brown University	\$313,881.00	<a href="#">2039354</a>
Collaborative Research: EAGER: SaTC-EDU: Dynamic Adaptive Machine Learning for Teaching Hardware Security (DYNAMITES)	2020	NY	New York University	\$150,000.00	<a href="#">2039607</a>
EAGER: SaTC-EDU: Training Mid-Career Security Professionals in Machine Learning and Data-Driven Cybersecurity	2020	IL	University of Chicago	\$299,945.00	<a href="#">2041970</a>
EAGER: SaTC-EDU: Identifying Educational Conceptions and Challenges in Cybersecurity and Artificial Intelligence	2020	MI	Regents of the University of Michigan - Ann Arbor	\$300,000.00	<a href="#">2039445</a>
EAGER: SaTC-EDU: Teaching Security in Undergraduate Artificial Intelligence Courses Using Transparency and Contextualization	2020	UT	University of Utah	\$316,000.00	<a href="#">2041960</a>
Collaborative Research: EAGER: SaTC-EDU: Safeguarding STEM Education and Scientific Knowledge in the Age of Hyper-Realistic Data Generated Using Artificial Intelligence	2020	DC	Challenger Center for Space Science Education	\$100,000.00	<a href="#">2039614</a>
EAGER: SaTC-EDU: Artificial Intelligence for Cybersecurity Education via a Machine Learning-Enabled Security Knowledge Graph	2021	AZ	Arizona State University	\$300,000.00	<a href="#">2114789</a>

Collaborative Research: EAGER: SaTC-EDU: Artificial Intelligence-Enhanced Cybersecurity: Workforce Needs and Barriers to Learning	2021	IL	University of Illinois at Urbana-Champaign	\$168,670.00	<a href="#">2113955</a>
Collaborative Research: EAGER: SaTC-EDU: Artificial Intelligence-Enhanced Cybersecurity: Workforce Needs and Barriers to Learning	2021	WA	University of Washington	\$131,329.00	<a href="#">2113954</a>
EAGER: SaTC-EDU: Integrating Cybersecurity into Artificial Intelligence Education	2021	CO	University of Colorado at Boulder	\$297,712.00	<a href="#">2115028</a>
EAGER: SaTC-EDU: Transformative Educational Approaches to Meld Artificial Intelligence and Cybersecurity Mindsets	2021	AL	Auburn University	\$299,941.00	<a href="#">2115025</a>
Collaborative Research: EAGER: SaTC-EDU: Just-in-Time Artificial Intelligence-Driven Cyber Abuse Education in Social Networks	2021	FL	Florida International University	\$192,921.00	<a href="#">2114911</a>
Collaborative Research: EAGER: SaTC-EDU: Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cybersecurity	2020	TX	University of Texas at Dallas	\$239,855.00	<a href="#">2039542</a>
Collaborative Research: EAGER: SaTC-EDU: Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cybersecurity	2020	TX	University of Texas at Tyler	\$29,719.00	<a href="#">2039408</a>
EAGER: SaTC-EDU: Artificial Intelligence and Cybersecurity Research and Education at Scale	2020	AZ	University of Arizona	\$297,719.00	<a href="#">2038483</a>
EAGER: SaTC AI-Cybersecurity: Faking It: Facilitating Public Awareness of Cybersecurity Issues in AI	2021	FL	University of South Florida	\$300,000.00	<a href="#">2114952</a>
EAGER: SaTC-EDU: Improving Cybersecurity Education for Adolescents with Autism Through Automated Augmented Self-Monitoring Applications	2021	FL	The University of Central Florida Board of Trustees	\$299,987.00	<a href="#">2114808</a>
Collaborative Research: EAGER: SaTC-EDU: Just-in-Time Artificial Intelligence-Driven Cyber Abuse Education in Social Networks	2021	FL	The University of Central Florida Board of Trustees	\$106,636.00	<a href="#">2114948</a>
EAGER: SaTC-EDU: Privacy Enhancing Techniques and Innovations for AI-Cybersecurity Cross Training	2020	GA	Georgia Tech Research Corporation	\$300,000.00	<a href="#">2038029</a>
Collaborative Research: EAGER: SaTC-EDU: Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cybersecurity	2020	TX	University of North Texas	\$30,236.00	<a href="#">2039434</a>

EAGER: SaTC-EDU: A Case- and Play-Based Learning Module for Cybersecurity and Artificial Intelligence Education for Early Teen Learners	2021	CA	Looking Glass Ventures, LLC	\$299,995.00	<a href="#">2113803</a>
Collaborative Research: EAGER SaTC-EDU: Artificial Intelligence and Cybersecurity: From Research to the Classroom	2021	IL	University of Illinois at Urbana-Champaign	\$80,000.00	<a href="#">2115040</a>
EAGER: SaTC-EDU: Discovery, Analysis, Research and Exploration Based Experiential Learning Platform Integrating Artificial Intelligence and Cybersecurity	2020	DC	Howard University	\$300,000.00	<a href="#">2039583</a>
Collaborative Research: EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity	2021	NY	SUNY at Buffalo	\$70,000.00	<a href="#">2114982</a>
EAGER: Visualizing Cyber Defense Networks	2018	CA	SRI International	\$299,947.00	<a href="#">1824258</a>
SaTC-EDU: EAGER: Peer Instruction for Cybersecurity Education	2018	VA	Virginia Commonwealth University	\$43,831.00	<a href="#">1901733</a>
Collaborative Research: EAGER: SaTC-EDU: Learning Platform and Education Curriculum for Artificial Intelligence-Driven Socially-Relevant Cybersecurity	2021	NC	North Carolina Agricultural & Technical State University	\$100,000.00	<a href="#">2114936</a>
Collaborative Research: EAGER: SaTC-EDU: Teaching High School Students about Cybersecurity and Artificial Intelligence Ethics via Empathy-Driven Hands-On Projects	2021	CO	University of Denver	\$97,822.00	<a href="#">2115008</a>
Collaborative Research: EAGER: SaTC-EDU: Teaching High School Students about Cybersecurity and Artificial Intelligence Ethics via Empathy-Driven Hands-On Projects	2021	CO	University of Colorado at Boulder	\$44,999.00	<a href="#">2115004</a>
Collaborative Research: EAGER: SaTC-EDU: Teaching High School Students about Cybersecurity and Artificial Intelligence Ethics via Empathy-Driven Hands-On Projects	2021	IL	University of Illinois at Urbana-Champaign	\$154,754.00	<a href="#">2114991</a>



**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.

**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) surveys 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.

**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 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 National Science Foundation (NSF) and the 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.