CyberCorps®

Defending America's Cyberspace

2023 **BIENNIAL REPORT**

CyberCorps® Scholarship For Service (SFS)

U.S. National Science Foundation | January 2024

Request this document in an accessible format by visiting nsf.gov/accessibility

TABLE OF CONTENTS

From electronic banking and e-mails to healthcare and homeland security, society relies heavily on cyber professionals to protect and support the Nation's critical infrastructure. And, in the age of emerging technologies, such as artificial intelligence (AI) and quantum computing, the CyberCorps® Scholarships for Service (SFS) program stands as a national treasure in addressing the escalated demand for more cybersecurity professionals nationwide.

For decades, an interagency partnership with the U.S. National Science Foundation (NSF), the U.S. Office of Personnel Management, and the Department of Homeland Security has supported U.S. institutions of higher education to grow the cybersecurity workforce through the CyberCorps® SFS program. Starting in 2001 with a 31-person cohort, the program has grown exponentially, graduating more than 4,500 students who have accepted critical roles securing the Nation's cyberspace by working at federal, state, tribal, and local government organizations.

To continue strengthening and diversifying the cyber workforce, NSF partnered with the Office of the National Cyber Director in the White House in the summer of 2023 to unveil the National Cyber Workforce and Education Strategy. The interagency partnership underscores the critical demand for a robust diverse workforce and the need for different cyber education pathways that help the Nation maintain its competitive edge on the global stage.

Through program efforts like the Bridge to Cyber initiative and outreach programs for aspiring principal investigators from historically Black colleges and universities, the CyberCorps® SFS program is taking bold steps to make the Nation's cybersecurity workforce more inclusive, diverse, and accessible. New models, like the Security Operations Center and cooperative education, are also pioneering ways to develop new cybersecurity talents. The SFS program also takes a comprehensive approach to fostering early interest in cybersecurity. Initiatives focused on K-12 education, including GenCyber, and an award to the College Board supporting the creation of an Advanced Placement Course in cybersecurity are some of these examples.

The CHIPS and Science Act, which authorized historic investments in research and innovation in key technology focus areas, also marks a significant milestone by expanding the scope of the program. Moreover, the CyberCorps® SFS program now encompasses cybersecurity aspects of AI, aerospace, and more. The program expansion is a recognition of the evolving landscape of cybersecurity and its integral role in national security. Because of these efforts, the CyberCorps® SFS program has seen a remarkable increase in the number of students from diverse backgrounds as well as students from geographically diverse institutions.

In closing, I extend a hearty congratulations to the CyberCorps® SFS students and institutions for their ongoing commitment to protect U.S. cyberspace and for making STEM excellence a priority. I am pleased to introduce this Congressionally mandated 2023 Biennial CyberCorps® SFS report of the program's accomplishments.

/s/
James L. Moore III, PhD
Assistant Director
Directorate for STEM Education (EDU)
U.S. National Science Foundation

CYBERCORPS® SFS PROGRAM OVERVIEW

Cybersecurity plays a vital role in the rapidly advancing information age. With the ever-increasing reliance on digital systems and technologies, the protection of sensitive data, infrastructure, and networks becomes crucial. The interconnectedness of the global economy, government agencies, and individuals amplifies the potential impact of cyber threats, ranging from data breaches and identity theft to more sophisticated attacks on critical infrastructure and national security.

To effectively combat these threats, it is critical to cultivate an innovative cybersecurity education system. Equipping individuals with the knowledge and skills necessary to safeguard against cyber threats is an essential defense strategy and a strategic advantage in ensuring national security. By creating a well-trained and competent cybersecurity workforce, the Nation can remain at the forefront of cybersecurity, ready to respond to evolving threats and protect against cyber-espionage and cyberterrorism.

Moreover, cybersecurity education plays a pivotal role in sustaining economic growth. Businesses, both large and small, are increasingly reliant on digital operations and data storage. A single cyber-attack can lead to devastating consequences, resulting in financial losses, reputational damage, and even closures of businesses. An educated and vigilant cybersecurity workforce helps shield businesses from these threats, promoting a secure digital environment that fosters innovation and encourages investment.

In the quest for technological advancement, cybersecurity education is the bedrock for future innovations in secure cyberspace. As technology evolves, so do the tactics of cyber adversaries. A skilled workforce can help to develop cutting-edge cybersecurity solutions that keep pace with rapid technological advancements, enabling a secure and resilient digital landscape. This, in turn, could help to foster an environment of trust and confidence in adopting emerging technologies, such as artificial intelligence (AI), quantum computing, and advanced communications technologies.

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

The Cybersecurity Enhancement Act of 2014 laid the foundation for the program's expansion. This act was further amended by the National Defense Authorization Acts for 2018 and 2021, empowering the NSF to collaborate with the U.S. Office of Personnel Management (OPM) and the Department of Homeland Security (DHS) to sustain and advance the CyberCorps® SFS program.

The 2023 National Cybersecurity Strategy and the 2023 National Cyber Workforce and Education Strategy align with the primary goal of the CyberCorps® SFS program to develop a superior cybersecurity workforce. Through collaborative effort among various government entities, the CyberCorps® SFS program plays a critical role in cultivating a skilled and diverse cybersecurity workforce that is well-prepared to tackle the ever-evolving challenges in cyberspace. By nurturing cyber talent, the program helps the Nation to remain resilient in the face of cyber threats.

Originally, the CyberCorps® SFS program featured two distinct tracks. The first track, known as the Scholarship Track, provided funding to SFS institutions, enabling them to grant scholarships lasting up to three years to students pursuing undergraduate or graduate degrees in the area of cybersecurity. All scholarship recipients were required to work after graduation in an approved organization in a position related to cybersecurity for a period equal to the duration of the scholarship. The second track, referred to as the Capacity Building Track, had a goal of augmenting the U.S. higher education enterprise by enhancing its ability to produce skilled cybersecurity professionals.

While the Scholarship Track continues, in 2018, the Capacity Building Track merged with the NSF cross-agency Secure and Trustworthy Cyberspace (SaTC) program. This merger created the Education Designation (EDU) of the SaTC program. Through this integration, the CyberCorps® SFS program gained access to a broad network of cybersecurity experts, researchers, and educators. The EDU designation played a role in facilitating knowledge exchange and promoting cutting-edge cybersecurity education research. By harnessing the expertise of the cybersecurity community, the program is cultivating a superior cybersecurity workforce to meet the Nation’s ever-growing demand.

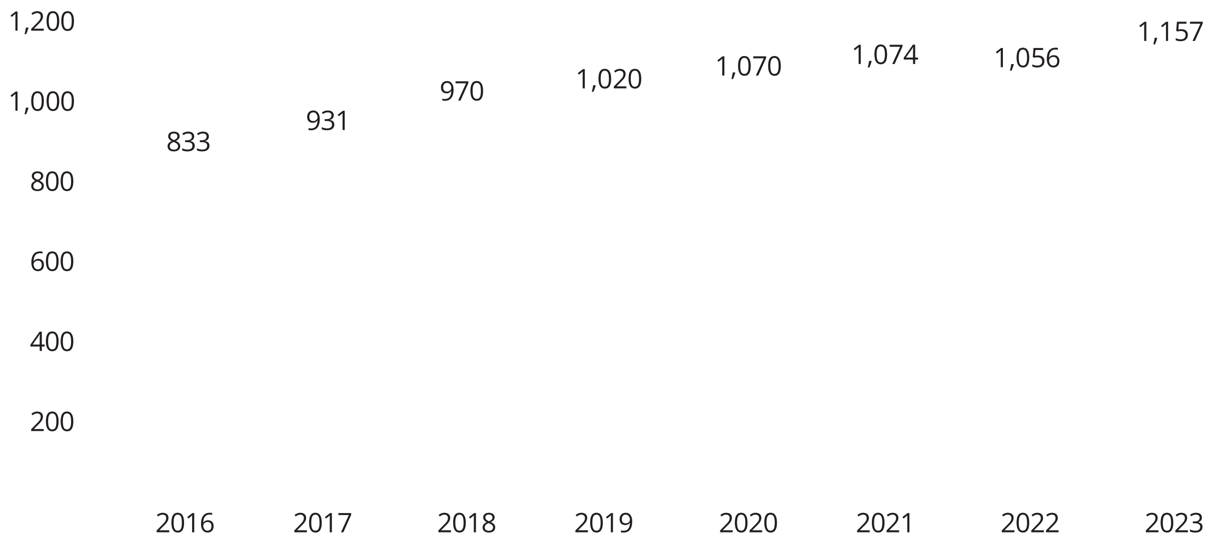


Figure 1 CyberCorps SFS Student Enrollment

The first cohort of 31 CyberCorps® SFS students enrolled in Fall 2001. By the following year, nine students had graduated. Over the years, the program has grown substantially. A total of 5,573 students have enrolled since its inception. Figure 1 illustrates the annual enrollment of both new and continuing students since 2016. As of October 2023, a total of 4,512 talented individuals have graduated from the CyberCorps® SFS program.

As illustrated in Figure 2, the CyberCorps® SFS program’s reach extends across 104 higher education institutions located in 43 states and territories, including the District of Columbia (DC) and Puerto Rico. Appendix G provides the complete list of SFS institutions.

Recognizing that community colleges can play an important role in preparing the future cybersecurity workforce, the program has also forged partnerships between 28 community colleges and SFS institutions.

Through the CyberCorps® SFS program, NSF contributes to the multi-agency efforts convened by the National Initiative for Cybersecurity Education (NICE), which are intended to strengthen collective work to address the Nation’s cybersecurity challenges. The goals of the SFS 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® SFS graduates in the cybersecurity mission of the federal Government; and
4. Strengthen partnerships between institutions of higher education and federal, state, local, and tribal governments.

The immediate objective of the program, as outlined in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, is to place students in government cybersecurity positions. This involves ensuring that a minimum of 70% of scholarship recipients secure positions within the executive branch of the federal government, no more than 20% are placed in non-executive federal, state, local, or tribal government organizations or Federally Funded Research and Development Centers (FFRDCs), and up to 10% secure roles as educators at SFS institutions.

CYBERCORPS® SFS PROGRAM OVERVIEW

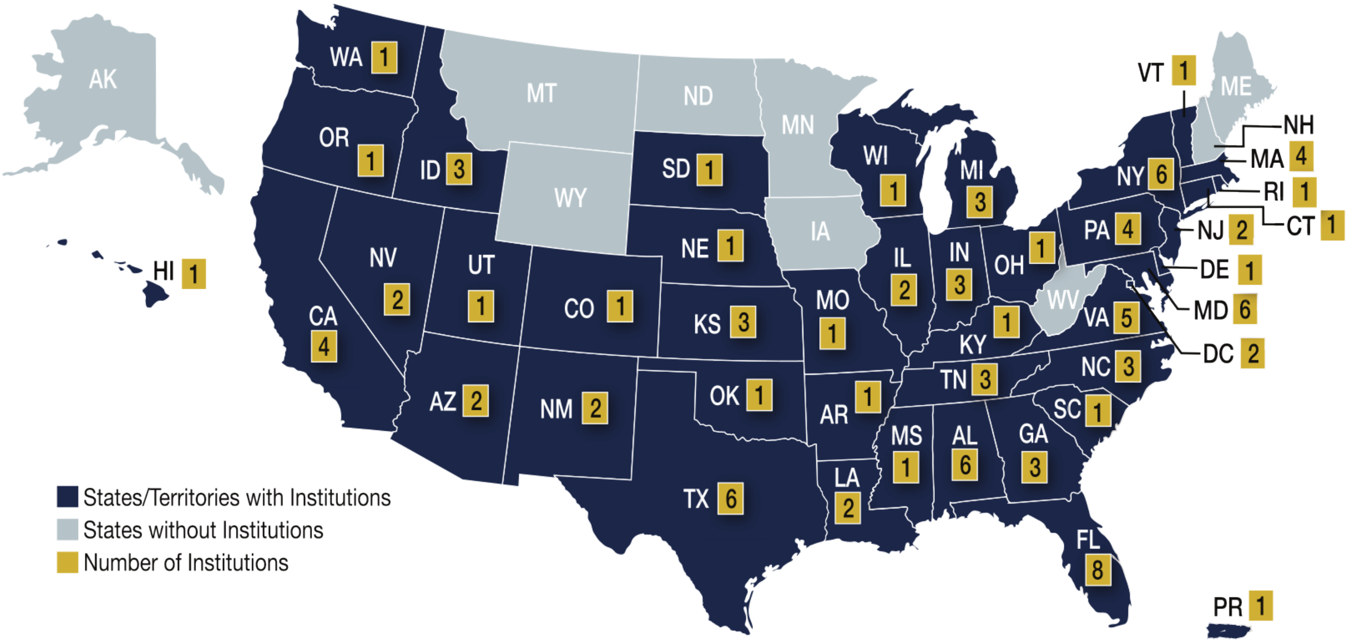


Figure 2 CyberCorps SFS Participating Institutions (2023)

SCHOLARSHIPS

The CyberCorps® SFS program provides awards to higher education institutions through grants. The grantee institutions in turn award scholarships to students pursuing studies in cybersecurity, through a competitive student selection process. CyberCorps® SFS scholarships cover up to three years of stipends, tuition, and professional development allowances for students. CyberCorps® SFS scholarship recipients must be U.S. citizens or lawful permanent residents. Additionally, they must be enrolled as full-time students in a coherent formal program with a specific focus on cybersecurity.

The program accommodates students across more than 178 distinct areas of study, with Computer Science being the most common major. As shown in Figure 3, SFS students come from across the Nation, with California, Texas, and New York being the primary home states. The universities with the largest enrollment of SFS scholars are shown in Table 1; the cumulative new enrollment is the sum of the new SFS enrollment each year from 2016 to 2023. Students range from sophomores in associate's degree programs through research-oriented doctoral degree candidates. In the past two years (2022-2023), graduates have mostly attained master's degrees (52.1%), followed by bachelor's degrees (40.3%), doctoral degrees (5.4%), and associate's degrees (2.2%). CyberCorps® SFS graduates consistently maintain high grade point averages (GPAs) and 82% graduate with a GPA of 3.6 or higher.

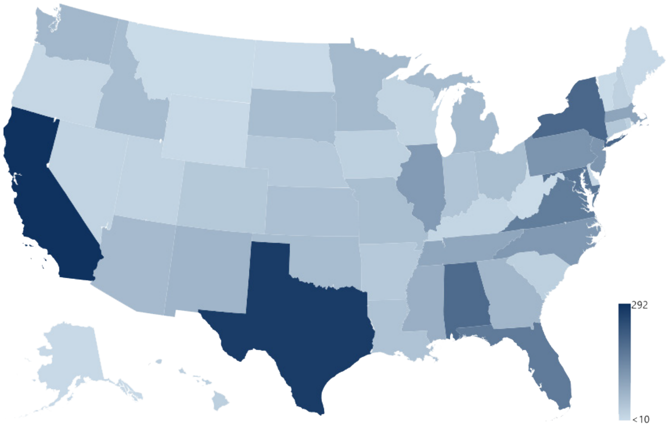


Table 1 Top Universities by Cumulative New Enrollment (2016-2023)[1]

CyberCorps® SFS Institution	Total Cumulative Enrollment
University of Alabama, Huntsville	91
Florida State University	70
CSU - San Bernardino	62
University of Texas at El Paso	55
Carnegie Mellon University	53
University of Texas at Dallas	51
George Washington University	49

SFS scholarship recipients agree to work after graduation in the cybersecurity mission of a federal executive agency, Congress (including any agency, entity, office, or commission established in the legislative branch), an interstate agency, a state, local or tribal government or government-affiliated non-profit considered to be critical infrastructure, or as an educator in the field of cybersecurity at a qualified institution of higher education, as defined in 15 U.S.C. 7442(b)(3)(B). Table 2 outlines the top employers for SFS students, a list that includes the National Security Agency (NSA), Department of Energy (DOE), various branches of the armed forces, and DHS.

The employment will be for a period equal to the duration of the scholarship and to be started within 18 months and to be completed within five years of entering the Commitment Phase of the SFS program. Failure to satisfy the academic requirements of the program or to complete the service obligation results in forfeiture of the scholarship award, which must either be repaid or shall be treated as a Direct Unsubsidized Loan subject to repayment.

Table 2 CyberCorps® SFS Student Top Placements (2001-2023)[2]

Post Graduation Organization	Students
National Security Agency	762
Department of Energy	434
Department of Navy	396
State/Local/Tribal Government/Critical Infrastructure	290
Department of Army	221
Department of Homeland Security	179
Department of Air Force	176
Department of Defense	132
Federal Reserve System and Banks	129
Department of Justice	124

[1] Data as of October 1, 2023.
[2] Data as of October 1, 2023.

PROGRAM MANAGEMENT

As outlined in the SFS statute (15 U.S. Code § 7442), oversight and administration of the CyberCorps® SFS program are entrusted to NSF in collaboration with OPM and DHS. This collaborative framework ensures the program's effectiveness and alignment with national cybersecurity objectives. The SFS program office is an office managing the SFS program through partnership between NSF and OPM. The program has four goals as described in the SFS program overview. While all three agencies work together on all four goals, NSF's strength is in the first two goals; OPM's in goal (3); and DHS in goal (4).

U.S. National Science Foundation

The NSF CyberCorps® SFS Program Office (the "Program Office") plays a central role in overseeing program operation. This role encompasses a broad spectrum of responsibilities, ranging from issuing program solicitations, overseeing the merit review process, conducting site visits, and post-award management of awards. Review of annual and final reports submitted by SFS awardees ensures that projects adhere to program objectives. The Program Office receives feedback and outcomes from the independent evaluation team at OPM, which helps strategic planning and continuous improvement of the program.

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

The Program Office partners with OPM on SFS scholar monitoring. Additionally, a partnership with DHS, in particular through CyberCorps® SFS Job Fairs, facilitates connections between students and government agencies. The Program Office also receives deferral or discharge requests from scholarship recipients. Deferral means an approved extension of the period for completion of the service obligation. A deferral can be requested based on enrollment in a program of study or engagement in approved professional activity for further professional development or CyberCorps® SFS workforce readiness, a condition under the Family and Medical Leave Act (FMLA), a call or order to federal or state active duty or active service, or other exceptional circumstances significantly affecting the scholarship recipient's ability to serve, as determined by the NSF Director. A discharge of service obligation or repayment can be requested based on the circumstances of death, total and permanent disability, or extreme hardship. A scholarship recipient who fails to complete the service obligation must repay the scholarship. If not repaid, the CyberCorps® SFS scholarship amounts paid to the scholarship recipient, together with interest accruing from the date of the scholarship award shall be treated as a Direct Unsubsidized Loan. The scholarship recipient remains liable for any amounts that are not repaid. Such amounts, if not repaid, shall be referred to the U.S. Department of the Treasury for collection.

U.S. Office of Personnel Management

The OPM Program Management Office (the "Management Office") creates and disseminates program documents, including Student Service Agreements, policy directives, and general guidance. These documents form a framework for the administration of scholarships.

The Management Office also facilitates the onboarding process for new scholarship recipients. It tracks scholarship recipients from program entry through the completion of the post-graduation service obligation, which includes monitoring academic progress in collaboration with participating institutions during the scholarship phase. Additionally, the Management Office reviews and approves student job offers, ensuring alignment with program objectives, and monitors the service obligations reported by scholars. For students not fulfilling their service obligations, the Management Office coordinates the collection of data for repayments and repayment waiver requests.

Finally, the Management Office hosts the CyberCorps® SFS program website (https://sfs.opm.gov/), which is an interactive platform where scholarship recipients access program-related information, post resumes, and connect with registered and approved organizations seeking cybersecurity talent. This complements the Management Office's coordination of CyberCorps® SFS Job Fairs, which provide resources and informational sessions that help connect SFS talent to employment opportunities.

Department of Homeland Security

The Cybersecurity and Infrastructure Security Agency (CISA) within DHS is a strategic partner in advancing cybersecurity education and workforce development. It helps to foster partnerships between CyberCorps® SFS institutions and various levels of government—federal, state, local, and tribal. CISA serves as a technical advisor, leveraging its expertise to guide the program. Moreover, CISA sponsors the annual CyberCorps® SFS Job Fairs. Additionally, CISA organizes and maintains the CyberCorps® SFS Hall of Fame to recognize and celebrate the outstanding contributions of SFS scholars to the cybersecurity field.

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

Selection of CyberCorps® SFS Institutions

NSF operates as a proposal-driven funding agency, committed to propelling innovative research and development initiatives in STEM research and education. At the core of its mission is NSF's Merit Review Process. All proposals submitted to NSF are assessed on their intellectual merit and broader impacts. Additional program-specific criteria exist for the CyberCorps® SFS program, which are listed in the program's solicitation[3].

CyberCorps® SFS New PI Boot Camp

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

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

SFS New Scholars Seminar Series (NS3)

The CyberCorps® SFS program supports the New Scholars Seminar Series (NS3), as a part of the Tennessee Tech SFS award, NSF #2043324. This SFS onboarding program aims to achieve the following outcomes for the SFS students: (1) Understand the importance of being an SFS scholar; (2) Learn about being a successful SFS scholar; (3) Understand responsibilities of being an SFS scholar; (4) Understand importance of soft skills for cybersecurity professionals; (5) Acquire a knowledge of resources; and (6) Gain motivation to become successful as a SFS scholar. In 2022, the NS3 consisted of 12 sessions over eight weeks beginning on September 27, 2022. Ninety SFS students from 39 SFS schools across the U.S. attended the NS3 seminar series virtually in Fall 2022. The NS3 covered a broad range of topics, including ethics and etiquette in research, technical writing skills, interpersonal skills, resume writing, and equitable communication and treatment.

FACILITATING GOVERNMENT HIRING

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

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

Hiring Managers and Human Resources Consultants of agencies can register as agency officials at the OPM SFS Portal, gaining access to the pool of SFS scholars. They may also engage SFS students for internships during the students' academic terms, laying the groundwork for potential permanent placements upon graduation.

[3] The SFS Program solicitation, https://new.nsf.gov/funding/opportunities/cybercorps-scholarship-service-sfs-0

CYBERCORPS® SFS JOB FAIRS

To enhance direct engagement, the CyberCorps® SFS program conducts closed hiring events specifically for SFS students every year. The Winter CyberCorps® SFS Job Fair is an in-person job fair jointly sponsored by NSF and DHS. It typically takes place over a three-day period at a DC metro-area hotel. During the pandemic, this job fair was held online. It went back to in-person in 2023, when it was held at the Gaylord National Resort and Convention Center from January 11 to January 13, 2023. Attending the 2023 Winter Job Fair were 698 scholarship recipients and 191 faculty representing 97 colleges and universities including nine new SFS schools. Participants were drawn from 37 states and territories, including DC and Puerto Rico. There were 77 agency booths with 326 agency representatives at the 2023 Job Fair.

WELCOME TO
CyberCorps®:
Scholarship For Service
2023 Job Fair
AGENDA AT-A GLANCE
Wednesday, January 11th
Opening Ceremony & Dinner
5:30 PM – 8:30 PM | Potomac Ballroom A
Thursday, January 12th
Breakfast: My SFS Story
8:00 AM – 9:00 PM | Potomac Ballroom A
SFS Job Fair & Exhibit
9:00 AM –12:00 PM | Potomac Ballroom C
Lunch: Alumni Panel
12:00 PM –1:00 PM | Potomac Ballroom A
SFS Job Fair & Exhibit
1:00 PM –4:00 PM | Potomac Ballroom C
Speed Networking w/ Refreshments
4:00 PM –6:00 PM | Potomac Ballroom A
Friday, January 13th
Breakfast: Closeout Rally
7:00 AM – 8:00 PM | Potomac Ballroom A
SFS Job Fair & Exhibit
8:00 AM –12:00 PM | Potomac Ballroom C
NSF

Traditionally, there has been an annual Virtual Career Fair as well, typically held in October. Beginning in 2023, the Virtual Career Fair was restructured as a series of agency information and resource sessions for SFS scholars.

The primary objective of the CyberCorps® SFS Job Fairs is to facilitate interactions and networking opportunities among CyberCorps® SFS students, PIs, government representatives, and invited guests. More specifically, the Job Fairs aim to address the following themes.

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

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

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

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

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

CYBERCORPS® SFS PROGRAM MONITORING AND EVALUATION

MONITORING

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

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

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

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

EVALUATION

Since starting the first cohort in 2001, the CyberCorps® SFS program has undergone periodic evaluations, developed and executed by the OPM AEB within the Division for Human Resources Solutions (HRS). The most recent comprehensive evaluation, spanning a five-year period, was concluded in 2020, and the next one is expected in 2025. The evaluation process employs a multi-method approach, incorporating diverse data sources, focus groups, annual data collections, on-site visits to colleges, interviews, analysis of SFS Program Office data, and review of external data spanning multiple years.

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

CYBERCORPS® SFS PROGRAM MONITORING AND EVALUATION

PUBLIC INFORMATION

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

A. Placement rates;

B. Where students are placed, including job titles and descriptions;

C. Salary ranges for students not released from obligations under this section;

D. How long after graduation students are placed;

E. How long students stay in the positions they enter upon graduation;

F. How many students are released from obligations;

G. What, if any, remedial training is required;

H. The disparity in any reporting between scholarship recipients and their respective institutions of higher education; and

I. Any recent statistics regarding the size, composition, and educational requirements of the federal cyber workforce.

A. Post Graduate Placement Rates

As of October 2023, the CyberCorps® SFS program has achieved a post-graduate placement rate of 94% in more than 140 government entities. For a comprehensive breakdown of the placement rates for each year, please refer to the detailed information provided in Appendix A.

B. Post-Graduation Placement

Appendix B includes a breakdown of placements categorized by agency, showing where the CyberCorps® SFS scholars have found post-graduation employment. Appendix C provides a list of job titles. Appendix D offers sample job descriptions, providing a perspective on the responsibilities and duties for SFS scholars post-graduation.

C. Salary Ranges 2018-2023

The salary ranges of SFS scholars graduated from 2018 to 2023 are illustrated in Table 3.

Table 3 Salary Ranges of SFS Graduates

Degree (N)	Salary Range	Average Salary
Master's Degree (627)	$24,552 - $187,000	$83,357
Total, All Degrees (1689)	$21,875 - $249,000	$80,923

D. Average Time from Graduation to Employment

CyberCorps® SFS scholars are given 18 months from their graduation date to commence fulfilling their service requirement. Requests for deferring this service obligation are evaluated on a case-by-case basis. Factors such as eligibility for Family and Medical Leave Act (FMLA) coverage or pursuit of further education or professional development within the cybersecurity domain are among the factors taken into consideration when deferrals are requested. Table 4 shows the time from graduation to employment for SFS scholars who were first employed between 2012 and October 2023.

Table 4 Time from Graduation to Employment

Number of Months	Number of Students	%
0-3	1715	59%
4-6	703	24%
7-9	184	6%
10-12	101	4%
13-15	65	2%
16-18	69	2%
Over 18	87	3%

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

The OPM CyberCorps® SFS Program Management Office is performing SFS student portal system updates to collect information about the time students stay in the positions they enter upon graduation. Paperwork Reduction Act (PRA) clearance procedures have been initiated, and once approved by the Office of Management and Budget (OMB), portal updates are expected to launch in fiscal year 2024. In the interim, the QMS is used to measure this item.

The OPM's AEB administered the annual SFS graduate data collection in the summer of 2023. The data collection is part of the QMS and includes Service Obligation Completed (SOC) and Pulse graduates. The SOC graduates are scholars who completed their service obligation within the last year. The Pulse graduates are scholars who completed their service obligation the previous 1-8 years. The data collection was conducted over a 6-week period by AEB.

The 2023 SOC graduates reported the time they stayed in the positions they entered upon graduation. Promotions to a higher grade or more pay within a career ladder (e.g., Series 2210 GS 9/11/12/13) were considered the same position. Table 5 presents the SOC graduate data.

Table 5 Time Students Stay in the Positions They Enter upon Graduation from SOC Graduate Data

Duration in Position	% of Students
6 to 12 months	15.5%
3 years	8.4%

The 2023 Pulse graduates also reported the time they stayed in the positions they entered upon graduation. Table 6 shows the 2023 Pulse graduate data.

Table 6 Time Students Stay in the Positions They Enter upon Graduation from Pulse Graduate Data

Duration in Position	% of Students
less than 6 months	1.9%
6 to 12 months	9.7%
2 years	23.5%
3 years	25.4%
4 years	3.1%
5 years	2.9%
6 years	0.7%
7 years	1.5%
still in the same position[5]	31.3%

F. Students Released from Obligation

Between 2014 and 2023, a total of 12 students were released from their obligations. This comprised six releases within the academic phase, and one partial and five full releases within the employment phase. Additionally, there are currently four pending release requests. Detailed data can be found in Appendix E.

[4] "Still in the same position" in Table 5 means the average is approximately three years or longer.
[5] "Still in the same position" in Table 6 means the average is approximately seven years or longer.

G. What, if any, Remedial Training is Required

The OPM CyberCorps® SFS Program Management Office is performing SFS student portal system updates to collect data related to remedial training. The PRA clearance procedures have been initiated, and once approved by OMB, portal updates are expected to launch in fiscal year 2024. In the interim, the QMS is used for data collection on remedial training. The OPM's AEB administered the annual SFS data collection in the summer of 2023. The data collection included SOC and Pulse graduates.

The 2023 SOC graduates reported whether they were directed to take training outside the mandatory agency training (e.g., Travel Card training), types of training, and if their supervisor identified the training as remedial. Remedial was defined as basic technical or non-technical knowledge or skills needed to perform their jobs. The SOC graduate remedial training data is shown in Table 7.

Table 7 Percentage of Graduates Directed to Take Remedial Training from SOC Graduate Data

Directed to Take Remedial Training	% of Students
No	89.9%

The 2023 SOC graduate data indicates that 10.1% of graduates were directed to take remedial training. Types of training varied from non-cybersecurity related training (e.g., leadership) to cybersecurity-related training, such as the SysAdmin, Audit, Network, and Security (SANS) training, and other cyber-related training.

The 2023 Pulse graduates also reported whether they were directed to take remedial training. Results from the 2023 Pulse graduates are presented in Table 8. The 2023 Pulse graduate data indicates that 6.9% of graduates were directed to take remedial training. The types of training mirrored 2023 SOC graduate results which included both non-cybersecurity related training and cyber-related training.

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

Directed to Take Remedial Training	% of Students
Yes	6.9%
No	93.1%

H. Disparity in Reporting (2018 – 2023)

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

I. Federal Cybersecurity Workforce Statistics

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

INCREASING NATIONAL CAPACITY IN CYBERSECURITY EDUCATION

The CyberCorps® SFS program strengthens the capacity of the Nation's higher education system to cultivate skilled cybersecurity professionals by soliciting proposals in response to the EDU designation of the NSF SaTC program (SaTC-EDU).

SaTC-EDU encourages submission of proposals that explore and advance evidence-based and evidence-generating approaches to enhancing cybersecurity education and workforce development across diverse educational levels—from K-12 to undergraduate, graduate, and professional. Specifically, SaTC-EDU supports projects aiming to:

- Improve cybersecurity learning and learning environments in both formal and informal settings;
- Conduct cybersecurity 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, the program also encourages applications of effective research studies at different types of institutions and with different types of student groups to produce new knowledge about the efficacy and transferability of findings.

The complete list of SaTC-EDU projects funded in FY 2022-2023 is in Appendix I.

SATC-EDU DIRECTIONS WORKSHOP

To address various challenges and gaps within the field of cybersecurity education, the CyberCorps® SFS program sponsored a SaTC-EDU workshop, held on November 7 and 8, 2023, at the University of Texas at Dallas. The workshop brought together researchers, educators, and practitioners in the cybersecurity and privacy community. The objectives of the workshop included:

1. Involving a larger research and education community in cybersecurity and privacy, fostering collaboration and knowledge-sharing among professionals in the field of cybersecurity and privacy;
2. Ensuring that members of the cybersecurity and privacy education community understand education research and evaluation techniques necessary to ensure project success; and
3. Exploring the inclusion of projects in critical areas such as AI and machine learning, quantum computing, and aerospace systems as they relate to cybersecurity and privacy.

The workshop aimed to benefit the next generation of cybersecurity and privacy professionals by integrating cutting-edge research with education initiatives. The workshop emphasized that a well-educated workforce is essential to develop countermeasures against cyber threats. It explored technical directions in cybersecurity education and highlighted the need to integrate cybersecurity research and education.

The workshop included invited talks, panel discussions, poster sessions, and lightning talks on various topics related to cybersecurity education. The event also featured breakout sessions on critical areas and encouraged the participation of individuals from diverse backgrounds.

K-12 INITIATIVES

The National Defense Authorization Acts for Fiscal Years 2018 and 2021 modified the SFS statute and indicated that the SFS program, through coordination with other agencies as needed, should grant awards to improve pre-college cybersecurity education, by providing funding to summer cybersecurity camps or similar programs across the Nation at the K-12 level. The objectives are to: (1) increase students' interest in cybersecurity careers; (2) help students practice appropriate/safe online behavior and understand the principles of cybersecurity; (3) improve teaching methods for delivering cybersecurity content in K-12 computer science curricula; and (4) promote the recruitment, training, and retention of teachers in the field of cybersecurity.

In response to this legislation, the CyberCorps® SFS program supports investments in K-12 education through the SaTC-EDU designation. In addition to the SaTC-EDU projects, the SFS program also supports GenCyber, an initiative focused on K-12 students and teachers, as described below.

GENCYBER - INSPIRING THE NEXT GENERATION OF CYBER STARS

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

GenCyber program goals are to: (1) ignite, sustain, and increase awareness of secondary cybersecurity content and cybersecurity postsecondary and career opportunities for participants through year-round engagement; (2) increase student diversity in cybersecurity college and career readiness pathways at the secondary level; and (3) facilitate teacher readiness within a teacher learning community to learn, develop, and deliver cybersecurity content for the secondary classroom in collaboration with other nationwide initiatives.

The GenCyber program has made significant progress and diversified over the years. In the summer of 2020/21, 156 camps and four capacity-building grants were awarded, including 111 student camps, 41 teacher camps, and four combined student and teacher camps. A total of 98 institutions, including 31 new participants, from 46 states, DC, and Puerto Rico, participated. The GenCyber program served approximately 7,400 students and 1,980 teachers, and in 2022, the program hosted 102 camps in 36 states and DC, with an estimated participation of around 2,600 students and 785 teachers.

In 2023, the program funded a total of 160 camps and capacity-building projects, including 114 student camps, 42 teacher camps, and four combined student and teacher camps. The program's reach extended to 109 institutions, with 10 new institutions joining. The camps were hosted in 47 states, along with DC and Puerto Rico. Maine, Iowa, and Oregon were the only states that did not host a GenCyber program during this period.

SUPPORTING CHIPS AND SCIENCE ACT PRIORITY AREAS

The CHIPS and Science Act recognizes the importance of five areas – AI, quantum computing, aerospace, semiconductors, and advanced communications technologies – in shaping the future of technology and innovation. The Act expanded the scope of the CyberCorps® SFS program by adding cybersecurity-related aspects of other fields, including AI, quantum computing, and aerospace. The initiatives and efforts of the program to support those areas are described next.

ARTIFICIAL INTELLIGENCE (AI)

The CHIPS and Science Act of 2022 (P.L. 117-167) section 10313(d) requires the Director of NSF, in coordination with OPM, to create a report on the need and feasibility, and if appropriate, a plan to establish a Scholarship for Service program to recruit and train the next generation of AI professionals to meet the needs of federal, state, local, and tribal governments. The report will be submitted to the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Science, Space, and Technology of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Oversight and Reform of the House of Representatives. The report is being finalized and will include:

(A) Recent statistical data on the size, composition, and educational requirements of the federal AI workforce, including an assessment of current and future demand for additional AI professionals across the Federal Government.

(B) An assessment of the capacity of institutions of higher education to produce graduates with degrees, certifications, and relevant skills related to AI that meet the current and future needs of the federal workforce.

(C) Evaluation of the need, feasibility, and if appropriate, plans to establish a Federal AI Scholarship-for-Service (AI-SFS) program similar to the CyberCorps® SFS program.

NSF has been collaborating with the National Institute of Standards and Technology (NIST), NSA, OPM, and Department of Defense (DoD) to establish criteria required by the CHIPS Act to designate qualified institutions of higher education to be eligible to participate in an AI-SFS program. Such criteria will include—

- measures of the institution's demonstrated excellence in the education of students in the field of AI; and
- measures of the institution's ability to attract and retain a diverse and nontraditional student population in the fields of science, technology, engineering, and mathematics, which may include the ability to attract women, minorities, and individuals with disabilities.

NSF and its partners are analyzing information to determine if the Center of Academic Excellence in Cybersecurity (CAE-C) model is translatable to AI. A parallel effort focuses on developing a modern taxonomy/classification of the federal AI workforce, similar to the NICE Cybersecurity Workforce Framework maintained by NIST, or the DoD Cyber Workforce Framework (DCWF).

In August 2023, the CyberCorps® SFS program funded a workshop on AI education, NSF Award #2330257, to bring thought-leaders together to respond to increasing concerns and opportunities raised by recent AI developments and to develop strategies for increasing the scope, capacity, and diversity of AI education for K-12 and post-secondary students, current members of the workforce, and the public.

There is a need to develop educational programs and curricula that can increase capacity and diversity among AI professionals as well as to increase awareness of the implications of using AI-driven technologies. The goals for this workshop included developing guidelines for curricula with a scope of content that will reflect the competencies needed in the workforce. Questions included: "Where are we today and where should we be directing our efforts to increase capacity and diversity?" and "How can we classify the competencies and descriptions of the workforce in AI to estimate capacity?" Major findings are summarized below.

Quality AI Education: Strategies for establishing guidelines for quality AI education across all levels of education are being addressed by organizations such as TeachAI.org and the ACM/AAAI Committees for curriculum guidelines. A gap in the development of curriculum guidelines exists for public AI literacy and the need to enhance the offerings and effectiveness of adult AI education.

Increasing Capacity in AI Education: Increasing capacity in AI requires a comprehensive educational approach, including curricular development, teacher training, and public awareness initiatives across various educational levels. Enhancing AI capacity requires a combination of revised educational approaches, informed partnerships, and a commitment to fostering an inclusive and adaptable AI understanding across disciplines. Creating trusted information sources and utilizing public resources and organizations to share information is essential.

Increasing Diversity in AI Education: The complex challenge of promoting diversity and inclusivity in AI education across various educational levels requires more research. The strategies and metrics encompass demographic representation, accessibility, teacher training, interdisciplinary collaboration, and the contextualization of materials.

The overarching goal is to create inclusive AI education that addresses the unique needs and backgrounds of learners and educators at each level while considering the intersecting factors that shape their experiences.

AI in Education: The integration of AI into education is poised to redefine the equilibrium between theoretical understanding and skill acquisition. As AI automates certain tasks and challenges traditional learning pathways, the educational community must reassess the primary objectives of learning to ensure a holistic development of learners in this new paradigm.

QUANTUM COMPUTING

One of the most significant cyber threats today is the advent of quantum computers capable of solving complex mathematical problems exponentially faster than classical computers. This has an important implication for widely used public key cryptosystems, such as RSA that relies on the challenge of factoring large numbers. Quantum computers make it possible to rapidly decipher communications and transactions encrypted by such cryptosystems. As such, post-quantum cryptography (PQC) becomes an emerging field that focuses on designing encryption methods resilient to quantum attacks, ensuring data security in a quantum computing era.

On the other hand, quantum technology may also present a unique opportunity to enhance security. Quantum cryptography, which harnesses the principles of quantum mechanics, provides a means to create strong encryption methods.

Given the important role of quantum technology in preserving the integrity and confidentiality of our digital landscape, the CyberCorps® SFS program funded multiple cybersecurity-related quantum projects through the SaTC-EDU designation. A selection of projects is listed in Appendix J, including the QuSim project of the University of Nebraska at Omaha (NSF Award #1623380), the quantum security project of the Pennsylvania State University (NSF Award #2113839), and a joint project, QUINTET, between the University of Nebraska at Omaha and Kennesaw State University (NSF Awards #2324924 and 2324925). A summary of those projects is given below.

The QuaSim project of the University of Nebraska at Omaha introduces a pedagogical approach to address the challenge of teaching quantum cryptography resulting from traditional linear teaching methods and the high cost of quantum cryptographic equipment. QuaSim is a game-based simulator designed to enhance the learning experience for students studying quantum cryptography, by transforming conventional subject-based lectures into interactive project-based virtual simulations. Further, QuaSim offers an adaptive framework that continually customizes scenarios and assesses user responses to enhance learning. The incorporation of abductive theorem proving, and data analysis enable QuaSim to adjust game scenarios in response to user performance, allowing instructors to quantifiably link student progress with specific knowledge components and design effective lesson plans. Overall, the project makes quantum cryptography more accessible and engaging through interactive learning.

Traditional quantum computing courses tend to be theoretical, while industry advancements focus on practical applications. The quantum security project of Pennsylvania State University seeks to bridge the gap by developing a hands-on undergraduate curriculum using the Quantum Security and Trust (QUEST) framework. This approach provides low-cost, cloud-based access to quantum hardware and simulators, and promotes personalized learning through engaging activities. This makes complex quantum computing concepts more accessible to a wide range of undergraduate students. Overall, through early engagement in students' academic careers, the project prepares a workforce ready to navigate the challenges and opportunities that will arise as quantum computing becomes more accessible and integrated into the cybersecurity landscape.

The joint project of the University of Nebraska at Omaha and Kennesaw State University uses an experiential learning platform, QUINTET, to address challenges in teaching secure quantum communications and quantum networking. By providing a comprehensive, hands-on curriculum, QUINTET aims to enhance educators' ability to teach these complex topics and offer students a more engaging and effective learning experience. The curriculum allows students to apply their knowledge through activities and games, using both simulations and real quantum hardware. By providing practical experience, this project aims to prepare a skilled workforce capable of addressing the challenges and opportunities in the fields of secure quantum communications and quantum networking.

AEROSPACE

Both aviation and aerospace are vital to national security and economic prosperity. The safety of passengers and crew members on airliners depends on the reliability and integrity of aviation systems, which depend extensively on software and communication systems. Cyberattacks on these systems can lead to serious consequences, such as compromised flight navigation. Aviation and aerospace infrastructures, such as military aircrafts and satellites, play a crucial role in national security. Cyberattacks targeting these assets can undermine a Nation's ability to respond to threats and conduct intelligence operations. Finally, the aerospace industry is an important sector of the national economy, and a disruption caused by cyberattacks would have far-reaching economic consequences.

Unmanned Aerial Vehicles (UAVs) have recently been integrated and used across a range of sectors such as agriculture, infrastructure inspection, disaster management, and even warfare. However, UAVs are vulnerable to cyber-attacks, leading to unauthorized access, data breaches, or physical damage, potentially undermining critical operations and compromising national security.

To support cybersecurity education related to aerospace, the CyberCorps® SFS program funded a large project at Embry-Riddle Aeronautical University (ERAU), NSF Award #2146462, with a focus on aviation and aerospace. The SFS program also funded several projects related to security of aerospace and UAVs through the SaTC-EDU designation. A selection of such projects is listed in Appendix J, including the joint UAV project of ERAU and the University of Illinois at Chicago (NSF Awards #1956193 and 1955337), and the Space-Cybersecurity project of Indiana University. A summary of those projects is given below.

The aerospace-focused SFS project of the ERAU builds an environment that trains a diverse group of SFS scholars, by offering a comprehensive curriculum, student engagement opportunities, and hands-on research experiences. ERAU's strong connections to federal and state aviation agencies, as well as the aviation and aerospace industry, provide SFS scholars with unique opportunities to engage in various aviation and aerospace projects and events. ERAU's on-site resources in flight operations-related computation and communication services, including avionics and network systems, expose SFS scholars to attacks and protection at all stages of aviation and aerospace system development and operation.

The joint UAV project of ERAU and the University of Illinois at Chicago addresses cybersecurity challenges in the rapidly expanding field of UAVs, or drones. The project develops a comprehensive curriculum and program that includes cohesive course modules covering UAV cybersecurity topics, a practical UAV cybersecurity laboratory platform, an open collaborative repository for sharing knowledge, and faculty development workshops. The project educates students and professionals about UAV cybersecurity, including hardware, communication, network, and data security.

The Indiana University's Space-Cybersecurity project is a supplement to the university's SFS project, NSF Award #1946537. This supplement addresses the growing importance of cybersecurity in the field of space and ground-based critical infrastructure. It builds capacity for safeguarding space assets by diversifying and expanding the space-cybersecurity talent pipeline. It encompasses six thrust areas: promoting diversity in the space cybersecurity workforce, identifying vulnerabilities in scientific cyberinfrastructures supporting space systems, developing protective tools and standards, building curriculum, recruitment and outreach, and workforce development. This supplement addresses the need to offer workforce development opportunities in space-cybersecurity, aligning with the increasing reliance on space-based technologies around the globe.

SEMICONDUCTORS

Semiconductors and microelectronics are the foundation of all types of digital devices and systems. As such, hardware security is crucial to prevent security breaches of information systems and safeguard the digital landscape. It is critical that cybersecurity experts gain insights into the design and structure of microchips or integrated circuits (ICs). This knowledge enables them to recognize potential vulnerabilities in chip design and manufacturing. By comprehending these vulnerabilities, they can devise strategies to defend against hardware-based attacks, such as Trojan insertions and side-channel attacks.

Cybersecurity professionals also need to be able to develop and implement countermeasures at the hardware level, e.g., embedding security features directly into the chip architecture. By understanding semiconductor technologies, cybersecurity professionals can effectively collaborate with hardware engineers during system design.

Through the SaTC-EDU designation, the CyberCorps® SFS program has funded multiple projects related to semiconductor hardware security education. A selection of projects is listed in Appendix J, including the joint HACE Lab project of the Florida Institute of Technology and the University of Florida (NSF Awards # 1623310 and 1623299), the PHIKS project of the University of Florida (NSF Award #1821780), the joint DYNAMITES project of New York University and Texas A&M (NSF Awards #2039607 and 2039610), and the joint Hardware Security for All project of the University of Florida and Florida International University (NSF Awards #2114165 and 2114200).

The HACE Lab project is a collaboration project between the Florida Institute of Technology and the University of Florida to enhance semiconductor education with a focus on hardware security and trust issues. It creates a comprehensive collection of course materials centered around hardware security. The project's Hardware Attack and Countermeasure Evaluation (HACE) Lab enables remote access and assists instructors in delivering a curriculum that equips students with essential skills in hardware security. Topics such as Trojan attacks, supply chain concerns, side-channel attacks, reverse engineering, piracy, and trustworthy design are addressed.

The HACE Lab platform enriches existing cybersecurity programs and simplifies the adoption and distribution of practical training modules, by providing access to specialized hardware, security analysis tools, metrics, and benchmarks.

The PHIKS project led by the University of Florida aims to advance semiconductor and cybersecurity education by addressing challenges in teaching hardware security. Despite the growth of the hardware security community, certain advanced topics, such as physical attacks and counterfeit detection, are under-explored. This is primarily due to limited access to essential instrumentation, the multidisciplinary nature of the subject, and levels of hardware complexity. The PHIKS project delves into these complex topics and develops a variety of course modules, including counterfeit IC detection, fault injection, destructive and non-destructive reverse engineering, and probing techniques. It also provides training in hardware inspection equipment, such as advanced microscopes and X-ray systems, and associated image-processing techniques.

The DYNAMITES project is a collaboration project between New York University and Texas A&M, to bridge educational gaps by merging AI and hardware security to empower students to address evolving hardware security threats. It explores AI's role in helping students to understand hardware, including using AI to generate new challenges, and assessing how AI impacts students' mindset. The project develops DYNAMITES, a dynamic adaptive machine learning tool designed to enhance students' practical skills in hardware attack and defense exercises. Additionally, the project aims to advance automated scanning and patching of hardware vulnerabilities. The project makes hardware security education more accessible and equips future professionals with critical skills.

Hardware Security for All, a joint project by the University of Florida and Florida International University, integrates hardware security principles into existing core courses within engineering undergraduate programs. The objective is to reach and train a large pool of engineering students so that they are well-prepared to enter the cybersecurity workforce with skills in hardware security. Six key hardware security concepts, such as digital design and embedded systems, are woven into the foundational engineering courses. Course materials are available online, extending the project's benefits to universities and community colleges across the Nation.

ADVANCED COMMUNICATIONS TECHNOLOGIES

Advanced communications technologies are the underpinning of telecommunication and computer networks, supporting the Internet and numerous applications, including social media, Email, and mobile services. Communications technologies play a critical role in shaping the modern world and national economy. Advanced communications technologies are also crucial to national security in that modern defense systems rely on advanced communications for secure and efficient command and control.

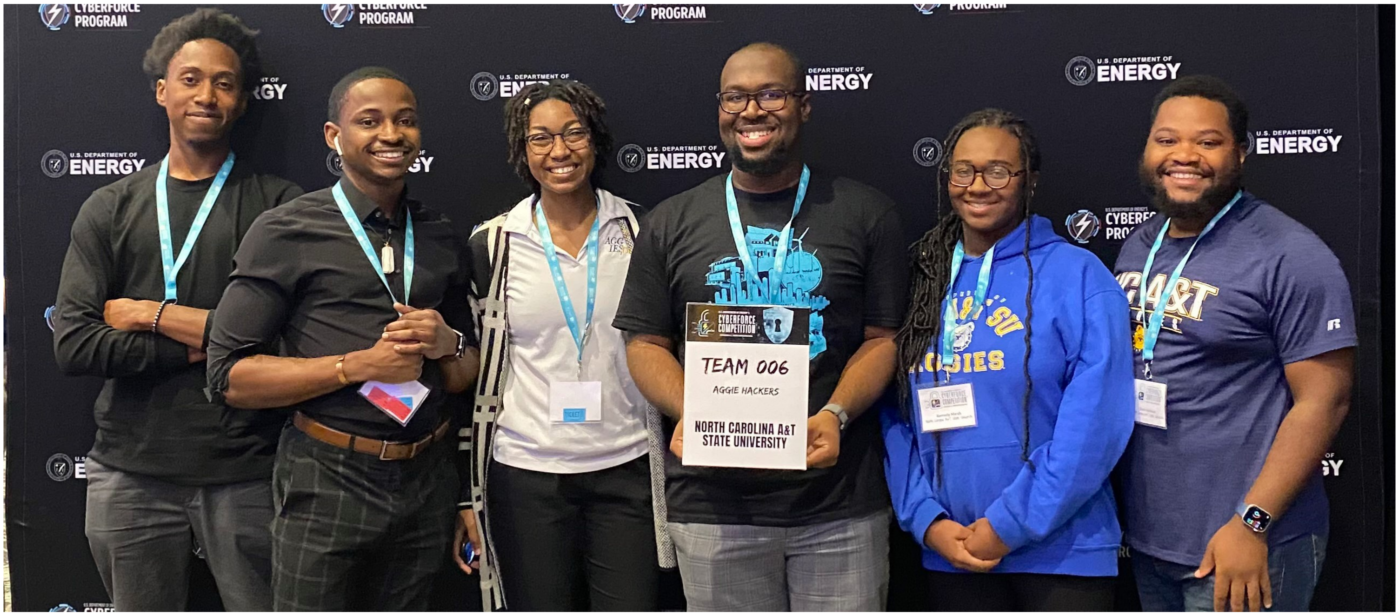
However, Advanced communication technologies pose cybersecurity and privacy challenges. Understanding these technologies is crucial for developing robust cybersecurity mechanisms, safeguarding sensitive data, and ensuring the privacy of individuals and organizations. The CyberCorps® SFS program has funded multiple projects on cybersecurity-related advanced communications through the SaTC-EDU designation. A selection of projects is listed in Appendix J, including the Radio Wars project of Drexel University (NSF Award #1723606), the Moving Target Defense project of Arizona State University (NSF Award #1723440), and the joint NextG and AI Integration project of the University of South Florida and the University of Oklahoma (NSF Awards #2321270 and 2321271). A summary of those projects follows.

The Radio Wars project of Drexel University addresses the growing demand for students skills in integrating security into communication system design. Leveraging the software-defined radio (SDR) platform, the project offers an interdisciplinary curriculum with hands-on experience to train engineering students. The students engage in Radio Wars competitions to learn how to securely transmit information and develop their understanding of the fundamentals of wireless communications, encryption, authentication, and power management for wireless devices. The project fosters a cybersecurity mindset for students, and exposes high school students to cybersecurity, engineering, and STEM fields.

The Moving Target Defense (MTD) project of Arizona State University develops a computer network based MTD curriculum for undergraduates and graduates in computer science. It introduces MTD concepts and establishes a cloud-based hands-on laboratory for broader accessibility. Hands-on learning modules focus on advanced computer networking technologies, such as Software Defined Networking (SDN) and Network Function Virtualization (NFV), together with MTD. Industry partners and a teacher training workshop help to disseminate developed MTD learning modules and hands-on exercises.

The emergence of 5G and NextG networks has introduced new security and privacy challenges. The NextG and AI Integration project of the University of South Florida and the University of Oklahoma focuses on integrating AI techniques into wireless network security. The project prepares the future workforce to handle the complexities of modern wireless networks, bridging the gap between wireless security and AI techniques. Through curriculum modules and project-based training, students gain practical experience across various layers of wireless communications. The project utilizes special wireless equipment to promote a real-world experiment-in-the-loop learning experience in AI techniques integrated for 5G/NextG security.

INCREASING DIVERSITY AND INCLUSION IN THE CYBERSECURITY WORKFORCE



NSF is committed to empowering STEM talent to fully participate in science and engineering. U.S. global competitiveness depends critically on the preparedness of the Nation's STEM workforce, especially in high-priority areas, such as cybersecurity.[6] Proposals submitted to the CyberCorps® SFS program are evaluated in part on the presence of "evidence-based broadening participation strategies at the institution and specific plans for recruitment, mentoring, and retention of SFS 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 of CyberCorps® SFS participants has increased slightly since the 2021 CyberCorps® SFS Biennial Report was published, additional efforts by all stakeholders are needed to implement best practices to address diversity, equity, inclusion, and accessibility (DEIA) challenges related to broadening participation. The aim of the CyberCorps® SFS program is to increase the participation of populations traditionally underrepresented in the cybersecurity workforce, including students from underrepresented groups, under-resourced populations, and students/institutions from rural regions and EPSCoR[8] states.

The following Minority-Serving Institutions[7] are currently receiving support from the CyberCorps® SFS program:

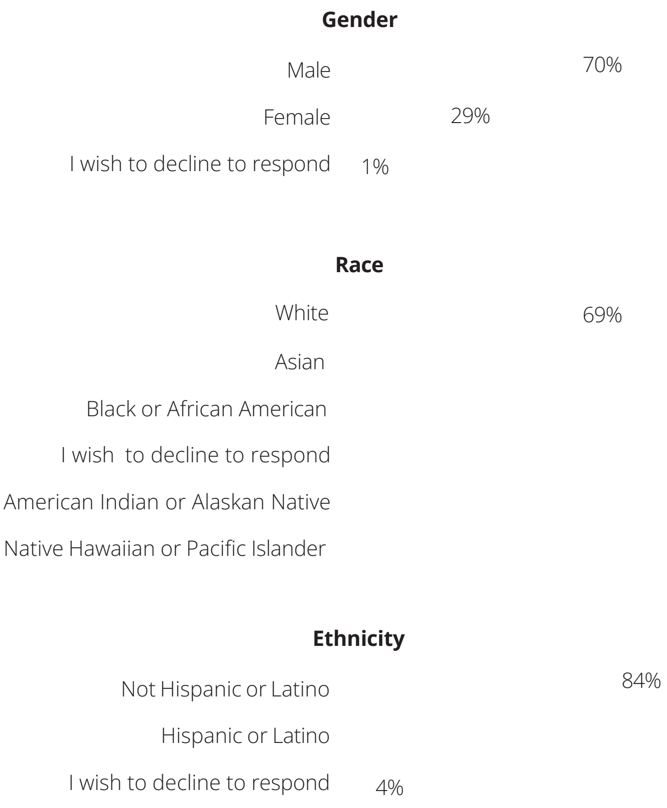
- Tuskegee University - HBCU
- University of Arizona - HSI
- California State Polytechnic University-Pomona - HSI and AANAPISI
- California State University-Sacramento - HSI and AANAPISI
- California State University-San Bernardino - HSI
- Florida International University - HSI
- University of Central Florida - HSI
- Georgia State University - AANAPISI and PBI
- University of Hawaii at Manoa – AANAPISI and ANNHI
- Bowie State University - HBCU
- Morgan State University - HBCU
- University of Maryland-Baltimore County - AANAPISI
- North Carolina A&T State University - HBCU
- New Mexico Institute of Mining and Technology - HSI
- University of New Mexico-Main Campus - HSI
- Sam Houston State University - HSI
- University of Houston - HSI and AANAPISI
- The University of Texas at El Paso - HSI
- The University of Texas at San Antonio - HSI
- Hampton University - HBCU
- Marymount University - HSI
- Norfolk State University - HBCU
- Virginia Polytechnic Institute and State University - AANAPISI
- University of Washington-Tacoma Campus - AANAPISI

[6] U.S. National Science Foundation (2022 – 2026) Strategic Plan, p. 29. U.S. National Science Foundation, Alexandria, VA. Retrieved from: https://www.nsf.gov/publications/pub_summ.jsp?ods_key=nsf22068.

[7] Minority-Serving Institution (MSI) Abbreviations used include: HBCU: Historical Black Colleges and Universities; HSI: Hispanic Serving Institution; AANAPISI: Asian American Native American Pacific Islander Serving Institution; ANNHI: Asian American and Native American Pacific Islander Serving Institution.

[8] EPSCoR: Established Program to Stimulate Competitive Research.

Figure 4 CyberCorps® SFS Recipients' Demographics



The SFS program has supported three specific initiatives to attract, retain, and graduate students from diverse backgrounds. These efforts were announced in the Roundtable on "The State of Cybersecurity in the Black Community", hosted by the Office of National Cyber Director (ONCD) and are briefly introduced next.

BRIDGE TO CYBER PROGRAM

The Bridge to Cyber program is a three-year collaboration between SFS and the Center for Inclusive Computing (CIC) at Northeastern University. CIC engages with interested SFS schools to develop bridge programs designed to increase diversity in the cybersecurity workforce. Bridge programs connect individuals with no background in cybersecurity, including those from populations historically marginalized in tech/cyber, to opportunities to earn advanced degrees in cybersecurity. These programs enable the participation of individuals who may have undergraduate degrees in subjects other than computing to pursue graduate education in cybersecurity at SFS institutions. The first cohort of seven institutions' Bridge programs began in 2023 and a call for a second cohort of programs went out in Fall 2023. The first cohort includes: George Washington University, New York University, Oakland University, Old Dominion University, Tuskegee University, University of Alabama at Birmingham, and University of Rhode Island. A brief introduction to the programs at these institutions follows.

New York University's Bridge to Cyber Program is designed to equip over 800 recent college graduates and mid-career professionals annually, including those from low-income backgrounds, with foundational computer science skills that will enhance their eligibility for STEM programs such as a master's degree in cybersecurity. Oakland University's Bridge to Cyber program (B2C@OU) provides professionals from non-computing backgrounds a flexible and cost-effective pathway to develop crucial cybersecurity skills, facilitating admission to the Master of Cybersecurity program, with a strong emphasis on recruiting historically underrepresented students and anticipating a total enrollment of 60 over two years. Tuskegee University's Cyber Bridge program is specifically designed for non-computer science majors from historically marginalized populations in technology to create pathways for prospective students to enter the SFS program before graduation, with an initial pilot cohort expected to enroll 15 students. The Cybersecurity Bridge for Enrollees New to Technology program, at Old Dominion University, is designed to attract and support graduate students from historically marginalized backgrounds in technology, featuring comprehensive elements like focus groups, expert consultations, customized online training, and a commitment to inclusivity. The George Washington University program is tailored to students with a bachelor's degree from any accredited college and offers accessibility through minimal math prerequisites and affordable tuition, with plans to enroll 25-50 students annually.

INCREASING DIVERSITY AND INCLUSION IN THE CYBERSECURITY WORKFORCE

The University of Rhode Island's OnRamp program equips graduates from non-computing backgrounds with the technical foundation required for success in the Cybersecurity master's program, with an initial goal to prepare 20 students. The University of Alabama at Birmingham's program welcomes graduates from all undergraduate majors without a Computer Science background, offering the foundational knowledge necessary for entry into the Master Cybersecurity program, with the inaugural cohort of 20 students set to begin in Fall 2024.

JUMPSTART TO CYBER PROGRAM

The Jumpstart to Cyber program is a one-year collaboration between SFS, Sinclair Community College, NCyTE and SANS Institute. The program focuses on engaging and empowering individuals with no background in cyber, with a goal of increasing participation of members of groups underrepresented in cybersecurity. A no-cost, six-week program was launched in the summer of 2023 to serve individuals interested in learning cybersecurity fundamentals. This tiered summer program is offered in partnership with the SANS Institute. The program offered an "Anytime Anywhere" training opportunity to participants through an initial gamified learning experience, followed by an opportunity to complete a SANS training course and earn the SANS GIAC certification in Cyber. Participants were supported with access to mentors with subject-matter expertise in cybersecurity. The program received around 1200 applications for 250 seats and attracted a large percentage of applicants from underrepresented groups. The program's ultimate objective is to credential 250 students with the GIAC Foundational Cybersecurity Technologies (GFACT) certification. An overview of the JumpStart program is provided below.

Of 1,174 students who registered to participate in the gamified learning experience, 225 were selected to move forward to the second part of the program, the SANS SEC 275 course. Of the 225 students eligible, 169 registered. Of those, 97% represent diverse learning backgrounds, with 52% identifying as female. Additionally, 77.5% identify with a race or ethnicity that enhances diversity in the field of cybersecurity.

As of December 5, 2023, 76 students among the 169 enrolled had successfully completed SEC275 and passed the GFACT examination. The remaining members of the cohort are in the process of completing their SEC275 coursework and will take the GFACT after their coursework is complete. The SANS team is building a plan to re-engage 38 students who took SEC275 but never attempted the GFACT exam to assess if they are still interested in the certification.

SANS and Sinclair have organized a JumpStart into Cyber Capture the Flag event for January 4-6, 2024. During this event, students compete for the remaining 81 slots available for SEC275 enrollment. While the event welcomes all participants, only students from the initial pool of 1,174 registrations have the opportunity to qualify to enter SEC275.

Upon conclusion of the JumpStart program, a total of 250 students will have received support to complete SEC275 training and attain the GFACT certification.

OUTREACH AND ENGAGEMENT INITIATIVE FOR ASPIRING PIS FROM HBCUS

This initiative involves SFS/SaTC program officers (POs) partnering with NSF's Historically Black Colleges and Universities - Undergraduate Program (HBCU-UP) Program to encourage the submission of proposals by HBCU, Predominately Black Institutions (PBIs), and investigators who are underrepresented in accordance with NSF's priority goals. The outreach and engagement activities included a four-hour long session held on September 7, 2023, for approximately 40 faculty (informed by two listening sessions with smaller groups held in May), which highlighted funding programs housed within the STEM Education Directorate at NSF. A panel of PIs discussed strategies for overcoming challenges and best practices. Breakout rooms were available for networking. The session also encouraged attendees to join a peer support group hosted by the SFS program at Tuskegee University.

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.

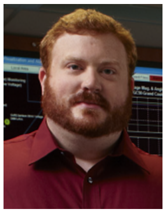
Institutions can nominate more than one candidate for consideration. A committee then evaluates each nominee based on their achievements and contributions to the cybersecurity community. After the committee selects a finalist, CISA announces the annual Hall of Fame recipient at the Winter CyberCorps® SFS Job Fair. Since recognizing the first three recipient inductees into the Hall of Fame in 2018, a total of eight 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, received both the Presidential Early Career Award for Scientists and Engineers (PECASE) and the Hope College Young Alumni Award in 2017. In 2013, he received the Director of National Intelligence Galileo Award and the U.S. Department of Defense David O. Cooke Excellence in Public Administration Award. Ever motivated to share and apply his extensive knowledge, Dykstra mentors university students and junior NSA employees. Dykstra graduated from an SFS program at Iowa State University with a master's degree in information assurance in 2004. He also received a doctoral degree from the University of Maryland Baltimore County, another SFS school, in 2013. Dykstra is currently a cybersecurity expert employed by the NSA.

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

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

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



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

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

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

FUTURE OF CYBERCORPS® SFS PROGRAM

The future of the CyberCorps® SFS program is important to consider within the framework of the broad landscape of national cybersecurity workforce development and education. Cyber threats continue to evolve, and the demand for skilled cybersecurity professionals has never been higher. The CyberCorps® SFS program is an important initiative supporting the 2023 National Cybersecurity Strategy and the 2023 National Cyber Workforce and Education Strategy. The program contributes directly by developing a skilled cyber workforce to help ensure that the Nation's cybersecurity needs are addressed by highly skilled SFS graduates who are prepared to tackle emerging threats.

Looking forward, the CyberCorps® SFS program will be promoting more interdisciplinary approaches, fostering collaborations between cybersecurity and other STEM disciplines. In particular, the program will invest in projects intended to ensure the security of AI, quantum computing, aerospace, semiconductors, and advanced communications technologies. These priority areas have become increasingly integral to national security and technological advancement.

While the CyberCorps® SFS program holds significant promise to support the National Cyber Workforce and Education Strategy and the CHIPS and Science Act priority areas, the current shortage of qualified cybersecurity faculty poses a significant challenge. As the demand for cybersecurity professionals continues to escalate, the need for experienced and knowledgeable faculty to educate the next generation of cybersecurity experts is becoming more intense. To address this need, the SFS program will continue to support professional development opportunities for educators who are interested in cybersecurity education and workforce development.

To promote diversity and inclusion, the CyberCorps® SFS program will continue initiatives to engage underrepresented groups, under-resourced populations, and institutions in rural regions and EPSCoR states. The program will continue engaging with HBCUs, Hispanic-serving institutions (HSIs), and tribal colleges to create tailored pathways for underrepresented students. The program is engaging with community colleges to establish or enhance their cybersecurity programs, which will help to empower students from economically disadvantaged backgrounds to participate in the SFS program. In addition, the program will continue to support novel education and mentoring models to help develop cybersecurity competencies among SFS scholars.

APPENDIX A: POST GRADUATE PLACEMENT RATE BY ENROLLED YEARS

Source: SFS Master Roster and Placement Log as of October 1, 2023.

Enrolled Year	Placed	Non Grad Placed	In Process	Still Looking	Released	Repayment	Total	Graduate Placement Rate[8]	Still Looking within 18 Months	Still in School	Non Grad Release	Non Grad Repayment	Total Awarded SFS
2001	25	0	0	0	6	0	31	81%	0	0	0	0	31
2002	95	0	0	0	16	1	112	85%	0	0	2	1	115
2003	196	0	0	0	16	2	214	92%	0	0	1	4	219
2004	171	0	0	0	3	2	176	97%	0	0	0	9	185
2005	166	0	0	0	2	5	173	96%	0	0	4	5	182
2006	124	0	0	0	0	3	127	98%	0	0	1	5	133
2007	100	0	0	0	0	5	105	95%	0	0	1	5	111
2008	93	0	0	0	0	0	93	100%	0	0	0	1	94
2009	117	0	0	0	1	8	126	93%	0	0	4	3	133
2010	169	0	0	0	1	6	176	96%	0	0	2	3	181
2011	178	1	0	0	2	8	189	95%	0	0	2	4	195
2012	173	0	0	0	0	6	179	97%	0	0	2	5	186
2013	245	0	1	0	1	7	254	97%	0	0	1	13	268
2014	252	0	0	0	3	12	267	94%	0	0	0	10	277
2015	258	0	0	0	1	12	271	95%	0	0	0	6	277
2016	288	3	2	3	0	8	304	96%	0	1	2	6	313
2017	329	3	5	1	0	9	347	97%	1	1	2	6	357
2018	308	3	2	6	1	10	330	95%	2	1	1	5	339
2019	312	2	11	20	1	7	353	92%	11	10	2	8	384
2020	258	4	5	41	0	4	312	86%	47	10	2	4	375
2021	155	1	11	5	0	2	174	96%	86	95	0	9	364
2022	31	1	3	3	0	0	38	92%	31	320	0	2	391
2023	0	0	0	0	0	0	0	0%	1	462	0	0	463
Total	**4043**	**18**	**40**	**79**	**54**	**117**	**4351**	**94%**	**179**	**900**	**29**	**114**	**5573**

[8] 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 October 2023.

Commerce	63
Education	6
Health and Human Services	15
Housing and Urban Development	4
Justice	124
State	36
Treasury	48

Army	222
Navy	396

Argonne National Laboratory	8
Fermi National Accelerator Laboratory	1
Lawrence Berkeley National Laboratory	1
Los Alamos National Laboratory	45
Oak Ridge National Laboratory	28
Sandia National Laboratories	190
SLAC National Accelerator Laboratory	2

FFRDC	529
Aerospace Federally Funded Research and Development Center	23
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)	9
Jet Propulsion Laboratory (NASA)	11
Massachusetts Institute of Technology (MIT) - Lincoln Laboratory	73
MITRE Corporation	243
MITRE Corporation - Center for Advanced Aviation System Development	3
MITRE Corporation - Center for Enterprise Modernization	3
MITRE Corporation - CMS Alliance to Modernize Healthcare	1
MITRE Corporation - National Cybersecurity Center of Excellence	33
MITRE Corporation - National Security Engineering Center	44
National Defense Research Institute/RAND Corp.	1
North American Electric Reliability Corporation (NERC)	1
Software Engineering Institute (SEI)- Carnegie Mellon University	64
Southwest Research Institute	1
Board of Governors of the Federal Reserve System	60
Central Intelligence Agency (CIA)	78
Contractor/Private-Approved	15
Environmental Protection Agency	5
Executive Office of the President	2
Federal Communication Commission	3
Federal Deposit Insurance Corporation (FDIC)	46
Federal Reserve Banks	69
Federal Retirement Thrift Investment Board	1
Federal Trade Commission	3
Freddie Mac	1
General Services Administration	8
Government Accountability Office	52
Judicial Branch	4
National Aeronautics & Space Administration (NASA)	11
Nuclear Regulatory Commission	6
U.S. National Science Foundation (NSF)	7
U.S. Office Of Personnel Management (OPM)	10
Privacy & Civil Liberties Oversight Board (PCLOB)	1
Railroad Retirement Board (RRB)	6
Securities and Exchange Commission (SEC)	4
SFS Cyber Educator	4
Small Business Administration (SBA)	2
Social Security Administration (SSA)	13
Smithsonian	2
State/Local/Tribal	288
Tennessee Valley Authority (TVA)	3
U.S. Agency for Global Media (USAGM)	2
U.S. Agency for International Development (USAID)	4
U.S. Government	22
U.S. Postal Service (USPS)	8
U.S. Senate	5
UARC - John Hopkins University - Applied Physics Laboratory	119
CI Non-Profit	2
Other	1

APPENDIX C: JOB TITLES

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

Advanced Technology Security Specialist
Analyst
Analyst-Cybersecurity-Exp
AOS QCE Associate Professional Staff I
Application Security
Application Software IT Specialist
Applied Cybersecurity Engineer
Applied Research Mathematician
Assistant Cyber Security Engineer
Assistant Software Engineer
Assistant Staff - Engineering
Assistant Teaching Professor of Cybersecurity
Assistant Wargaming Fellow
Associate Artificial Intelligence Engineer
Associate Computer Security Engineer
Associate Cyber Software Engineer
Associate Cybersecurity Engineer
Associate Cybersecurity Specialist
Associate Embedded Security Engineer
Associate IT Auditor
Associate Professional Staff Asymmetric Operation Sector
Associate Professional Staff I
Associate Professional Staff I
Associate Staff I
Associative Professional Staff I
Audit and Compliance College Aide
Barksdale Scholar - Multi-System Reliability Analysis
Capabilities and Development Specialist
Capabilities Development Specialist
Capabilities Development Specialist - CNODP
Capabilities Development Specialist CAECO Intern
Capabilities Developmental Specialist
Civic Digital Fellow
Classified Information Systems Administrator
Cloud Engineer
Computer Scientist
Computer Engineer
Computer Forensic Analyst
Computer Network Defense Analyst
Computer Operator Programmer
Computer Scientist
Computer Scientist SCA-V Team Member
Computer Scientist Uic 60506 Navy Cyber Warfare Development Group
Computer Specialist (Lead Field Support Technician)
Computer Systems Engineer
Computer Systems Architect
Computing Systems Professional
Control Systems Cybersecurity Analyst
Cooperative Education Program
Cooperative Nuclear Counterproliferation
Counterintelligence Agent
Criminal Investigator
Critical Infrastructure Vulnerability Coordination Analyst
Cryptanalytic Computer Scientist
Cryptologic Computer Scientist
Cryptologic Warfare Officer
Cyber
Cyber Analyst
Cyber Analyst II
Cyber Analytics Associate
Cyber Associate Professional Staff I
Cyber Defense Infrastructure Support Specialist
Cyber Engineer Associate Level
Cyber Fellow
Cyber Network Professional - Offensive/Defensive Operations
Cyber New Professional
Cyber Operations Analyst
Cyber Operations Analyst Intermediate
Cyber Ops Engineer
Cyber Policy Analyst
Cyber R and D
Cyber Security Analyst
Cyber Security Co-Op
Cyber Security Engineer
Cyber Security Engineer I
Cyber Security Engineer II
Cyber Security Officer
Cyber Security Researcher
Cyber Security Technical Professional
Cyber Summer School Investigation Track
Cyber Systems Engineer
Cyber Systems Exploitation Researcher

APPENDIX C: JOB TITLES

Cyber Threat Intelligence Analyst
Cybersecurity Analyst
Cybersecurity Analyst - Counter Threat Automation
Cybersecurity Analyst Experienced
Cybersecurity Compliance Agent
Cybersecurity Division Threat Hunting
Cybersecurity Engineer
Cybersecurity Engineer (Temporary Hire Student)
Cybersecurity Engineer Student Trainee
Cybersecurity Instructor
Cybersecurity Intelligence Analyst
Cybersecurity Modeling and Visualization
Cybersecurity Officer
Cybersecurity R+D S+E
Cybersecurity R&D S&E
Cybersecurity Research and Development
Cybersecurity Research Intern
Cybersecurity Reverse Engineer
Cybersecurity Risk Management
Cybersecurity Scientist and Engineer
Cybersecurity Software Engineer
Cybersecurity Specialist
Cybersecurity Technical Staff
Cyberwarfare Operations Officer
Data Analyst
Data Architect
Data Scientist
Data Scientist - US Army Pacific (USARPAC)
Defensive Cybersecurity Co Op
Desktop Engineer Jr.
Developmental Program in the CAE Cyber Summer Program
DevOps Engineer - Associate
DevSecOps Analyst
Digital Investigative Analyst
Digital Network Exploit Analyst
Digital Network Exploitation Analyst
Digital Network Exploitation Analyst (Development Program)
Digital Operations Specialist
Digital Targeter
Discover Analyst
Discover Technical Analyst
Early Career Network Security Engineer - R and D
Electronic Classroom Support Technician

Electronic Technician Trainee
Electronics Engineer
Electronics Technician
Embedded Security Engineer
Energy Industry Analyst (IT)
Engineer
Excelsior Service Fellow at Cyber Command Center
Experienced Cybersecurity Analyst
Exploitation Analyst
Federal Government Employee
Financial Systems Administrator
Financial Systems Specialist (Cyber)
General Engineer
Grad Student in Cyber Systems
Graduate II-Cyber Security
Graduate Student in the Advanced Research
Graduate Student in the Advanced Research in Cyber Systems Group
Graduate Student ST
Hardware-Software Analysis Engineer
HR Business Intelligence and Analytics Analyst
Incident Manager
Information Management Specialist
Information Security Analyst
Information Security Professional I
Information Security Specialist
Information System Security Designer
Information System Security Engineer
Information Systems Auditor I
Information Systems Security Engineer
Information Technology (Infosec)
Information Technology
Information Technology (PCIP)
Information Technology (Student Trainee), GS-2299-7
Information Technology and Cyber Risk Management Analyst
Information Technology and Cyber Risk Management Analyst
Information Technology Auditor
Information Technology Cyber Risk Management Analyst
Information Technology Examination Analyst
Information Technology Management Student Trainee
Information Technology Security Analyst
Information Technology Security Specialist II
Information Technology Specialist
Information Technology Specialist (Security)

APPENDIX C: JOB TITLES

Information Technology Specialist (Security)
Infosec Professional
Instructor-CSE
Intelligence Officer
Intelligence Specialist
Interactive Operator
Intermediate Cyber Operations Specialist
Intermediate Cybersecurity Engineer
Internet and Technology Analyst
Investigative Specialist
ISSE
IT Analyst
IT and Cyber Risk Analyst
IT and Cyber Risk Management Analyst
IT Auditor
IT Auditor I
IT Cyber Risk Management Analyst (ITCA)
IT Cybersecurity Specialist
IT Cybersecurity Specialist (INFOSEC)
IT Cybersecurity Specialist (Technical Support)
IT Cybersecurity Specialist APPSW INFOSEC
IT Examination Analyst
IT Operations Engineer
IT Operations Engineer, Compute A
IT Professional I - Cyber Security Analyst
IT Programmer Analyst
IT Project Manager (PLCYPLN)
IT Security Analyst
IT Security Analyst - IT Programmer Analyst
IT Security Compliance Specialist I
IT Specialist
IT Specialist - GSAIT
IT Specialist (APPSW)
IT Specialist (APPSW/DATAMGT)
IT SPECIALIST (DATAMGT)
IT Specialist (INFOSEC)
IT SPECIALIST (NETWORK)
IT Specialist (PLCYPLN/ENTARCH)
IT Specialist (Security)
IT Specialist (Student Trainee)
IT Specialist (SYSADMIN/CUSTSPT)
IT Specialist (Systems Analysis)
IT Specialist Digital Forensic Examiner
IT Specialist Forensic Examiner (ITSFE)
IT Specialist- Digital Forensic Examiner
IT Specialist (PTOJMGT)
IT Specialist (SYSADMIN CUSTSPT)
IT Specialist/IT Cyber Specialist (INFO SEC)
IT Systems Analyst and System Administrator
IT Systems Specialist, Associate
Law Student Volunteer
Management and Program Analyst
Management Officer
Member of Technical Staff
MSIIP Program Participant
National Security Division/Counterintelligence and Export Control Section
Network Cybersecurity Engineer
Network Defense Analyst
Network Security Engineer
Network Systems Administrator I
Operational Support Technician
Operations Analyst II
Operations Research Analyst
Palace Acquire IT Specialist
Pathways Recent Graduate IT Specialist (APPSW)
Pathways Student Trainee
Pathways Student Trainee (Information Technology (INFOSEC))
PCIP
Penetration Tester
Post-Master Student in the Space Data Science and Systems Group
Post Masters ST
Post-masters Research Assistant
Program Analyst (Cyber)
Program Assistant
Program Director
Program Participant
Programmer Analyst I
Programmer and PCI Compliance Officer
R and D S and E Cybersecurity
R and D S and E in Systems Research and Analysis
R and D S and E, Cybersecurity
R and D Sand E, Computer Science
R and D Scientist II
R and D, S and E, Cybersecurity
R&D S&E, Cybersecurity
RD Cybersecurity Engineer

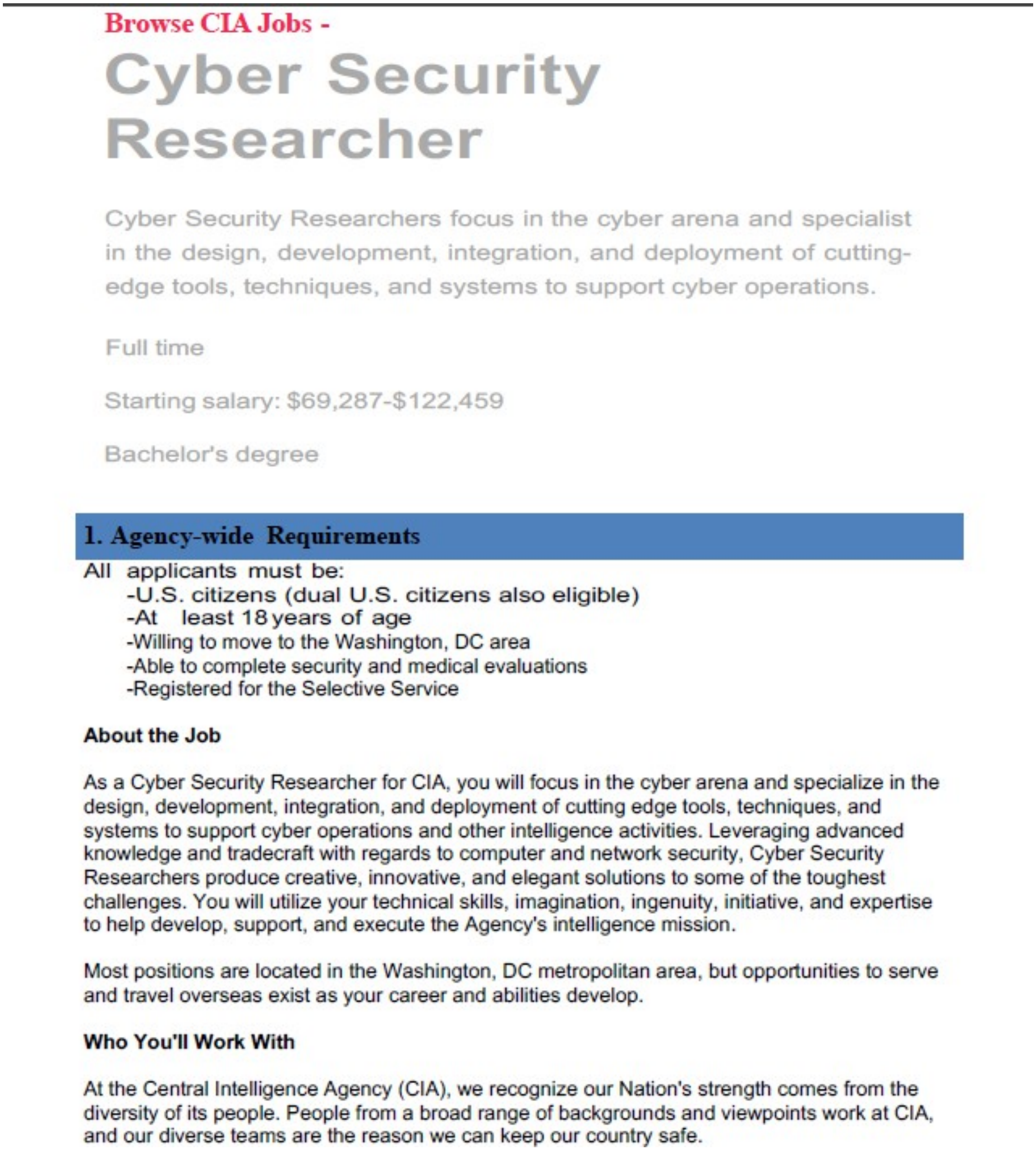
APPENDIX C: JOB TITLES

RD SE computer science
RD SE Cybersecurity
RD SE Cybersecurity (Early Career)
RD SE Cybersecurity Member
RD SE, Cybersecurity
Reliable Navigation in Urban Environments
Research and Development Associate
Research and development computer science
Research and Development Engineering
Research and Development Software Engineering - Cybersecurity
Research and Development Software Engineering Cybersecurity
Research Assistant
Research Associate
Research Computer Scientist
Research Development, Computer Science
Research Engineer II
Researcher II
RF Design Engineer
R&D SnE Cybersecurity
SCEP - Information Technology
Science and Engineering Cybersecurity
Scientist
Secure Data Driven Manufacturing Process Control Engineer
Secure Software Specialist
Security Network Architect
Security Operations Engineer
Senior Container Platform Engineer
Senior Cyber Engineer
Senior Professional Staff I
Senior Software Systems Engineer
Service Delivery Intern
Signal Officer
Signal Processing Engineer
Software and UI Engineer
Software Developer
Software Engineer
Software Engineer - Information Security Team
Software Engineer Submarine and Unmanned Systems
Software Support Specialist
Special Agent
Sr Professional Staff I
STEM Student Employment Program
Student Cooperative
Student success coordinator
Summer Associate
Summer Audit Intern 2023
Summer Signals Intelligence Collection Program
Supervisory Development Associate in Cyber and IT Risk
System Vulnerability Analyst
Systems Analyst II
Systems Engineer
Systems Programmer II
Systems Security Engineer
Technical Specialist
Technical Staff
Technical Support Engineer
Technology Support Technician
Telecommunications Specialist
Temporary Instructional Faculty
Tenure Track Assistant Professor
TITANS CA Center for Cyber Defenders Intern
TITANS Cybersecurity
TITANS Cybersecurity - R and D intern
TITANS Cybersecurity Graduate Intern
TITANS Graduate Summer Intern
Visiting Instructor
Wireless Security Analyst

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.



Browse CIA Jobs -

Cyber Security Researcher

Cyber Security Researchers focus in the cyber arena and specialist in the design, development, integration, and deployment of cutting-edge tools, techniques, and systems to support cyber operations.

Full time

Starting salary: $69,287-$122,459

Bachelor's degree

1. Agency-wide Requirements

All applicants must be:

- -U.S. citizens (dual U.S. citizens also eligible)
- -At least 18 years of age
- -Willing to move to the Washington, DC area
- -Able to complete security and medical evaluations
- -Registered for the Selective Service

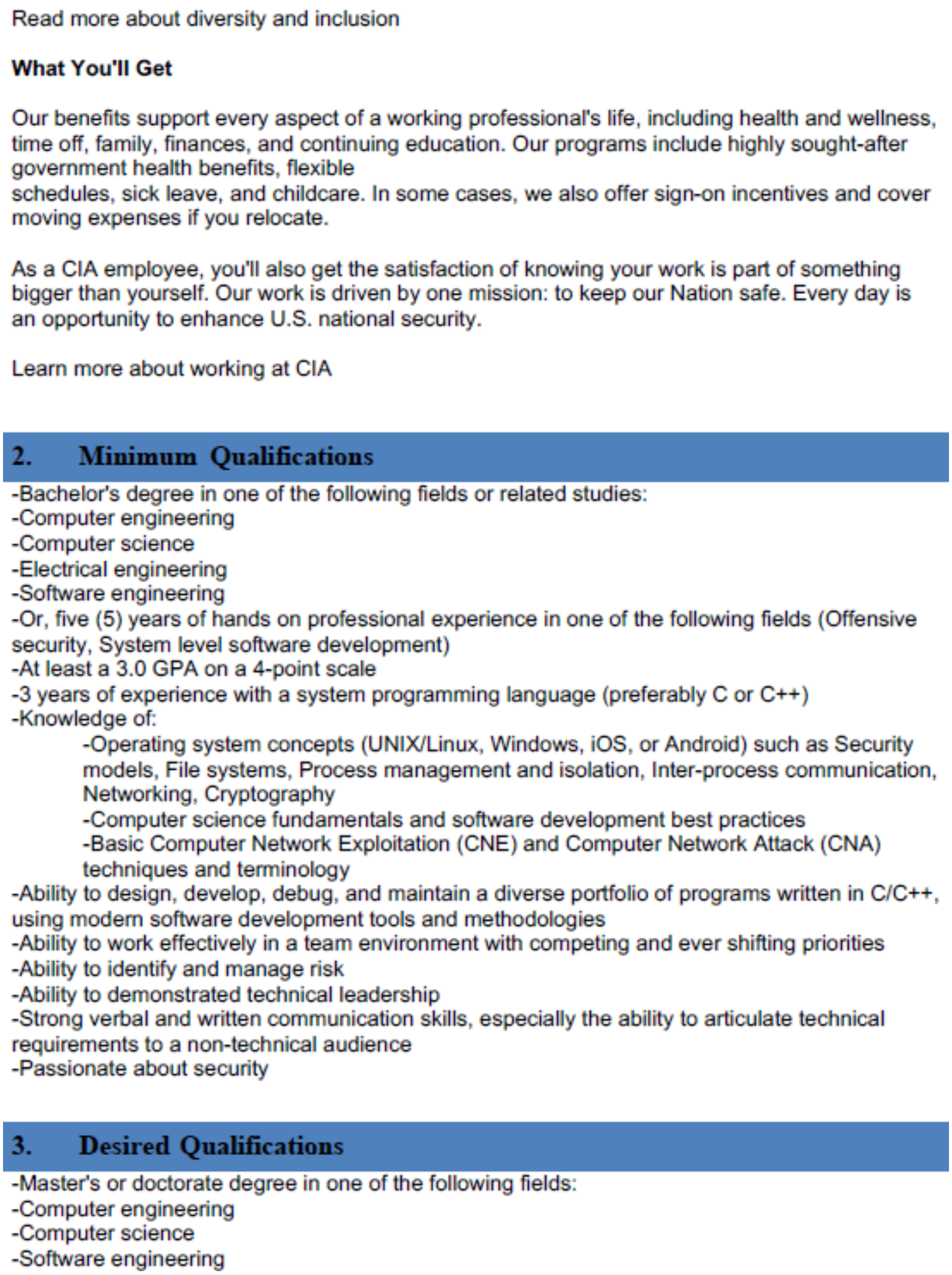
About the Job

As a Cyber Security Researcher for CIA, you will focus in the cyber arena and specialize in the design, development, integration, and deployment of cutting edge tools, techniques, and systems to support cyber operations and other intelligence activities. Leveraging advanced knowledge and tradecraft with regards to computer and network security, Cyber Security Researchers produce creative, innovative, and elegant solutions to some of the toughest challenges. You will utilize your technical skills, imagination, ingenuity, initiative, and expertise to help develop, support, and execute the Agency's intelligence mission.

Most positions are located in the Washington, DC metropolitan area, but opportunities to serve and travel overseas exist as your career and abilities develop.

Who You'll Work With

At the Central Intelligence Agency (CIA), we recognize our Nation's strength comes from the diversity of its people. People from a broad range of backgrounds and viewpoints work at CIA, and our diverse teams are the reason we can keep our country safe.



Read more about diversity and inclusion

What You'll Get

Our benefits support every aspect of a working professional's life, including health and wellness, time off, family, finances, and continuing education. Our programs include highly sought-after government health benefits, flexible
schedules, sick leave, and childcare. In some cases, we also offer sign-on incentives and cover moving expenses if you relocate.

As a CIA employee, you'll also get the satisfaction of knowing your work is part of something bigger than yourself. Our work is driven by one mission: to keep our Nation safe. Every day is an opportunity to enhance U.S. national security.

Learn more about working at CIA

2. Minimum Qualifications

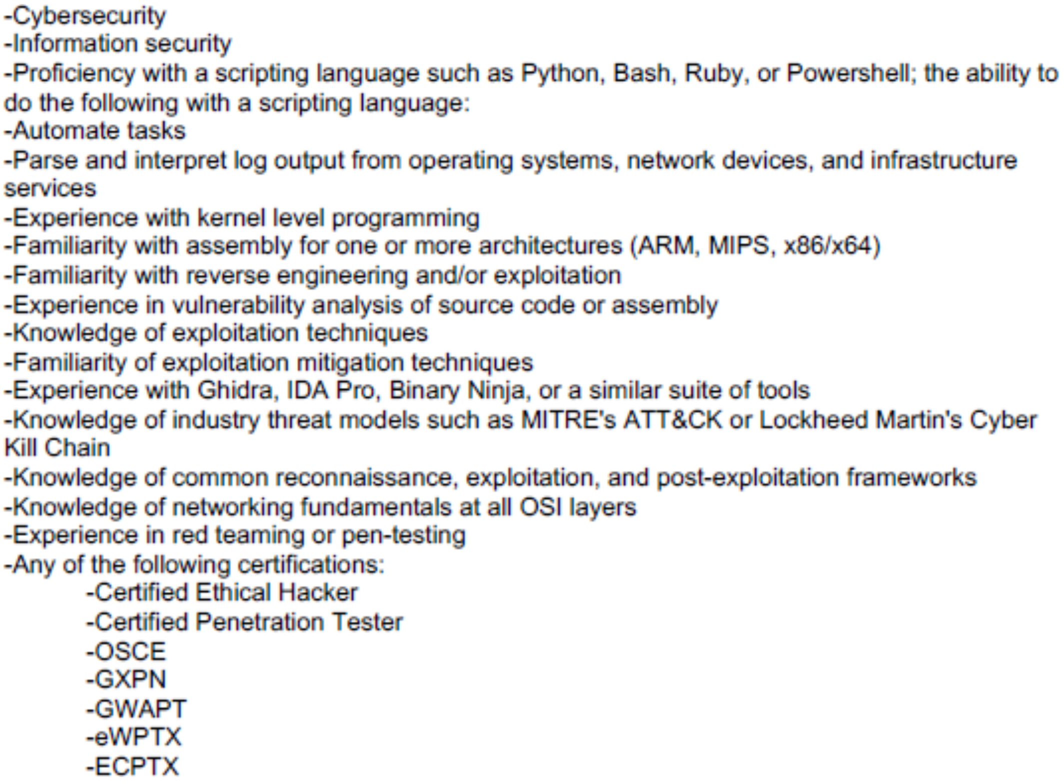
-Bachelor's degree in one of the following fields or related studies:
-Computer engineering
-Computer science
-Electrical engineering
-Software engineering
-Or, five (5) years of hands on professional experience in one of the following fields (Offensive security, System level software development)
-At least a 3.0 GPA on a 4-point scale
-3 years of experience with a system programming language (preferably C or C++)
-Knowledge of:

-Operating system concepts (UNIX/Linux, Windows, iOS, or Android) such as Security models, File systems, Process management and isolation, Inter-process communication, Networking, Cryptography
-Computer science fundamentals and software development best practices
-Basic Computer Network Exploitation (CNE) and Computer Network Attack (CNA) techniques and terminology

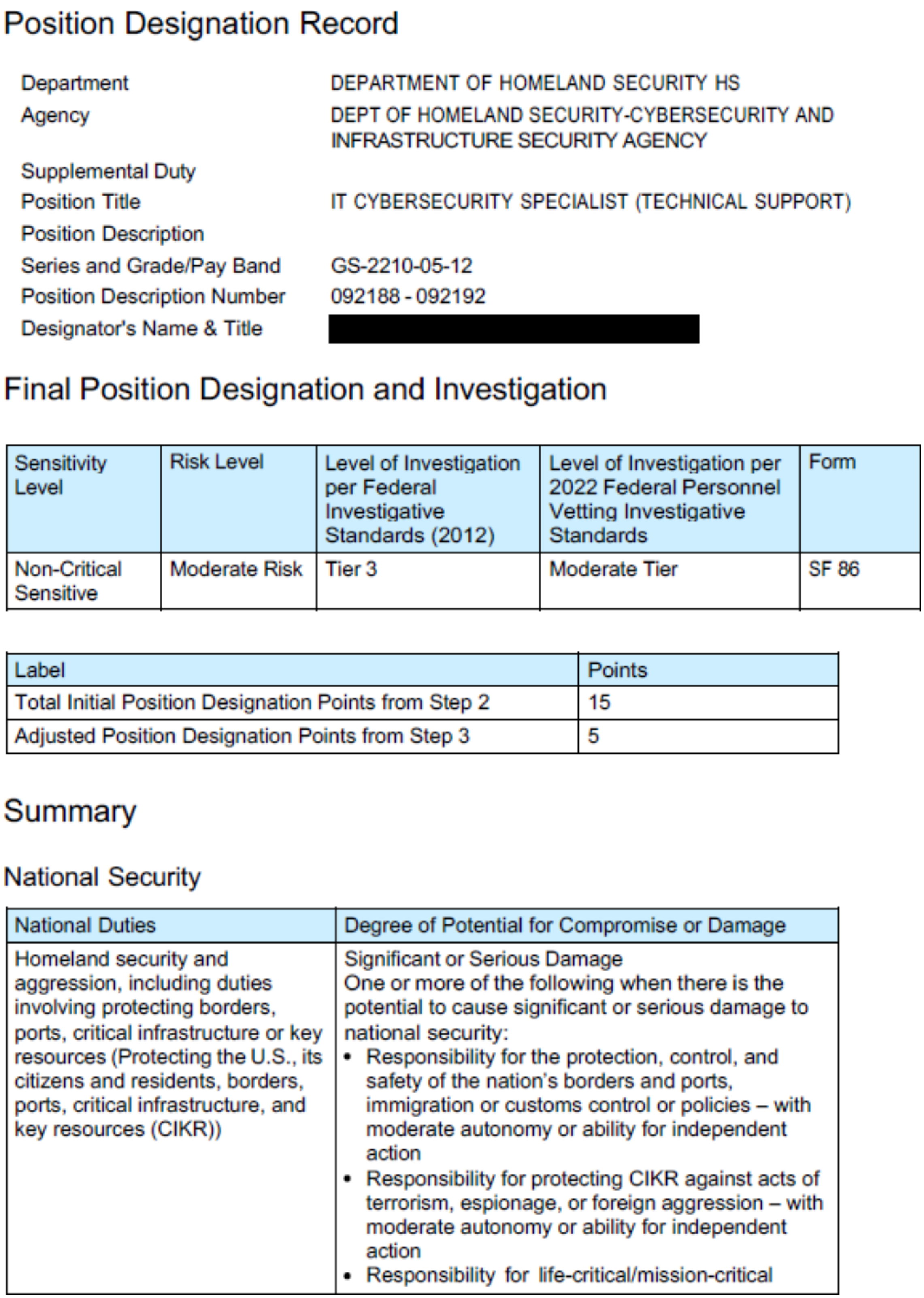
-Ability to design, develop, debug, and maintain a diverse portfolio of programs written in C/C++, using modern software development tools and methodologies
-Ability to work effectively in a team environment with competing and ever shifting priorities
-Ability to identify and manage risk
-Ability to demonstrated technical leadership
-Strong verbal and written communication skills, especially the ability to articulate technical requirements to a non-technical audience
-Passionate about security

3. Desired Qualifications

-Master's or doctorate degree in one of the following fields:
-Computer engineering
-Computer science
-Software engineering



-Cybersecurity
-Information security
-Proficiency with a scripting language such as Python, Bash, Ruby, or Powershell; the ability to do the following with a scripting language:
-Automate tasks
-Parse and interpret log output from operating systems, network devices, and infrastructure services
-Experience with kernel level programming
-Familiarity with assembly for one or more architectures (ARM, MIPS, x86/x64)
-Familiarity with reverse engineering and/or exploitation
-Experience in vulnerability analysis of source code or assembly
-Knowledge of exploitation techniques
-Familiarity of exploitation mitigation techniques
-Experience with Ghidra, IDA Pro, Binary Ninja, or a similar suite of tools
-Knowledge of industry threat models such as MITRE's ATT&CK or Lockheed Martin's Cyber Kill Chain
-Knowledge of common reconnaissance, exploitation, and post-exploitation frameworks
-Knowledge of networking fundamentals at all OSI layers
-Experience in red teaming or pen-testing
-Any of the following certifications:
    -Certified Ethical Hacker
    -Certified Penetration Tester
    -OSCE
    -GXPN
    -GWAPT
    -eWPTX
    -ECPTX



Position Designation Record

Department	DEPARTMENT OF HOMELAND SECURITY HS
Agency	DEPT OF HOMELAND SECURITY-CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
Supplemental Duty	
Position Title	IT CYBERSECURITY SPECIALIST (TECHNICAL SUPPORT)
Position Description	
Series and Grade/Pay Band	GS-2210-05-12
Position Description Number	092188 - 092192
Designator's Name & Title	[redacted]

Final Position Designation and Investigation

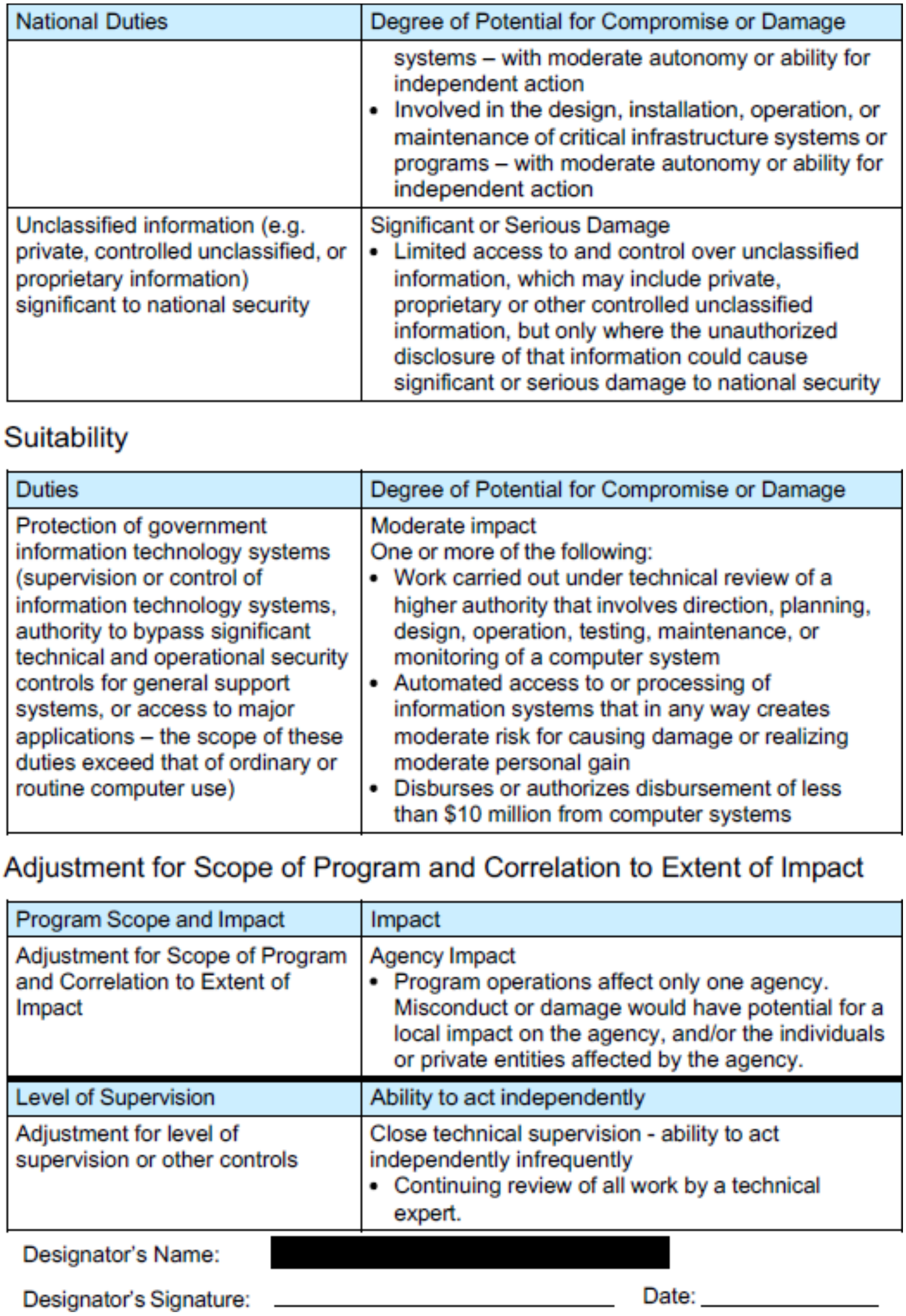
Sensitivity Level	Risk Level	Level of Investigation per Federal Investigative Standards (2012)	Level of Investigation per 2022 Federal Personnel Vetting Investigative Standards	Form
Non-Critical Sensitive	Moderate Risk	Tier 3	Moderate Tier	SF 86

Label	Points
Total Initial Position Designation Points from Step 2	15
Adjusted Position Designation Points from Step 3	5

Summary

National Security

National Duties	Degree of Potential for Compromise or Damage
Homeland security and aggression, including duties involving protecting borders, ports, critical infrastructure or key resources (Protecting the U.S., its citizens and residents, borders, ports, critical infrastructure, and key resources (CIKR))	Significant or Serious Damage One or more of the following when there is the potential to cause significant or serious damage to national security: • Responsibility for the protection, control, and safety of the nation's borders and ports, immigration or customs control or policies – with moderate autonomy or ability for independent action • Responsibility for protecting CIKR against acts of terrorism, espionage, or foreign aggression – with moderate autonomy or ability for independent action • Responsibility for life-critical/mission-critical



National Duties	Degree of Potential for Compromise or Damage
	systems – with moderate autonomy or ability for independent action • Involved in the design, installation, operation, or maintenance of critical infrastructure systems or programs – with moderate autonomy or ability for independent action
Unclassified information (e.g. private, controlled unclassified, or proprietary information) significant to national security	Significant or Serious Damage • Limited access to and control over unclassified information, which may include private, proprietary or other controlled unclassified information, but only where the unauthorized disclosure of that information could cause significant or serious damage to national security

Suitability

Duties	Degree of Potential for Compromise or Damage
Protection of government information technology systems (supervision or control of information technology systems, authority to bypass significant technical and operational security controls for general support systems, or access to major applications – the scope of these duties exceed that of ordinary or routine computer use)	Moderate impact One or more of the following: • Work carried out under technical review of a higher authority that involves direction, planning, design, operation, testing, maintenance, or monitoring of a computer system • Automated access to or processing of information systems that in any way creates moderate risk for causing damage or realizing moderate personal gain • Disburses or authorizes disbursement of less than $10 million from computer systems

Adjustment for Scope of Program and Correlation to Extent of Impact

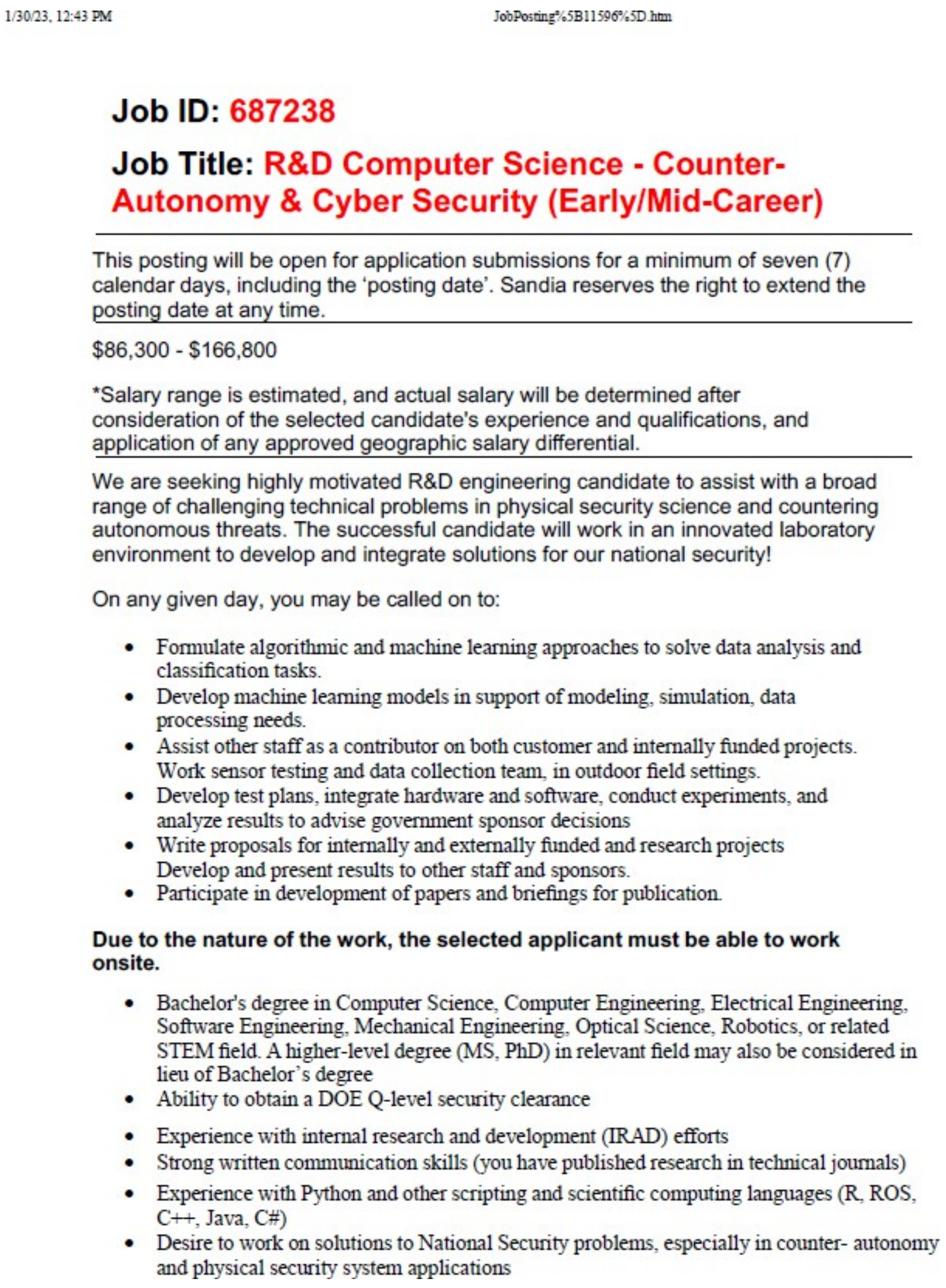
Program Scope and Impact	Impact
Adjustment for Scope of Program and Correlation to Extent of Impact	Agency Impact • Program operations affect only one agency. Misconduct or damage would have potential for a local impact on the agency, and/or the individuals or private entities affected by the agency.

Level of Supervision	Ability to act independently
Adjustment for level of supervision or other controls	Close technical supervision - ability to act independently infrequently • Continuing review of all work by a technical expert.

Designator's Name: [redacted]

Designator's Signature: ______________________ Date: ____________

APPENDIX D: SAMPLE JOB DESCRIPTIONS



1/30/23, 12:43 PM JobPosting%5B11596%5D.htm

Job ID: 687238

Job Title: R&D Computer Science - Counter-Autonomy & Cyber Security (Early/Mid-Career)

This posting will be open for application submissions for a minimum of seven (7) calendar days, including the 'posting date'. Sandia reserves the right to extend the posting date at any time.

$86,300 - $166,800

*Salary range is estimated, and actual salary will be determined after consideration of the selected candidate's experience and qualifications, and application of any approved geographic salary differential.

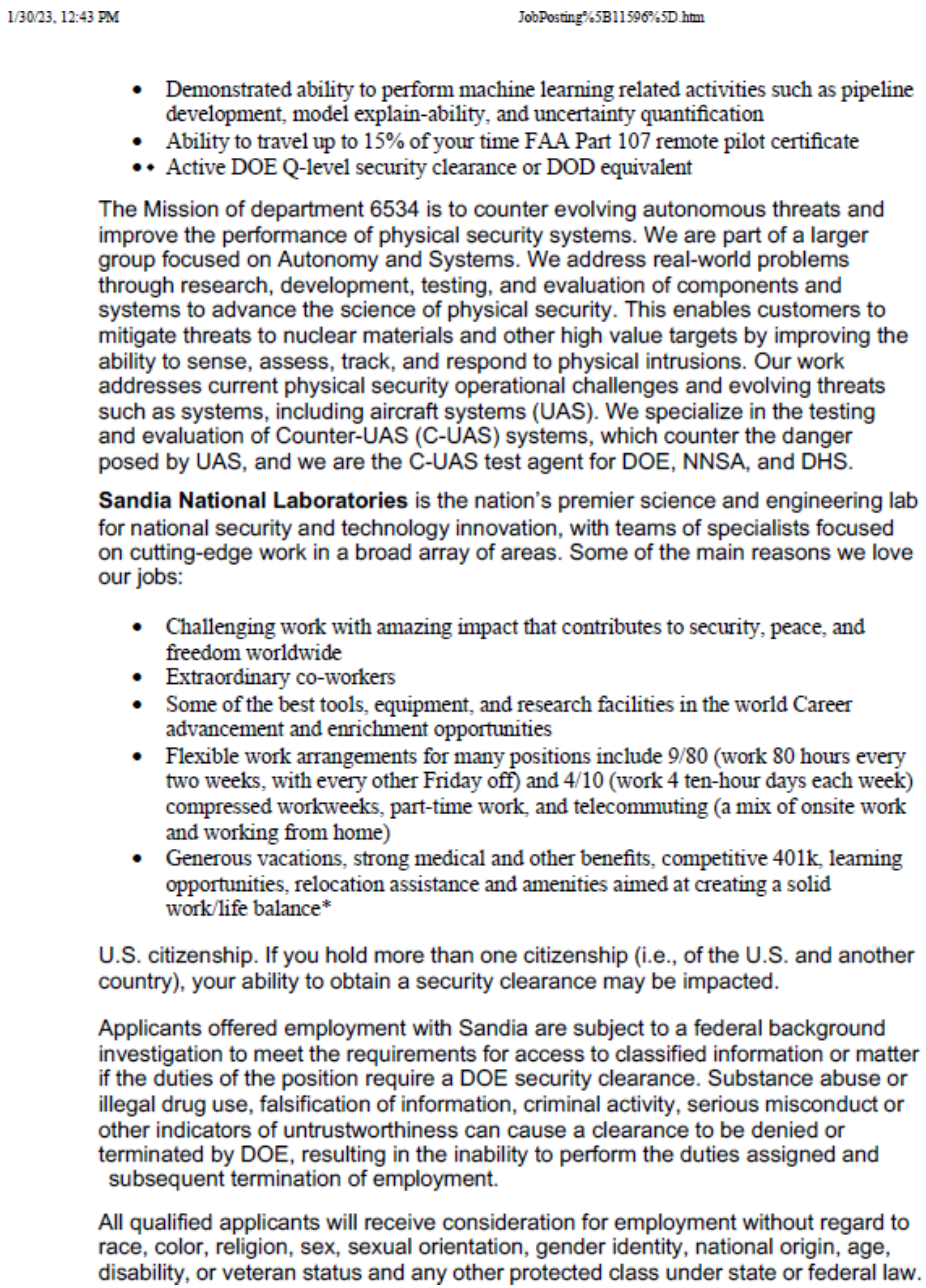
We are seeking highly motivated R&D engineering candidate to assist with a broad range of challenging technical problems in physical security science and countering autonomous threats. The successful candidate will work in an innovated laboratory environment to develop and integrate solutions for our national security!

On any given day, you may be called on to:

- Formulate algorithmic and machine learning approaches to solve data analysis and classification tasks.
- Develop machine learning models in support of modeling, simulation, data processing needs.
- Assist other staff as a contributor on both customer and internally funded projects. Work sensor testing and data collection team, in outdoor field settings.
- Develop test plans, integrate hardware and software, conduct experiments, and analyze results to advise government sponsor decisions
- Write proposals for internally and externally funded and research projects Develop and present results to other staff and sponsors.
- Participate in development of papers and briefings for publication.

Due to the nature of the work, the selected applicant must be able to work onsite.

- Bachelor's degree in Computer Science, Computer Engineering, Electrical Engineering, Software Engineering, Mechanical Engineering, Optical Science, Robotics, or related STEM field. A higher-level degree (MS, PhD) in relevant field may also be considered in lieu of Bachelor's degree
- Ability to obtain a DOE Q-level security clearance
- Experience with internal research and development (IRAD) efforts
- Strong written communication skills (you have published research in technical journals)
- Experience with Python and other scripting and scientific computing languages (R, ROS, C++, Java, C#)
- Desire to work on solutions to National Security problems, especially in counter- autonomy and physical security system applications



1/30/23, 12:43 PM JobPosting%5B11596%5D.htm

- Demonstrated ability to perform machine learning related activities such as pipeline development, model explain-ability, and uncertainty quantification
- Ability to travel up to 15% of your time FAA Part 107 remote pilot certificate
- • Active DOE Q-level security clearance or DOD equivalent

The Mission of department 6534 is to counter evolving autonomous threats and improve the performance of physical security systems. We are part of a larger group focused on Autonomy and Systems. We address real-world problems through research, development, testing, and evaluation of components and systems to advance the science of physical security. This enables customers to mitigate threats to nuclear materials and other high value targets by improving the ability to sense, assess, track, and respond to physical intrusions. Our work addresses current physical security operational challenges and evolving threats such as systems, including aircraft systems (UAS). We specialize in the testing and evaluation of Counter-UAS (C-UAS) systems, which counter the danger posed by UAS, and we are the C-UAS test agent for DOE, NNSA, and DHS.

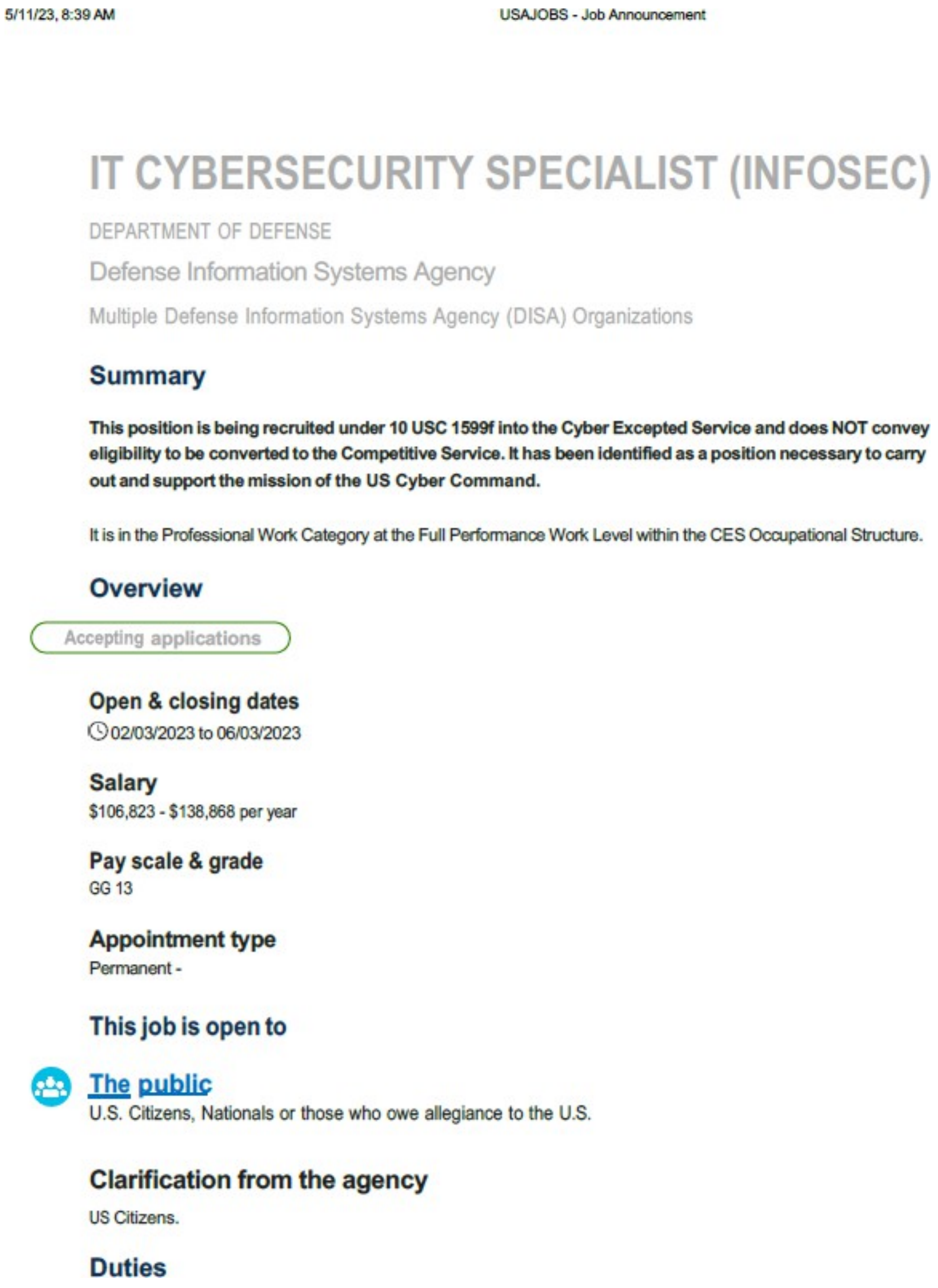
Sandia National Laboratories is the nation's premier science and engineering lab for national security and technology innovation, with teams of specialists focused on cutting-edge work in a broad array of areas. Some of the main reasons we love our jobs:

- Challenging work with amazing impact that contributes to security, peace, and freedom worldwide
- Extraordinary co-workers
- Some of the best tools, equipment, and research facilities in the world Career advancement and enrichment opportunities
- Flexible work arrangements for many positions include 9/80 (work 80 hours every two weeks, with every other Friday off) and 4/10 (work 4 ten-hour days each week) compressed workweeks, part-time work, and telecommuting (a mix of onsite work and working from home)
- Generous vacations, strong medical and other benefits, competitive 401k, learning opportunities, relocation assistance and amenities aimed at creating a solid work/life balance*

U.S. citizenship. If you hold more than one citizenship (i.e., of the U.S. and another country), your ability to obtain a security clearance may be impacted.

Applicants offered employment with Sandia are subject to a federal background investigation to meet the requirements for access to classified information or matter if the duties of the position require a DOE security clearance. Substance abuse or illegal drug use, falsification of information, criminal activity, serious misconduct or other indicators of untrustworthiness can cause a clearance to be denied or terminated by DOE, resulting in the inability to perform the duties assigned and subsequent termination of employment.

All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, age, disability, or veteran status and any other protected class under state or federal law.



5/11/23, 8:39 AM USAJOBS - Job Announcement

IT CYBERSECURITY SPECIALIST (INFOSEC)

DEPARTMENT OF DEFENSE

Defense Information Systems Agency

Multiple Defense Information Systems Agency (DISA) Organizations

Summary

This position is being recruited under 10 USC 1599f into the Cyber Excepted Service and does NOT convey eligibility to be converted to the Competitive Service. It has been identified as a position necessary to carry out and support the mission of the US Cyber Command.

It is in the Professional Work Category at the Full Performance Work Level within the CES Occupational Structure.

Overview

Accepting applications

Open & closing dates
02/03/2023 to 06/03/2023

Salary
$106,823 - $138,868 per year

Pay scale & grade
GG 13

Appointment type
Permanent -

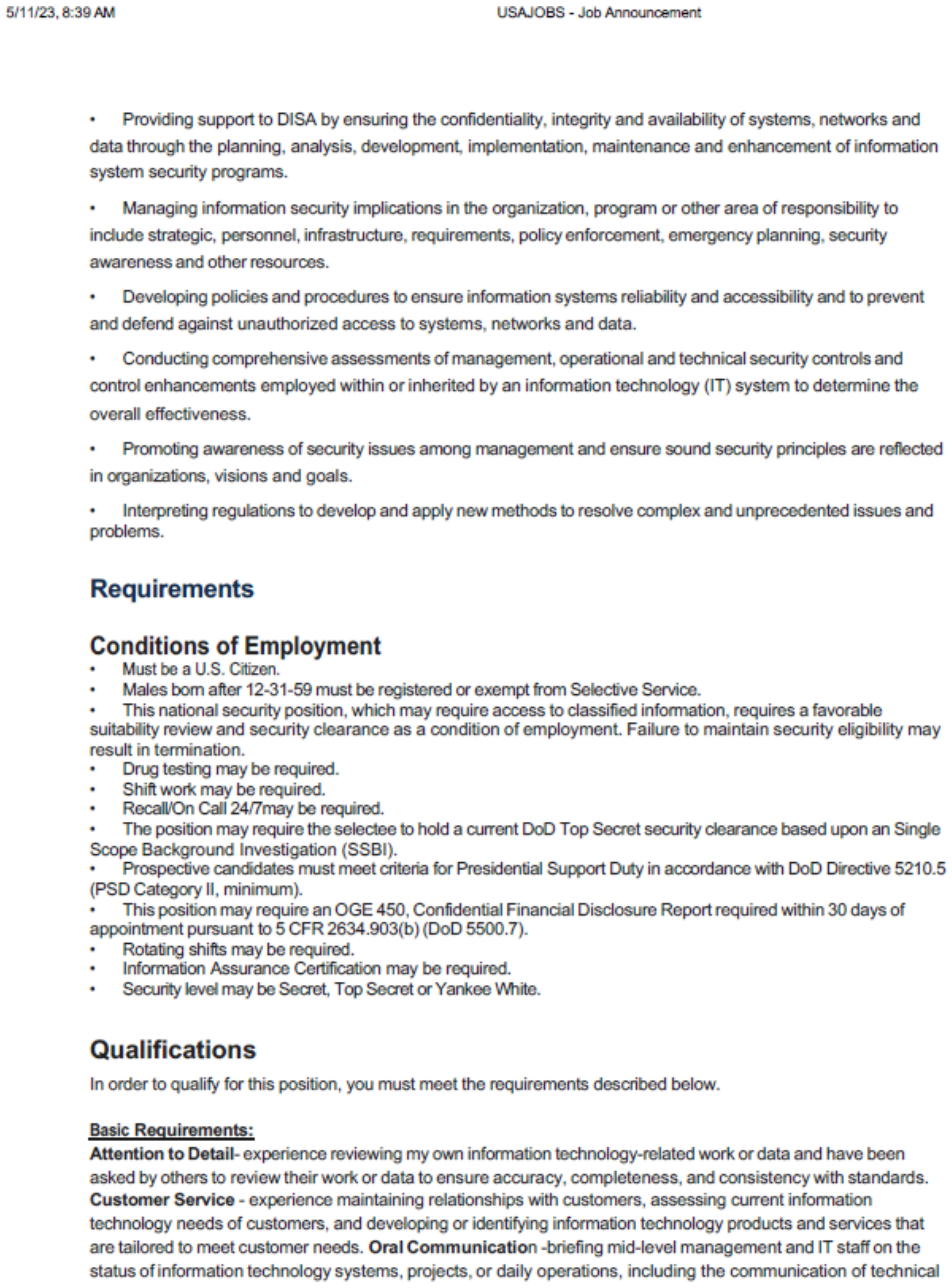
This job is open to

The public
U.S. Citizens, Nationals or those who owe allegiance to the U.S.

Clarification from the agency

US Citizens.

Duties



5/11/23, 8:39 AM USAJOBS - Job Announcement

- Providing support to DISA by ensuring the confidentiality, integrity and availability of systems, networks and data through the planning, analysis, development, implementation, maintenance and enhancement of information system security programs.
- Managing information security implications in the organization, program or other area of responsibility to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness and other resources.
- Developing policies and procedures to ensure information systems reliability and accessibility and to prevent and defend against unauthorized access to systems, networks and data.
- Conducting comprehensive assessments of management, operational and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness.
- Promoting awareness of security issues among management and ensure sound security principles are reflected in organizations, visions and goals.
- Interpreting regulations to develop and apply new methods to resolve complex and unprecedented issues and problems.

Requirements

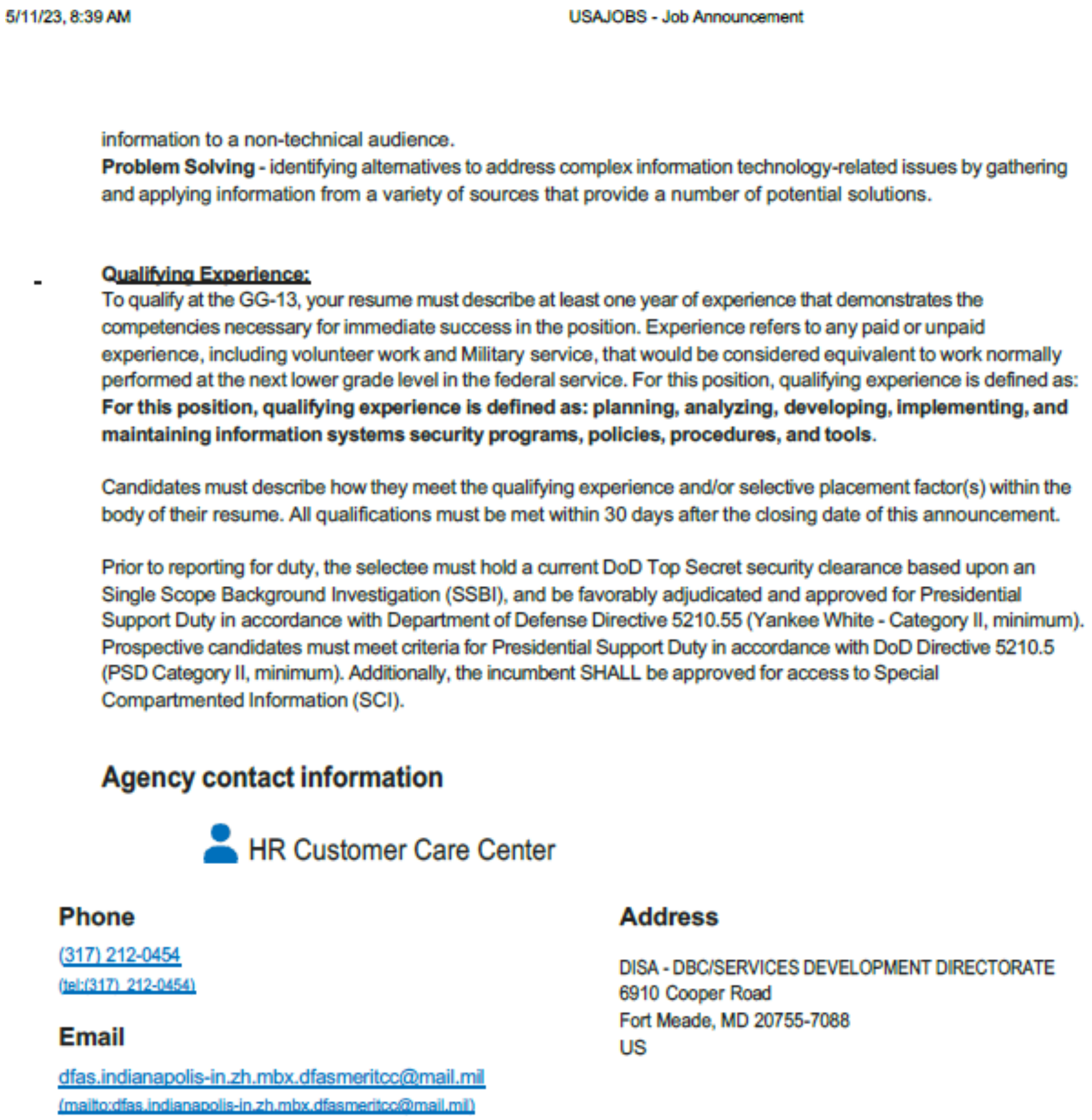
Conditions of Employment

- Must be a U.S. Citizen.
- Males born after 12-31-59 must be registered or exempt from Selective Service.
- This national security position, which may require access to classified information, requires a favorable suitability review and security clearance as a condition of employment. Failure to maintain security eligibility may result in termination.
- Drug testing may be required.
- Shift work may be required.
- Recall/On Call 24/7may be required.
- The position may require the selectee to hold a current DoD Top Secret security clearance based upon an Single Scope Background Investigation (SSBI).
- Prospective candidates must meet criteria for Presidential Support Duty in accordance with DoD Directive 5210.5 (PSD Category II, minimum).
- This position may require an OGE 450, Confidential Financial Disclosure Report required within 30 days of appointment pursuant to 5 CFR 2634.903(b) (DoD 5500.7).
- Rotating shifts may be required.
- Information Assurance Certification may be required.
- Security level may be Secret, Top Secret or Yankee White.

Qualifications

In order to qualify for this position, you must meet the requirements described below.

Basic Requirements:
Attention to Detail- experience reviewing my own information technology-related work or data and have been asked by others to review their work or data to ensure accuracy, completeness, and consistency with standards. **Customer Service** - experience maintaining relationships with customers, assessing current information technology needs of customers, and developing or identifying information technology products and services that are tailored to meet customer needs. **Oral Communication** -briefing mid-level management and IT staff on the status of information technology systems, projects, or daily operations, including the communication of technical



5/11/23, 8:39 AM USAJOBS - Job Announcement

information to a non-technical audience.
Problem Solving - identifying alternatives to address complex information technology-related issues by gathering and applying information from a variety of sources that provide a number of potential solutions.

- **Qualifying Experience:**

To qualify at the GG-13, your resume must describe at least one year of experience that demonstrates the competencies necessary for immediate success in the position. Experience refers to any paid or unpaid experience, including volunteer work and Military service, that would be considered equivalent to work normally performed at the next lower grade level in the federal service. For this position, qualifying experience is defined as: **For this position, qualifying experience is defined as: planning, analyzing, developing, implementing, and maintaining information systems security programs, policies, procedures, and tools**.

Candidates must describe how they meet the qualifying experience and/or selective placement factor(s) within the body of their resume. All qualifications must be met within 30 days after the closing date of this announcement.

Prior to reporting for duty, the selectee must hold a current DoD Top Secret security clearance based upon an Single Scope Background Investigation (SSBI), and be favorably adjudicated and approved for Presidential Support Duty in accordance with Department of Defense Directive 5210.55 (Yankee White - Category II, minimum). Prospective candidates must meet criteria for Presidential Support Duty in accordance with DoD Directive 5210.5 (PSD Category II, minimum). Additionally, the incumbent SHALL be approved for access to Special Compartmented Information (SCI).

Agency contact information

HR Customer Care Center

Phone

(317) 212-0454
(tel:(317) 212-0454)

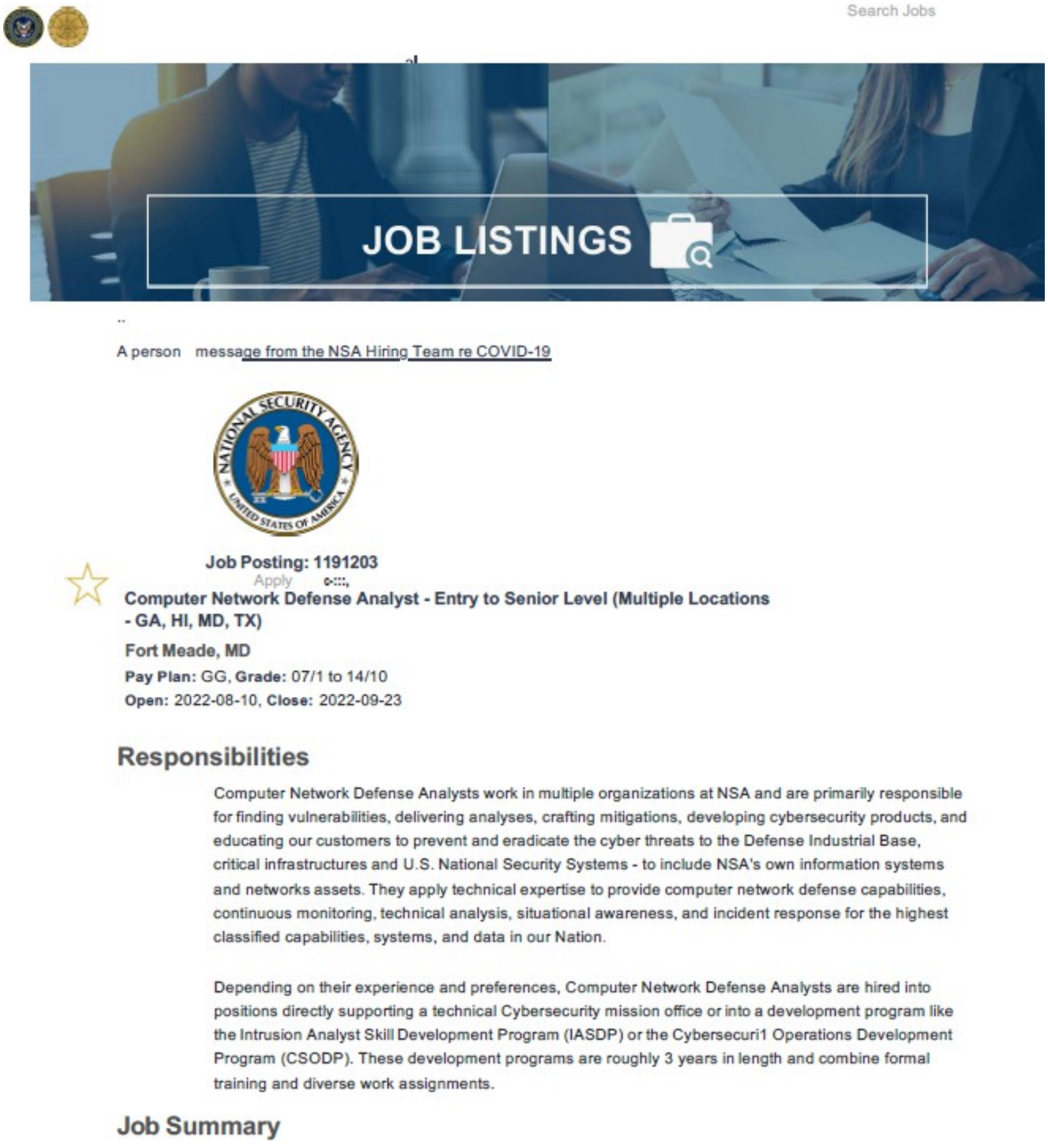
Email

dfas.indianapolis-in.zh.mbx.dfasmeritcc@mail.mil
(mailto:dfas.indianapolis-in.zh.mbx.dfasmeritcc@mail.mil)

Address

DISA - DBC/SERVICES DEVELOPMENT DIRECTORATE
6910 Cooper Road
Fort Meade, MD 20755-7088
US

APPENDIX D: SAMPLE JOB DESCRIPTIONS



A person   message from the NSA Hiring Team re COVID-19

Job Posting: 1191203

Computer Network Defense Analyst - Entry to Senior Level (Multiple Locations - GA, HI, MD, TX)

Fort Meade, MD

Pay Plan: GG, **Grade:** 07/1 to 14/10

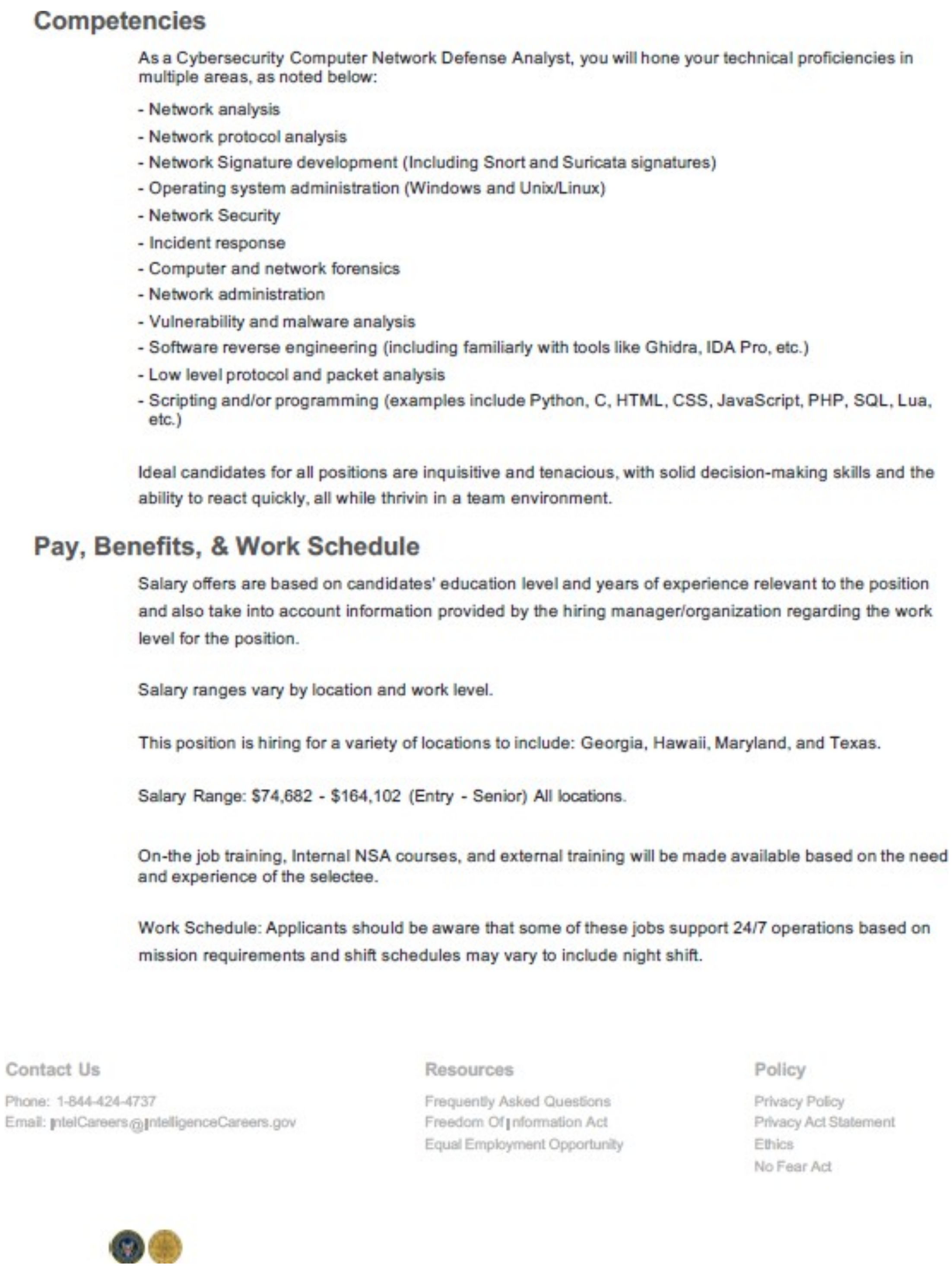
Open: 2022-08-10, **Close:** 2022-09-23

Responsibilities

Computer Network Defense Analysts work in multiple organizations at NSA and are primarily responsible for finding vulnerabilities, delivering analyses, crafting mitigations, developing cybersecurity products, and educating our customers to prevent and eradicate the cyber threats to the Defense Industrial Base, critical infrastructures and U.S. National Security Systems - to include NSA's own information systems and networks assets. They apply technical expertise to provide computer network defense capabilities, continuous monitoring, technical analysis, situational awareness, and incident response for the highest classified capabilities, systems, and data in our Nation.

Depending on their experience and preferences, Computer Network Defense Analysts are hired into positions directly supporting a technical Cybersecurity mission office or into a development program like the Intrusion Analyst Skill Development Program (IASDP) or the Cybersecuri1 Operations Development Program (CSODP). These development programs are roughly 3 years in length and combine formal training and diverse work assignments.

Job Summary



Competencies

As a Cybersecurity Computer Network Defense Analyst, you will hone your technical proficiencies in multiple areas, as noted below:

- Network analysis
- Network protocol analysis
- Network Signature development (Including Snort and Suricata signatures)
- Operating system administration (Windows and Unix/Linux)
- Network Security
- Incident response
- Computer and network forensics
- Network administration
- Vulnerability and malware analysis
- Software reverse engineering (including familiarly with tools like Ghidra, IDA Pro, etc.)
- Low level protocol and packet analysis
- Scripting and/or programming (examples include Python, C, HTML, CSS, JavaScript, PHP, SQL, Lua, etc.)

Ideal candidates for all positions are inquisitive and tenacious, with solid decision-making skills and the ability to react quickly, all while thrivin in a team environment.

Pay, Benefits, & Work Schedule

Salary offers are based on candidates' education level and years of experience relevant to the position and also take into account information provided by the hiring manager/organization regarding the work level for the position.

Salary ranges vary by location and work level.

This position is hiring for a variety of locations to include: Georgia, Hawaii, Maryland, and Texas.

Salary Range: $74,682 - $164,102 (Entry - Senior) All locations.

On-the job training, Internal NSA courses, and external training will be made available based on the need and experience of the selectee.

Work Schedule: Applicants should be aware that some of these jobs support 24/7 operations based on mission requirements and shift schedules may vary to include night shift.

Contact Us

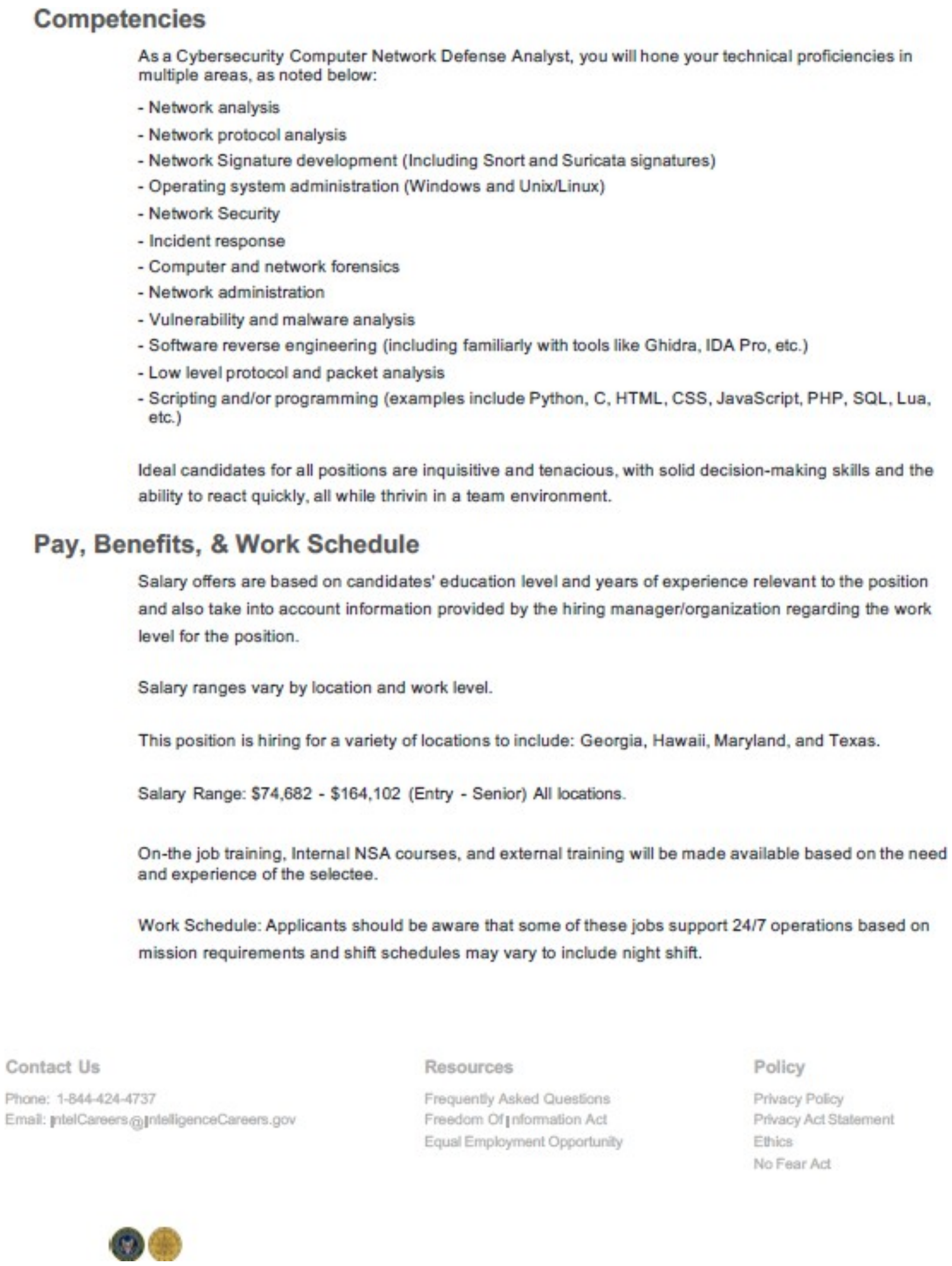
Phone: 1-844-424-4737
Email: IntelCareers@IntelligenceCareers.gov

Resources

Frequently Asked Questions
Freedom Of Information Act
Equal Employment Opportunity

Policy

Privacy Policy
Privacy Act Statement
Ethics
No Fear Act



Competencies

As a Cybersecurity Computer Network Defense Analyst, you will hone your technical proficiencies in multiple areas, as noted below:

- Network analysis
- Network protocol analysis
- Network Signature development (Including Snort and Suricata signatures)
- Operating system administration (Windows and Unix/Linux)
- Network Security
- Incident response
- Computer and network forensics
- Network administration
- Vulnerability and malware analysis
- Software reverse engineering (including familiarly with tools like Ghidra, IDA Pro, etc.)
- Low level protocol and packet analysis
- Scripting and/or programming (examples include Python, C, HTML, CSS, JavaScript, PHP, SQL, Lua, etc.)

Ideal candidates for all positions are inquisitive and tenacious, with solid decision-making skills and the ability to react quickly, all while thrivin in a team environment.

Pay, Benefits, & Work Schedule

Salary offers are based on candidates' education level and years of experience relevant to the position and also take into account information provided by the hiring manager/organization regarding the work level for the position.

Salary ranges vary by location and work level.

This position is hiring for a variety of locations to include: Georgia, Hawaii, Maryland, and Texas.

Salary Range: $74,682 - $164,102 (Entry - Senior) All locations.

On-the job training, Internal NSA courses, and external training will be made available based on the need and experience of the selectee.

Work Schedule: Applicants should be aware that some of these jobs support 24/7 operations based on mission requirements and shift schedules may vary to include night shift.

Contact Us

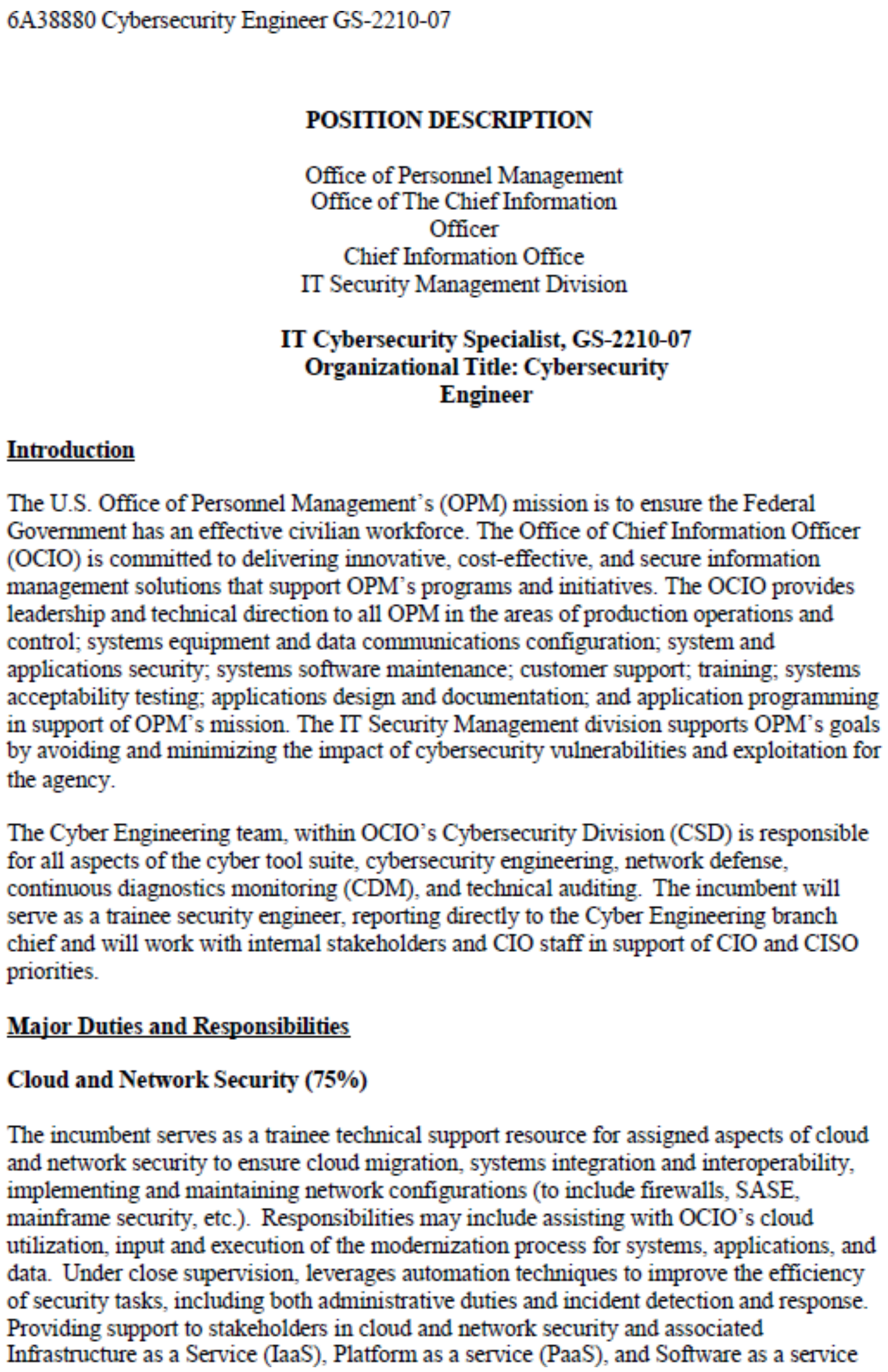
Phone: 1-844-424-4737
Email: IntelCareers@IntelligenceCareers.gov

Resources

Frequently Asked Questions
Freedom Of Information Act
Equal Employment Opportunity

Policy

Privacy Policy
Privacy Act Statement
Ethics
No Fear Act



6A38880 Cybersecurity Engineer GS-2210-07

POSITION DESCRIPTION

Office of Personnel Management
Office of The Chief Information
Officer
Chief Information Office
IT Security Management Division

IT Cybersecurity Specialist, GS-2210-07
**Organizational Title: Cybersecurity
Engineer**

Introduction

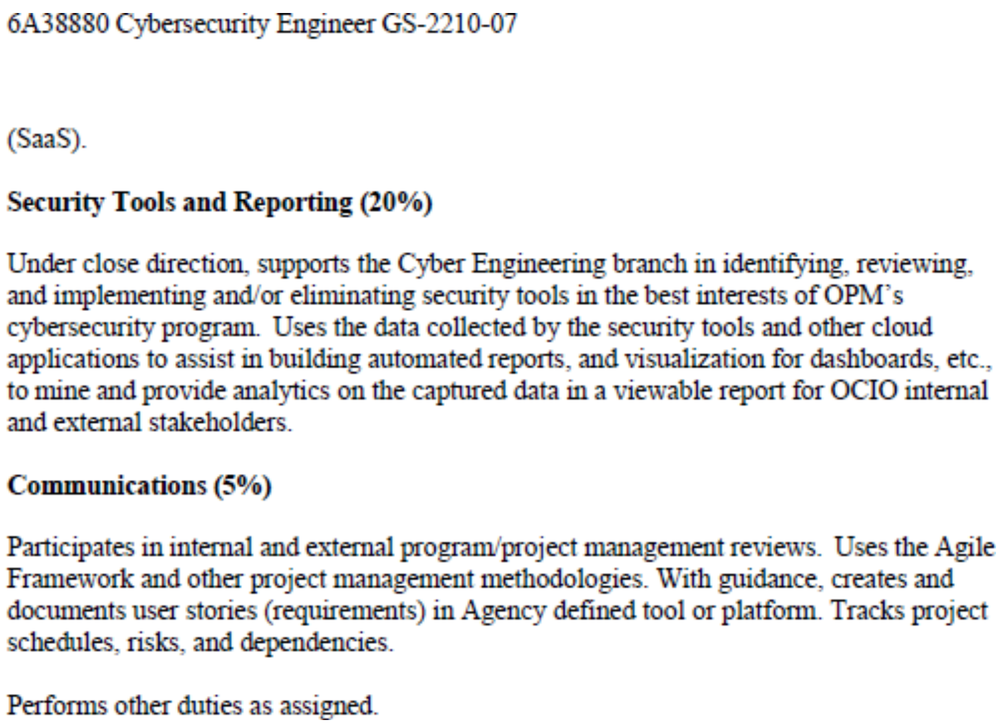
The U.S. Office of Personnel Management's (OPM) mission is to ensure the Federal Government has an effective civilian workforce. The Office of Chief Information Officer (OCIO) is committed to delivering innovative, cost-effective, and secure information management solutions that support OPM's programs and initiatives. The OCIO provides leadership and technical direction to all OPM in the areas of production operations and control; systems equipment and data communications configuration; system and applications security; systems software maintenance; customer support; training; systems acceptability testing; applications design and documentation; and application programming in support of OPM's mission. The IT Security Management division supports OPM's goals by avoiding and minimizing the impact of cybersecurity vulnerabilities and exploitation for the agency.

The Cyber Engineering team, within OCIO's Cybersecurity Division (CSD) is responsible for all aspects of the cyber tool suite, cybersecurity engineering, network defense, continuous diagnostics monitoring (CDM), and technical auditing. The incumbent will serve as a trainee security engineer, reporting directly to the Cyber Engineering branch chief and will work with internal stakeholders and CIO staff in support of CIO and CISO priorities.

Major Duties and Responsibilities

Cloud and Network Security (75%)

The incumbent serves as a trainee technical support resource for assigned aspects of cloud and network security to ensure cloud migration, systems integration and interoperability, implementing and maintaining network configurations (to include firewalls, SASE, mainframe security, etc.). Responsibilities may include assisting with OCIO's cloud utilization, input and execution of the modernization process for systems, applications, and data. Under close supervision, leverages automation techniques to improve the efficiency of security tasks, including both administrative duties and incident detection and response. Providing support to stakeholders in cloud and network security and associated Infrastructure as a Service (IaaS), Platform as a service (PaaS), and Software as a service



6A38880 Cybersecurity Engineer GS-2210-07

(SaaS).

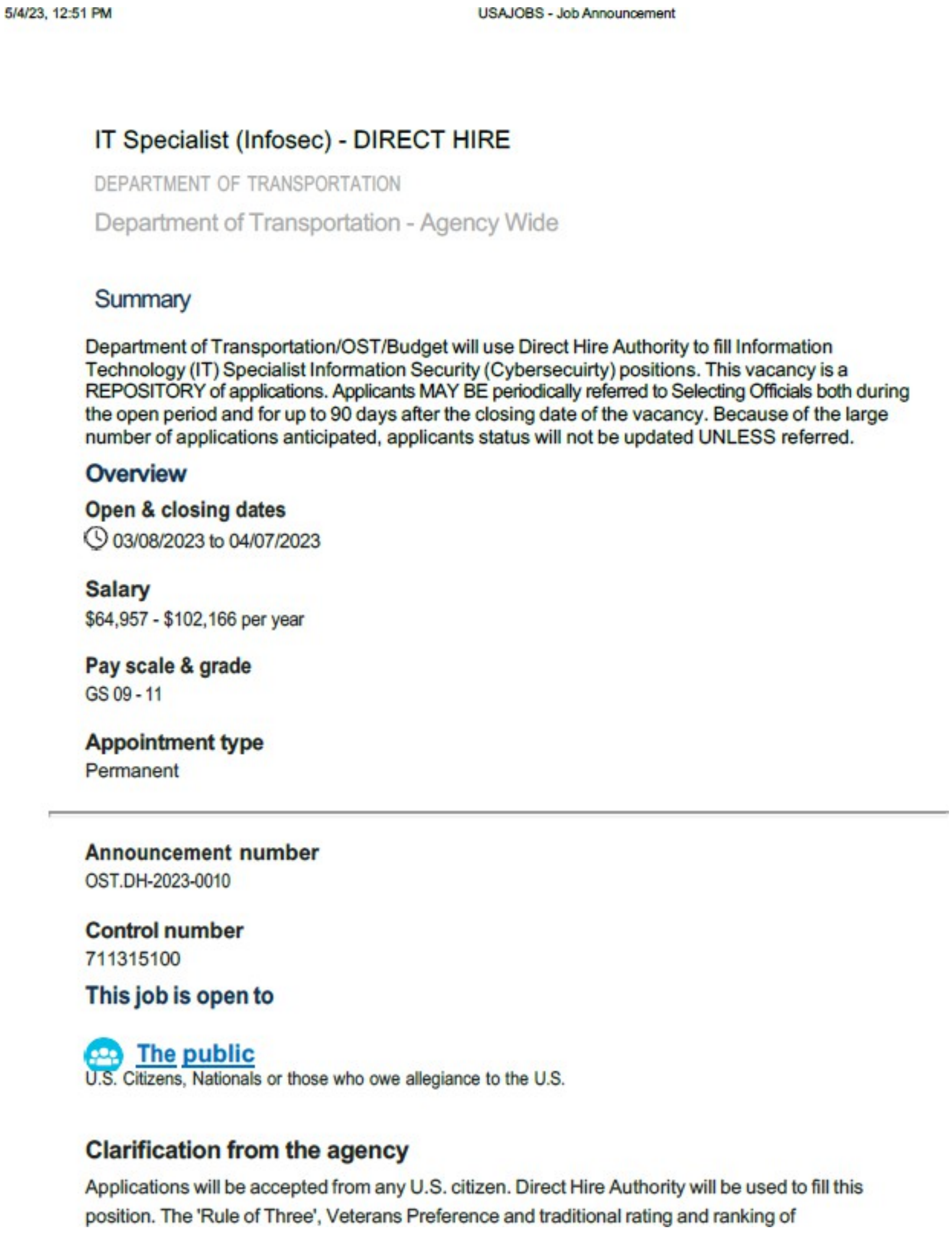
Security Tools and Reporting (20%)

Under close direction, supports the Cyber Engineering branch in identifying, reviewing, and implementing and/or eliminating security tools in the best interests of OPM's cybersecurity program. Uses the data collected by the security tools and other cloud applications to assist in building automated reports, and visualization for dashboards, etc., to mine and provide analytics on the captured data in a viewable report for OCIO internal and external stakeholders.

Communications (5%)

Participates in internal and external program/project management reviews. Uses the Agile Framework and other project management methodologies. With guidance, creates and documents user stories (requirements) in Agency defined tool or platform. Tracks project schedules, risks, and dependencies.

Performs other duties as assigned.



5/4/23, 12:51 PM USAJOBS - Job Announcement

IT Specialist (Infosec) - DIRECT HIRE

DEPARTMENT OF TRANSPORTATION

Department of Transportation - Agency Wide

Summary

Department of Transportation/OST/Budget will use Direct Hire Authority to fill Information Technology (IT) Specialist Information Security (Cybersecuirty) positions. This vacancy is a REPOSITORY of applications. Applicants MAY BE periodically referred to Selecting Officials both during the open period and for up to 90 days after the closing date of the vacancy. Because of the large number of applications anticipated, applicants status will not be updated UNLESS referred.

Overview

Open & closing dates

03/08/2023 to 04/07/2023

Salary

$64,957 - $102,166 per year

Pay scale & grade

GS 09 - 11

Appointment type

Permanent

Announcement number

OST.DH-2023-0010

Control number

711315100

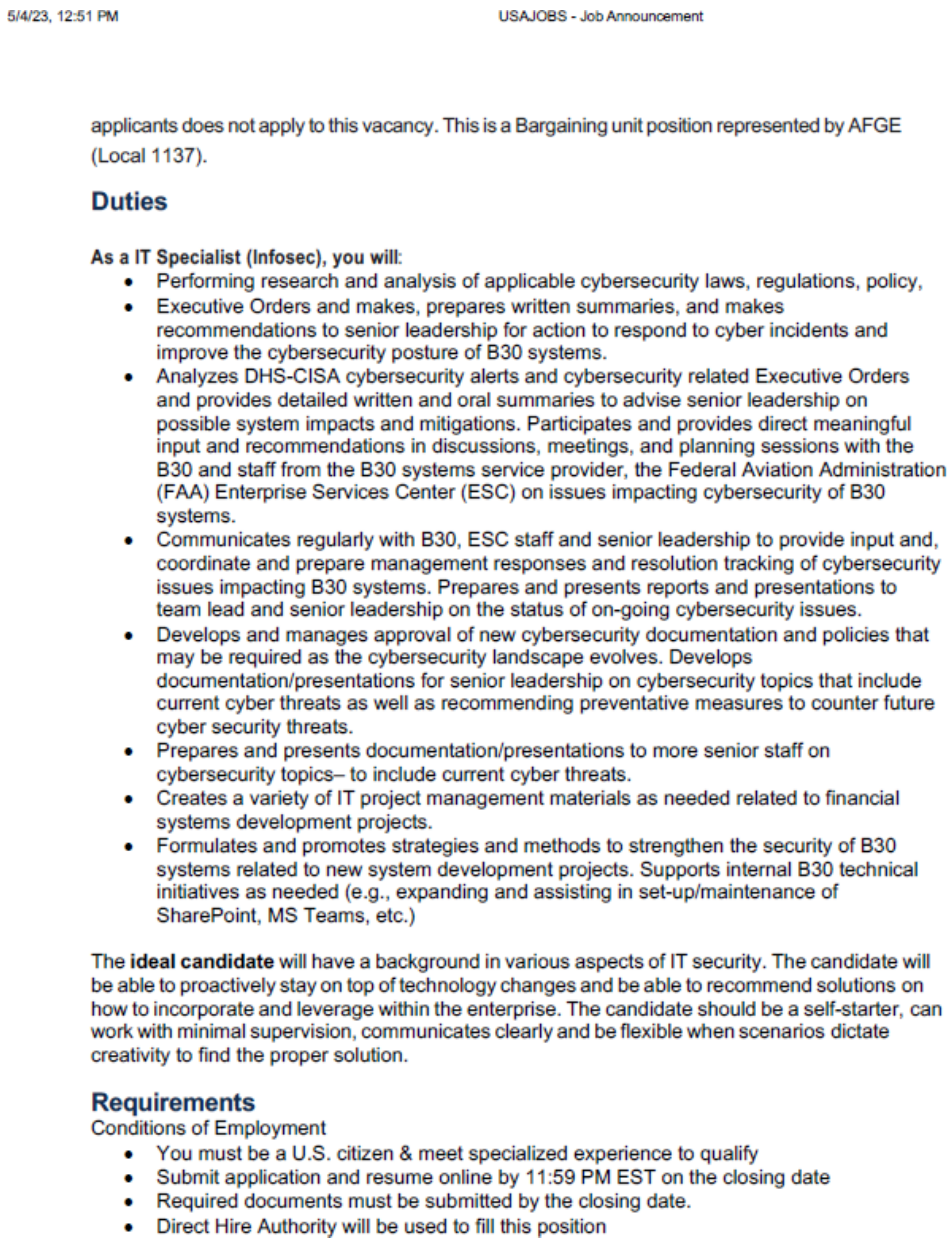
This job is open to

The public

U.S. Citizens, Nationals or those who owe allegiance to the U.S.

Clarification from the agency

Applications will be accepted from any U.S. citizen. Direct Hire Authority will be used to fill this position. The 'Rule of Three', Veterans Preference and traditional rating and ranking of



5/4/23, 12:51 PM USAJOBS - Job Announcement

applicants does not apply to this vacancy. This is a Bargaining unit position represented by AFGE (Local 1137).

Duties

As a IT Specialist (Infosec), you will:

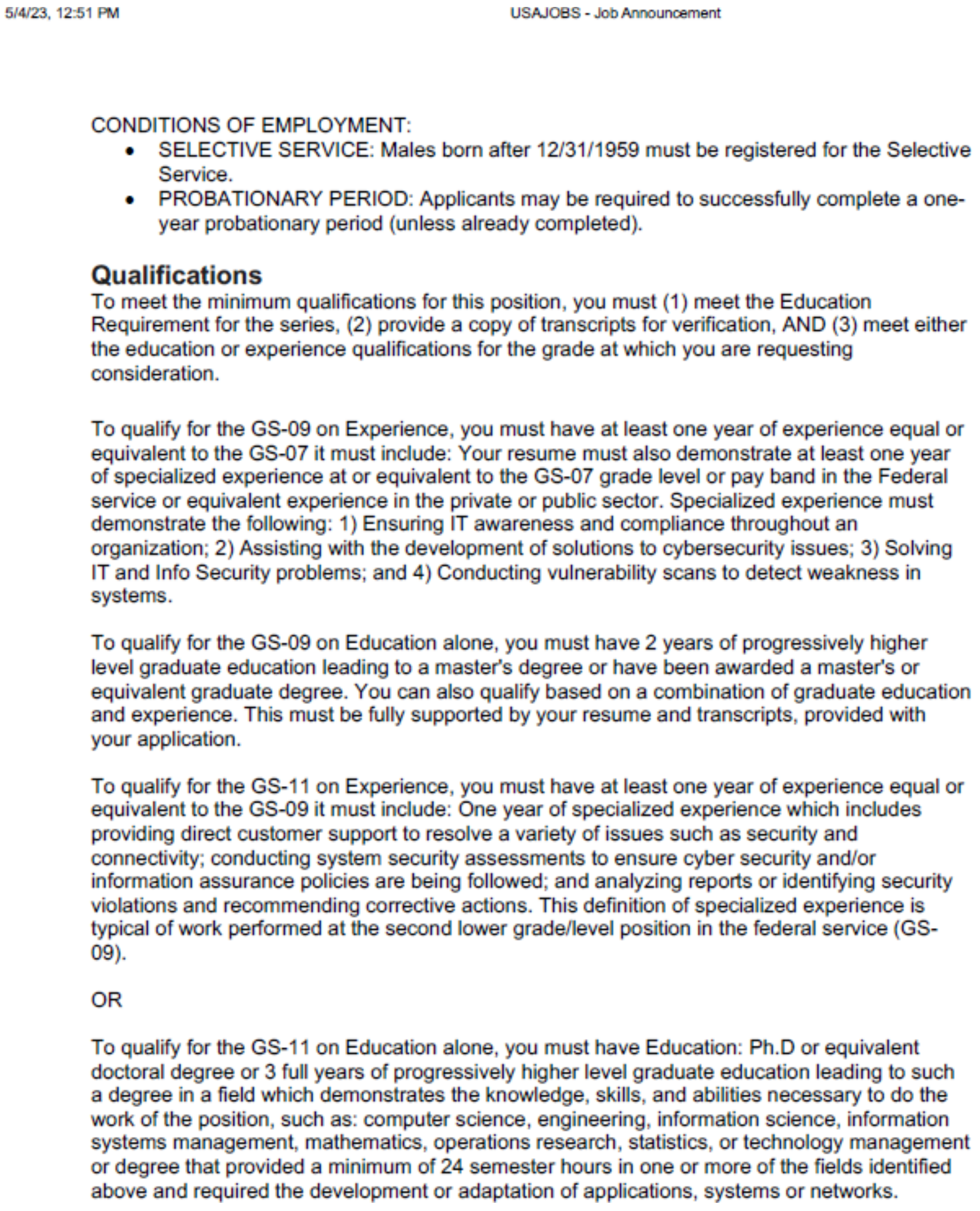
- Performing research and analysis of applicable cybersecurity laws, regulations, policy,
- Executive Orders and makes, prepares written summaries, and makes recommendations to senior leadership for action to respond to cyber incidents and improve the cybersecurity posture of B30 systems.
- Analyzes DHS-CISA cybersecurity alerts and cybersecurity related Executive Orders and provides detailed written and oral summaries to advise senior leadership on possible system impacts and mitigations. Participates and provides direct meaningful input and recommendations in discussions, meetings, and planning sessions with the B30 and staff from the B30 systems service provider, the Federal Aviation Administration (FAA) Enterprise Services Center (ESC) on issues impacting cybersecurity of B30 systems.
- Communicates regularly with B30, ESC staff and senior leadership to provide input and, coordinate and prepare management responses and resolution tracking of cybersecurity issues impacting B30 systems. Prepares and presents reports and presentations to team lead and senior leadership on the status of on-going cybersecurity issues.
- Develops and manages approval of new cybersecurity documentation and policies that may be required as the cybersecurity landscape evolves. Develops documentation/presentations for senior leadership on cybersecurity topics that include current cyber threats as well as recommending preventative measures to counter future cyber security threats.
- Prepares and presents documentation/presentations to more senior staff on cybersecurity topics– to include current cyber threats.
- Creates a variety of IT project management materials as needed related to financial systems development projects.
- Formulates and promotes strategies and methods to strengthen the security of B30 systems related to new system development projects. Supports internal B30 technical initiatives as needed (e.g., expanding and assisting in set-up/maintenance of SharePoint, MS Teams, etc.)

The **ideal candidate** will have a background in various aspects of IT security. The candidate will be able to proactively stay on top of technology changes and be able to recommend solutions on how to incorporate and leverage within the enterprise. The candidate should be a self-starter, can work with minimal supervision, communicates clearly and be flexible when scenarios dictate creativity to find the proper solution.

Requirements

Conditions of Employment

- You must be a U.S. citizen & meet specialized experience to qualify
- Submit application and resume online by 11:59 PM EST on the closing date
- Required documents must be submitted by the closing date.
- Direct Hire Authority will be used to fill this position



5/4/23, 12:51 PM USAJOBS - Job Announcement

CONDITIONS OF EMPLOYMENT:

- SELECTIVE SERVICE: Males born after 12/31/1959 must be registered for the Selective Service.
- PROBATIONARY PERIOD: Applicants may be required to successfully complete a one-year probationary period (unless already completed).

Qualifications

To meet the minimum qualifications for this position, you must (1) meet the Education Requirement for the series, (2) provide a copy of transcripts for verification, AND (3) meet either the education or experience qualifications for the grade at which you are requesting consideration.

To qualify for the GS-09 on Experience, you must have at least one year of experience equal or equivalent to the GS-07 it must include: Your resume must also demonstrate at least one year of specialized experience at or equivalent to the GS-07 grade level or pay band in the Federal service or equivalent experience in the private or public sector. Specialized experience must demonstrate the following: 1) Ensuring IT awareness and compliance throughout an organization; 2) Assisting with the development of solutions to cybersecurity issues; 3) Solving IT and Info Security problems; and 4) Conducting vulnerability scans to detect weakness in systems.

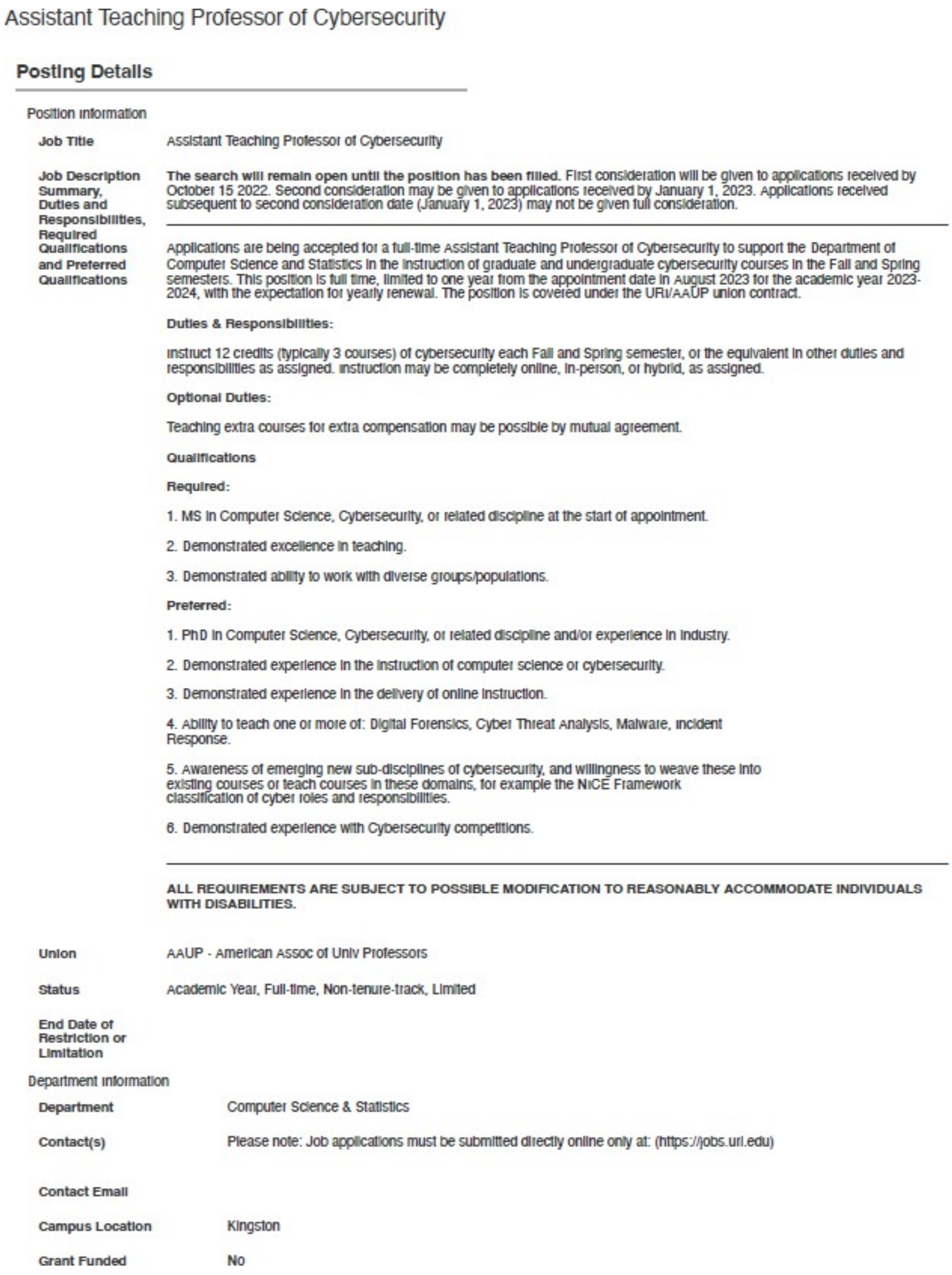
To qualify for the GS-09 on Education alone, you must have 2 years of progressively higher level graduate education leading to a master's degree or have been awarded a master's or equivalent graduate degree. You can also qualify based on a combination of graduate education and experience. This must be fully supported by your resume and transcripts, provided with your application.

To qualify for the GS-11 on Experience, you must have at least one year of experience equal or equivalent to the GS-09 it must include: One year of specialized experience which includes providing direct customer support to resolve a variety of issues such as security and connectivity; conducting system security assessments to ensure cyber security and/or information assurance policies are being followed; and analyzing reports or identifying security violations and recommending corrective actions. This definition of specialized experience is typical of work performed at the second lower grade/level position in the federal service (GS-09).

OR

To qualify for the GS-11 on Education alone, you must have Education: Ph.D or equivalent doctoral degree or 3 full years of progressively higher level graduate education leading to such a degree in a field which demonstrates the knowledge, skills, and abilities necessary to do the work of the position, such as: computer science, engineering, information science, information systems management, mathematics, operations research, statistics, or technology management or degree that provided a minimum of 24 semester hours in one or more of the fields identified above and required the development or adaptation of applications, systems or networks.

APPENDIX D: SAMPLE JOB DESCRIPTIONS



Assistant Teaching Professor of Cybersecurity

Posting Details

Position Information

Job Title Assistant Teaching Professor of Cybersecurity

Job Description Summary, Duties and Responsibilities, Required Qualifications and Preferred Qualifications

The search will remain open until the position has been filled. First consideration will be given to applications received by October 15 2022. Second consideration may be given to applications received by January 1, 2023. Applications received subsequent to second consideration date (January 1, 2023) may not be given full consideration.

Applications are being accepted for a full-time Assistant Teaching Professor of Cybersecurity to support the Department of Computer Science and Statistics in the instruction of graduate and undergraduate cybersecurity courses in the Fall and Spring semesters. This position is full time, limited to one year from the appointment date in August 2023 for the academic year 2023-2024, with the expectation for yearly renewal. The position is covered under the URI/AAUP union contract.

Duties & Responsibilities:

Instruct 12 credits (typically 3 courses) of cybersecurity each Fall and Spring semester, or the equivalent in other duties and responsibilities as assigned. Instruction may be completely online, in-person, or hybrid, as assigned.

Optional Duties:

Teaching extra courses for extra compensation may be possible by mutual agreement.

Qualifications

Required:

1. MS in Computer Science, Cybersecurity, or related discipline at the start of appointment.

2. Demonstrated excellence in teaching.

3. Demonstrated ability to work with diverse groups/populations.

Preferred:

1. PhD in Computer Science, Cybersecurity, or related discipline and/or experience in industry.

2. Demonstrated experience in the instruction of computer science or cybersecurity.

3. Demonstrated experience in the delivery of online instruction.

4. Ability to teach one or more of: Digital Forensics, Cyber Threat Analysis, Malware, Incident Response.

5. Awareness of emerging new sub-disciplines of cybersecurity, and willingness to weave these into existing courses or teach courses in these domains, for example the NICE Framework classification of cyber roles and responsibilities.

6. Demonstrated experience with Cybersecurity competitions.

ALL REQUIREMENTS ARE SUBJECT TO POSSIBLE MODIFICATION TO REASONABLY ACCOMMODATE INDIVIDUALS WITH DISABILITIES.

Union AAUP - American Assoc of Univ Professors

Status Academic Year, Full-time, Non-tenure-track, Limited

End Date of Restriction or Limitation

Department Information

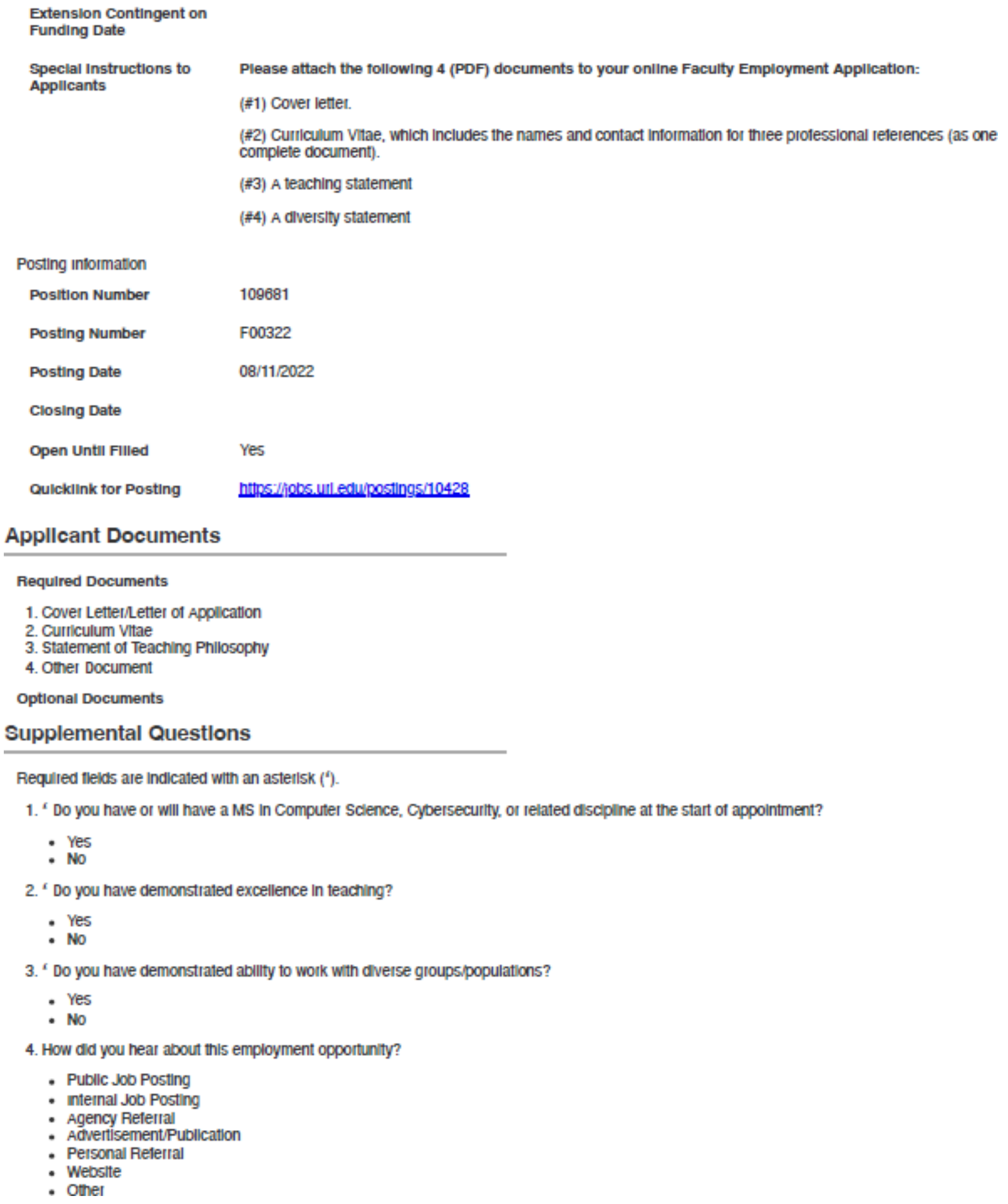
Department Computer Science & Statistics

Contact(s) Please note: Job applications must be submitted directly online only at: (https://jobs.uri.edu)

Contact Email

Campus Location Kingston

Grant Funded No



Extension Contingent on Funding Date	
Special Instructions to Applicants	**Please attach the following 4 (PDF) documents to your online Faculty Employment Application:** (#1) Cover letter. (#2) Curriculum Vitae, which includes the names and contact information for three professional references (as one complete document). (#3) A teaching statement (#4) A diversity statement

Posting Information

Position Number	109681
Posting Number	F00322
Posting Date	08/11/2022
Closing Date	
Open Until Filled	Yes
Quicklink for Posting	https://jobs.uri.edu/postings/10428

Applicant Documents

Required Documents

1. Cover Letter/Letter of Application
2. Curriculum Vitae
3. Statement of Teaching Philosophy
4. Other Document

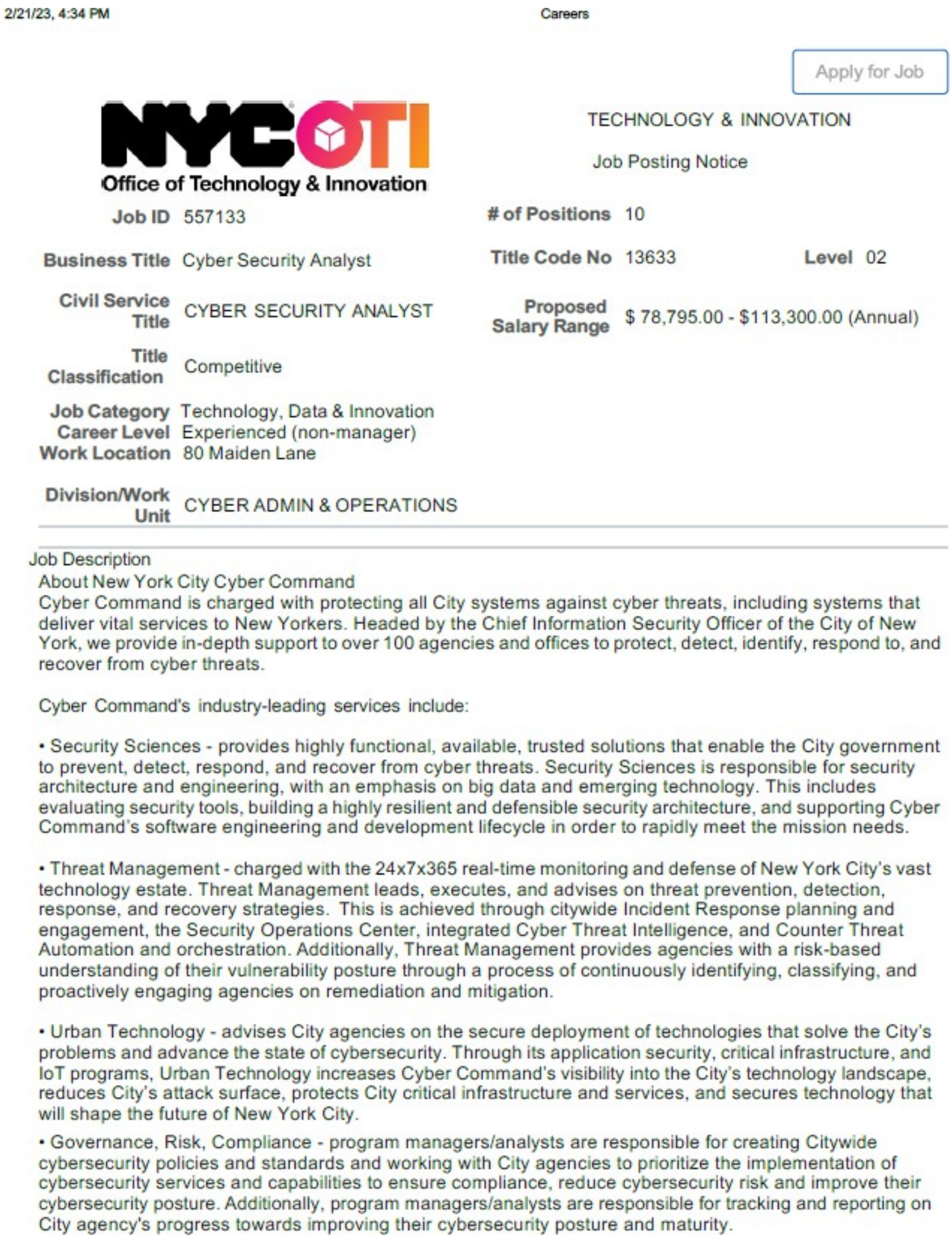
Optional Documents

Supplemental Questions

Required fields are indicated with an asterisk (*).

1. * Do you have or will have a MS in Computer Science, Cybersecurity, or related discipline at the start of appointment?
   - Yes
   - No
2. * Do you have demonstrated excellence in teaching?
   - Yes
   - No
3. * Do you have demonstrated ability to work with diverse groups/populations?
   - Yes
   - No
4. How did you hear about this employment opportunity?
   - Public Job Posting
   - Internal Job Posting
   - Agency Referral
   - Advertisement/Publication
   - Personal Referral
   - Website
   - Other

APPENDIX D: SAMPLE JOB DESCRIPTIONS



2/21/23, 4:34 PM Careers

Apply for Job

NYC OTI Office of Technology & Innovation

TECHNOLOGY & INNOVATION

Job Posting Notice

Job ID	557133	**# of Positions**	10
Business Title	Cyber Security Analyst	**Title Code No**	13633 **Level** 02
Civil Service Title	CYBER SECURITY ANALYST	**Proposed Salary Range**	$ 78,795.00 - $113,300.00 (Annual)
Title Classification	Competitive		
Job Category	Technology, Data & Innovation		
Career Level	Experienced (non-manager)		
Work Location	80 Maiden Lane		
Division/Work Unit	CYBER ADMIN & OPERATIONS		

Job Description

About New York City Cyber Command

Cyber Command is charged with protecting all City systems against cyber threats, including systems that deliver vital services to New Yorkers. Headed by the Chief Information Security Officer of the City of New York, we provide in-depth support to over 100 agencies and offices to protect, detect, identify, respond to, and recover from cyber threats.

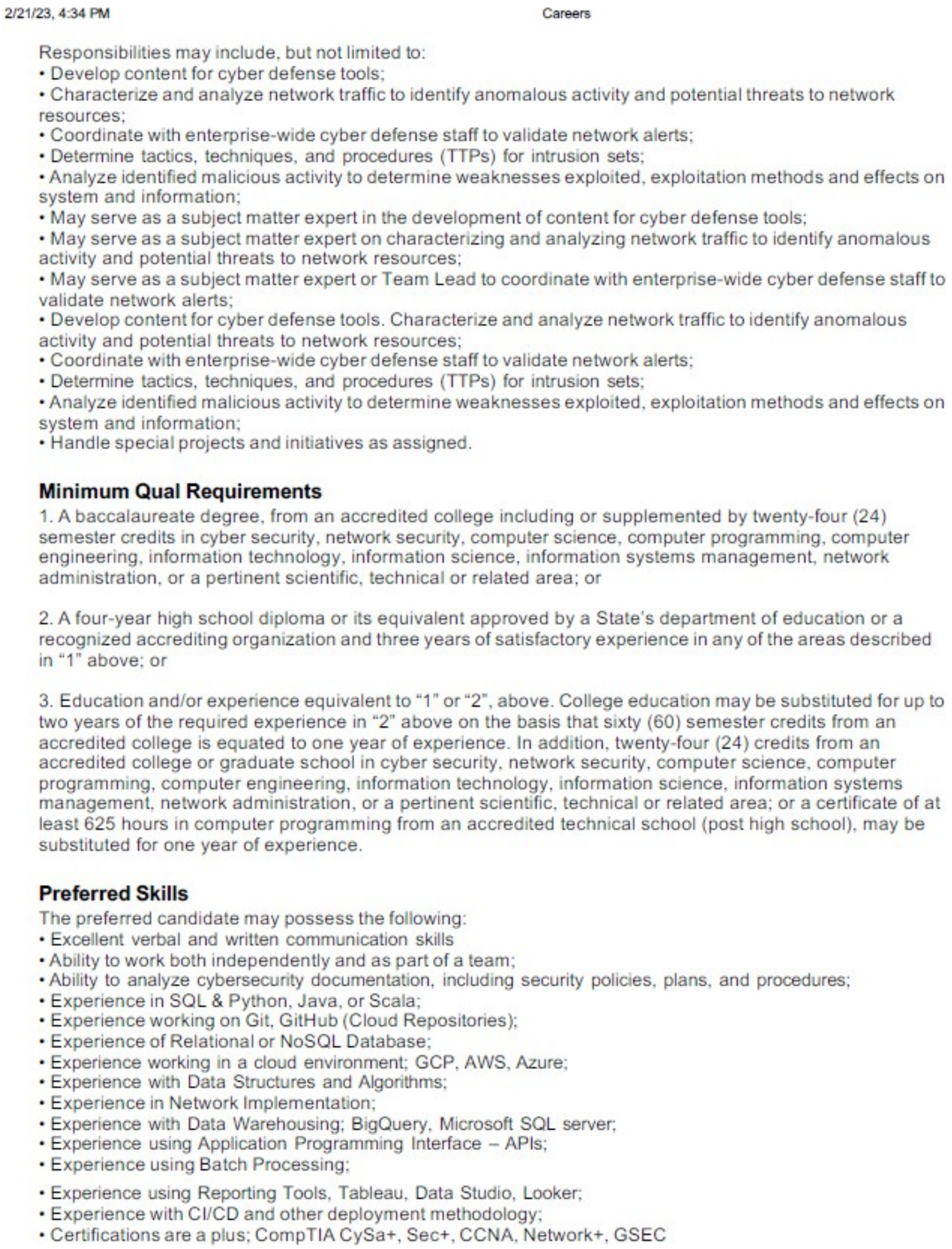
Cyber Command's industry-leading services include:

- Security Sciences - provides highly functional, available, trusted solutions that enable the City government to prevent, detect, respond, and recover from cyber threats. Security Sciences is responsible for security architecture and engineering, with an emphasis on big data and emerging technology. This includes evaluating security tools, building a highly resilient and defensible security architecture, and supporting Cyber Command's software engineering and development lifecycle in order to rapidly meet the mission needs.

- Threat Management - charged with the 24x7x365 real-time monitoring and defense of New York City's vast technology estate. Threat Management leads, executes, and advises on threat prevention, detection, response, and recovery strategies. This is achieved through citywide Incident Response planning and engagement, the Security Operations Center, integrated Cyber Threat Intelligence, and Counter Threat Automation and orchestration. Additionally, Threat Management provides agencies with a risk-based understanding of their vulnerability posture through a process of continuously identifying, classifying, and proactively engaging agencies on remediation and mitigation.

- Urban Technology - advises City agencies on the secure deployment of technologies that solve the City's problems and advance the state of cybersecurity. Through its application security, critical infrastructure, and IoT programs, Urban Technology increases Cyber Command's visibility into the City's technology landscape, reduces City's attack surface, protects City critical infrastructure and services, and secures technology that will shape the future of New York City.

- Governance, Risk, Compliance - program managers/analysts are responsible for creating Citywide cybersecurity policies and standards and working with City agencies to prioritize the implementation of cybersecurity services and capabilities to ensure compliance, reduce cybersecurity risk and improve their cybersecurity posture. Additionally, program managers/analysts are responsible for tracking and reporting on City agency's progress towards improving their cybersecurity posture and maturity.



2/21/23, 4:34 PM Careers

Responsibilities may include, but not limited to:
- Develop content for cyber defense tools;
- Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources;
- Coordinate with enterprise-wide cyber defense staff to validate network alerts;
- Determine tactics, techniques, and procedures (TTPs) for intrusion sets;
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods and effects on system and information;
- May serve as a subject matter expert in the development of content for cyber defense tools;
- May serve as a subject matter expert on characterizing and analyzing network traffic to identify anomalous activity and potential threats to network resources;
- May serve as a subject matter expert or Team Lead to coordinate with enterprise-wide cyber defense staff to validate network alerts;
- Develop content for cyber defense tools. Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources;
- Coordinate with enterprise-wide cyber defense staff to validate network alerts;
- Determine tactics, techniques, and procedures (TTPs) for intrusion sets;
- Analyze identified malicious activity to determine weaknesses exploited, exploitation methods and effects on system and information;
- Handle special projects and initiatives as assigned.

Minimum Qual Requirements

1. A baccalaureate degree, from an accredited college including or supplemented by twenty-four (24) semester credits in cyber security, network security, computer science, computer programming, computer engineering, information technology, information science, information systems management, network administration, or a pertinent scientific, technical or related area; or

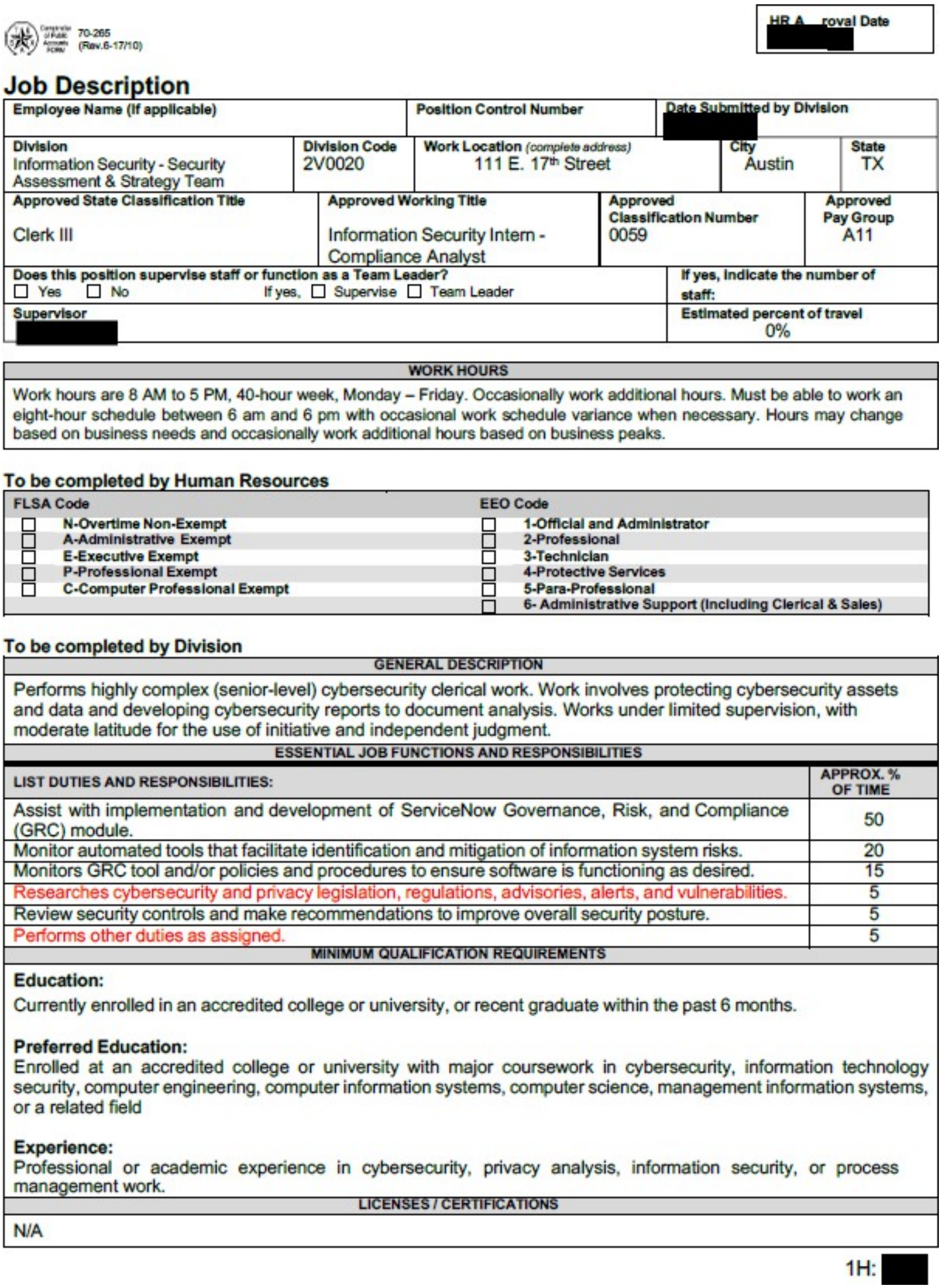
2. A four-year high school diploma or its equivalent approved by a State's department of education or a recognized accrediting organization and three years of satisfactory experience in any of the areas described in "1" above; or

3. Education and/or experience equivalent to "1" or "2", above. College education may be substituted for up to two years of the required experience in "2" above on the basis that sixty (60) semester credits from an accredited college is equated to one year of experience. In addition, twenty-four (24) credits from an accredited college or graduate school in cyber security, network security, computer science, computer programming, computer engineering, information technology, information science, information systems management, network administration, or a pertinent scientific, technical or related area; or a certificate of at least 625 hours in computer programming from an accredited technical school (post high school), may be substituted for one year of experience.

Preferred Skills

The preferred candidate may possess the following:
- Excellent verbal and written communication skills
- Ability to work both independently and as part of a team;
- Ability to analyze cybersecurity documentation, including security policies, plans, and procedures;
- Experience in SQL & Python, Java, or Scala;
- Experience working on Git, GitHub (Cloud Repositories);
- Experience of Relational or NoSQL Database;
- Experience working in a cloud environment; GCP, AWS, Azure;
- Experience with Data Structures and Algorithms;
- Experience in Network Implementation;
- Experience with Data Warehousing; BigQuery, Microsoft SQL server;
- Experience using Application Programming Interface – APIs;
- Experience using Batch Processing;
- Experience using Reporting Tools, Tableau, Data Studio, Looker;
- Experience with CI/CD and other deployment methodology;
- Certifications are a plus; CompTIA CySa+, Sec+, CCNA, Network+, GSEC

APPENDIX D: SAMPLE JOB DESCRIPTIONS



Comptroller of Public Accounts FORM 70-265 (Rev.6-17/10)

HR A roval Date
[redacted]

Job Description

Employee Name (If applicable)	**Position Control Number**	**Date Submitted by Division** [redacted]		
Division Information Security - Security Assessment & Strategy Team	**Division Code** 2V0020	**Work Location** *(complete address)* 111 E. 17th Street	**City** Austin	**State** TX
Approved State Classification Title Clerk III	**Approved Working Title** Information Security Intern - Compliance Analyst	**Approved Classification Number** 0059	**Approved Pay Group** A11	

Does this position supervise staff or function as a Team Leader?
□ Yes □ No   If yes, □ Supervise □ Team Leader

If yes, indicate the number of staff:

Supervisor
[redacted]

Estimated percent of travel
0%

WORK HOURS
Work hours are 8 AM to 5 PM, 40-hour week, Monday – Friday. Occasionally work additional hours. Must be able to work an eight-hour schedule between 6 am and 6 pm with occasional work schedule variance when necessary. Hours may change based on business needs and occasionally work additional hours based on business peaks.

To be completed by Human Resources

FLSA Code		EEO Code	
□	N-Overtime Non-Exempt	□	1-Official and Administrator
□	A-Administrative Exempt	□	2-Professional
□	E-Executive Exempt	□	3-Technician
□	P-Professional Exempt	□	4-Protective Services
□	C-Computer Professional Exempt	□	5-Para-Professional
		□	6- Administrative Support (Including Clerical & Sales)

To be completed by Division

GENERAL DESCRIPTION

Performs highly complex (senior-level) cybersecurity clerical work. Work involves protecting cybersecurity assets and data and developing cybersecurity reports to document analysis. Works under limited supervision, with moderate latitude for the use of initiative and independent judgment.

ESSENTIAL JOB FUNCTIONS AND RESPONSIBILITIES

LIST DUTIES AND RESPONSIBILITIES:	APPROX. % OF TIME
Assist with implementation and development of ServiceNow Governance, Risk, and Compliance (GRC) module.	50
Monitor automated tools that facilitate identification and mitigation of information system risks.	20
Monitors GRC tool and/or policies and procedures to ensure software is functioning as desired.	15
Researches cybersecurity and privacy legislation, regulations, advisories, alerts, and vulnerabilities.	5
Review security controls and make recommendations to improve overall security posture.	5
Performs other duties as assigned.	5

MINIMUM QUALIFICATION REQUIREMENTS

Education:
Currently enrolled in an accredited college or university, or recent graduate within the past 6 months.

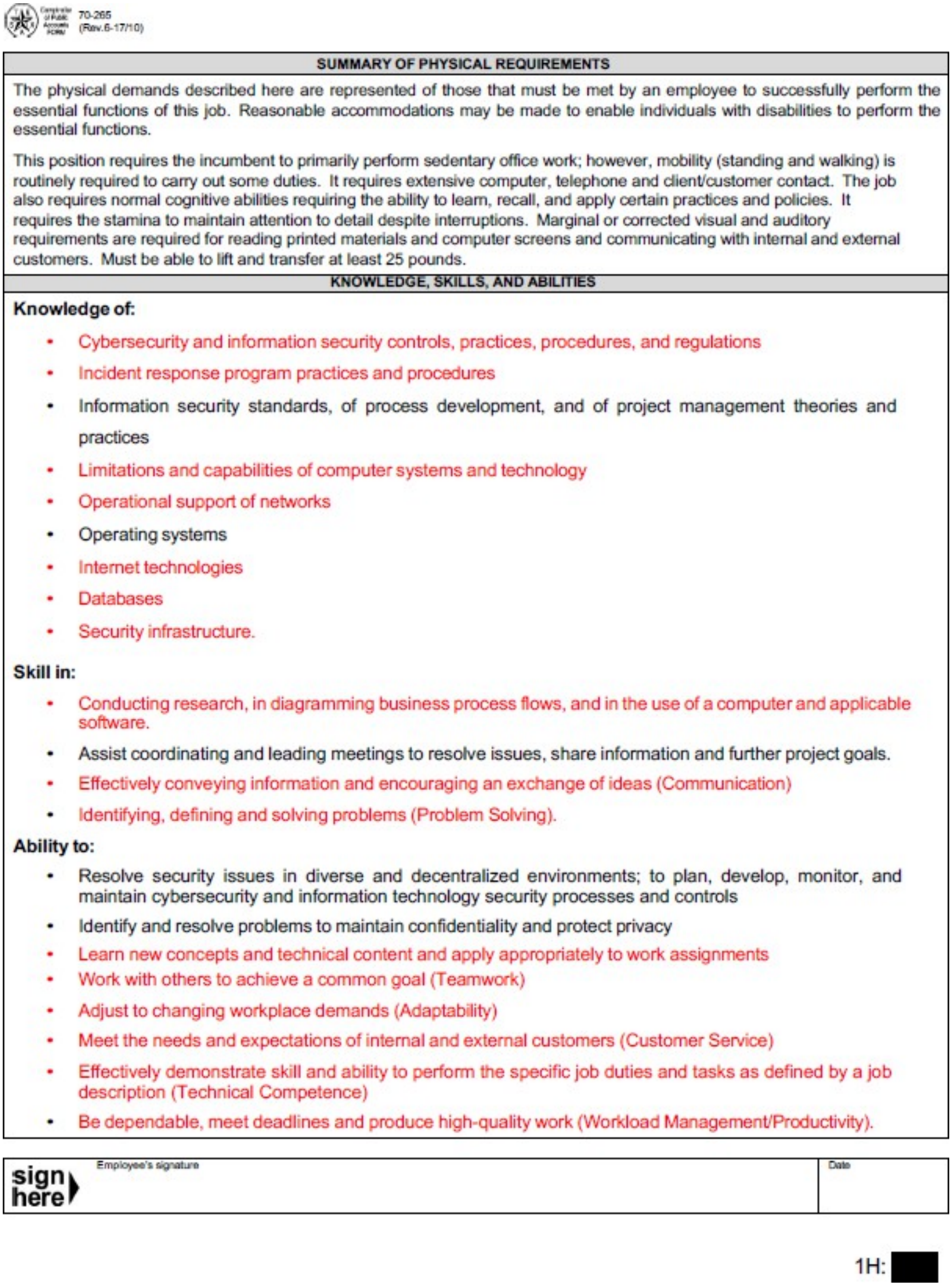
Preferred Education:
Enrolled at an accredited college or university with major coursework in cybersecurity, information technology security, computer engineering, computer information systems, computer science, management information systems, or a related field

Experience:
Professional or academic experience in cybersecurity, privacy analysis, information security, or process management work.

LICENSES / CERTIFICATIONS

N/A

1H: [redacted]



70-265
(Rev.6-17/10)

SUMMARY OF PHYSICAL REQUIREMENTS

The physical demands described here are represented of those that must be met by an employee to successfully perform the essential functions of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

This position requires the incumbent to primarily perform sedentary office work; however, mobility (standing and walking) is routinely required to carry out some duties. It requires extensive computer, telephone and client/customer contact. The job also requires normal cognitive abilities requiring the ability to learn, recall, and apply certain practices and policies. It requires the stamina to maintain attention to detail despite interruptions. Marginal or corrected visual and auditory requirements are required for reading printed materials and computer screens and communicating with internal and external customers. Must be able to lift and transfer at least 25 pounds.

KNOWLEDGE, SKILLS, AND ABILITIES

Knowledge of:

- Cybersecurity and information security controls, practices, procedures, and regulations
- Incident response program practices and procedures
- Information security standards, of process development, and of project management theories and practices
- Limitations and capabilities of computer systems and technology
- Operational support of networks
- Operating systems
- Internet technologies
- Databases
- Security infrastructure.

Skill in:

- Conducting research, in diagramming business process flows, and in the use of a computer and applicable software.
- Assist coordinating and leading meetings to resolve issues, share information and further project goals.
- Effectively conveying information and encouraging an exchange of ideas (Communication)
- Identifying, defining and solving problems (Problem Solving).

Ability to:

- Resolve security issues in diverse and decentralized environments; to plan, develop, monitor, and maintain cybersecurity and information technology security processes and controls
- Identify and resolve problems to maintain confidentiality and protect privacy
- Learn new concepts and technical content and apply appropriately to work assignments
- Work with others to achieve a common goal (Teamwork)
- Adjust to changing workplace demands (Adaptability)
- Meet the needs and expectations of internal and external customers (Customer Service)
- Effectively demonstrate skill and ability to perform the specific job duties and tasks as defined by a job description (Technical Competence)
- Be dependable, meet deadlines and produce high-quality work (Workload Management/Productivity).

sign here ▶ Employee's signature	Date

1H: [redacted]

APPENDIX E: STUDENTS RELEASED FROM OBLIGATIONS

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

Source: SFS Master Roster and Placement Log as of October 1, 2023.

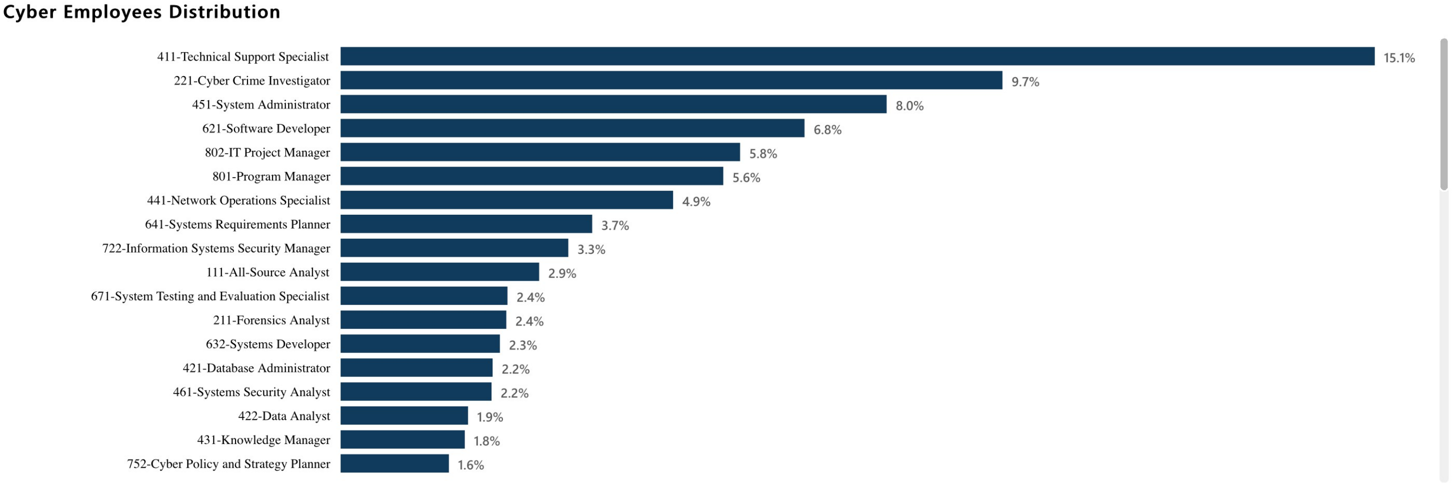
Year	Scholarships Awarded	Full Waiver: Academic Phase	Partial Waiver: Academic Phase	Full Waiver: Employment Phase	Partial Waiver: Employment Phase	Waiver Request Pending Decision	Total Waivers
2001	31	0	0	6	0	0	6
2002	115	2	0	16	0	0	18
2003	219	1	0	16	0	0	17
2004	185	0	0	3	0	0	3
2005	182	4	0	2	0	0	6
2006	133	1	0	0	0	0	1
2007	111	1	0	0	0	0	1
2008	94	0	0	0	0	0	0
2009	133	4	0	1	0	0	5
2010	181	2	0	1	0	0	3
2011	195	3	0	1	1	0	5
2012	186	2	0	0	0	0	2
2013	268	1	0	1	0	0	2
2014	277	0	0	3	0	0	3
2015	277	0	0	1	0	1	2
2016	313	0	0	0	0	0	0
2017	357	2	0	0	0	1	3
2018	339	1	0	1	0	0	2
2019	384	2	0	0	1	1	4
2020	375	1	0	0	0	1	2
2021	364	0	0	0	0	0	0
2022	391	0	0	0	0	0	0
2023	463	0	0	0	0	0	0
Total	**5,573**	**27**	**0**	**52**	**2**	**4**	**85**

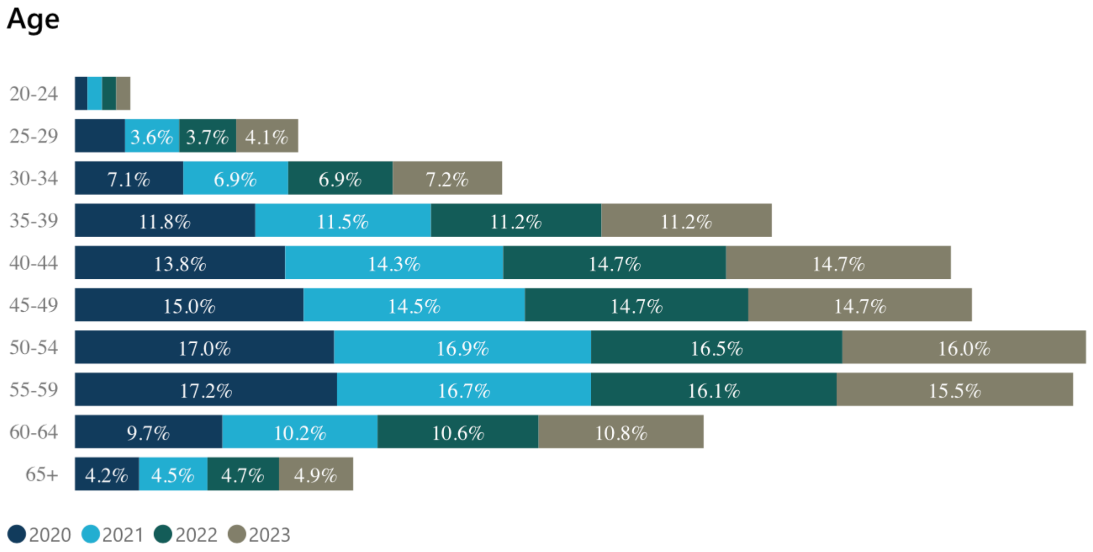
APPENDIX F: FEDERAL CYBERSECURITY WORKFORCE STATISTICS

OPM's Cyber Workforce Dashboard, https://www.opm.gov/data/data-products/cyber-workforce-dashboard/, is the source of the following data, as of December 2023.

FEDERAL CYBER WORKFORCE SUMMARY

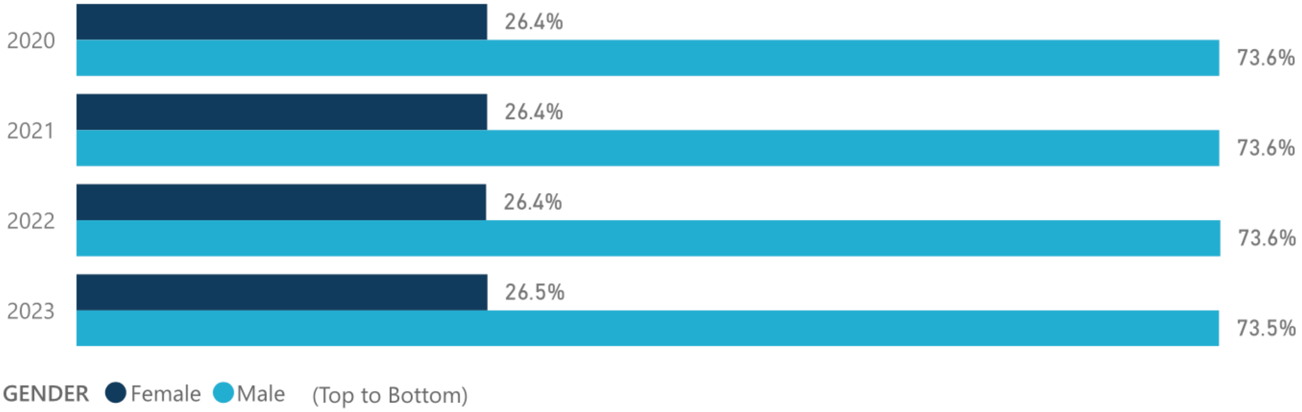
Average Age (Yr)	Average Adjusted Base Pay ($)	Average Length of Service (Yr)	Telework Eligible	Cyber 2-Yr. Retention Rate No Data will show for FY23 until full FY23 hire & separation data is available in EHRI-SDM	Government-wide 2-Yr. Retention Rate
48.0	$122.8K	14.0	67.1%	80.9%	72.9%



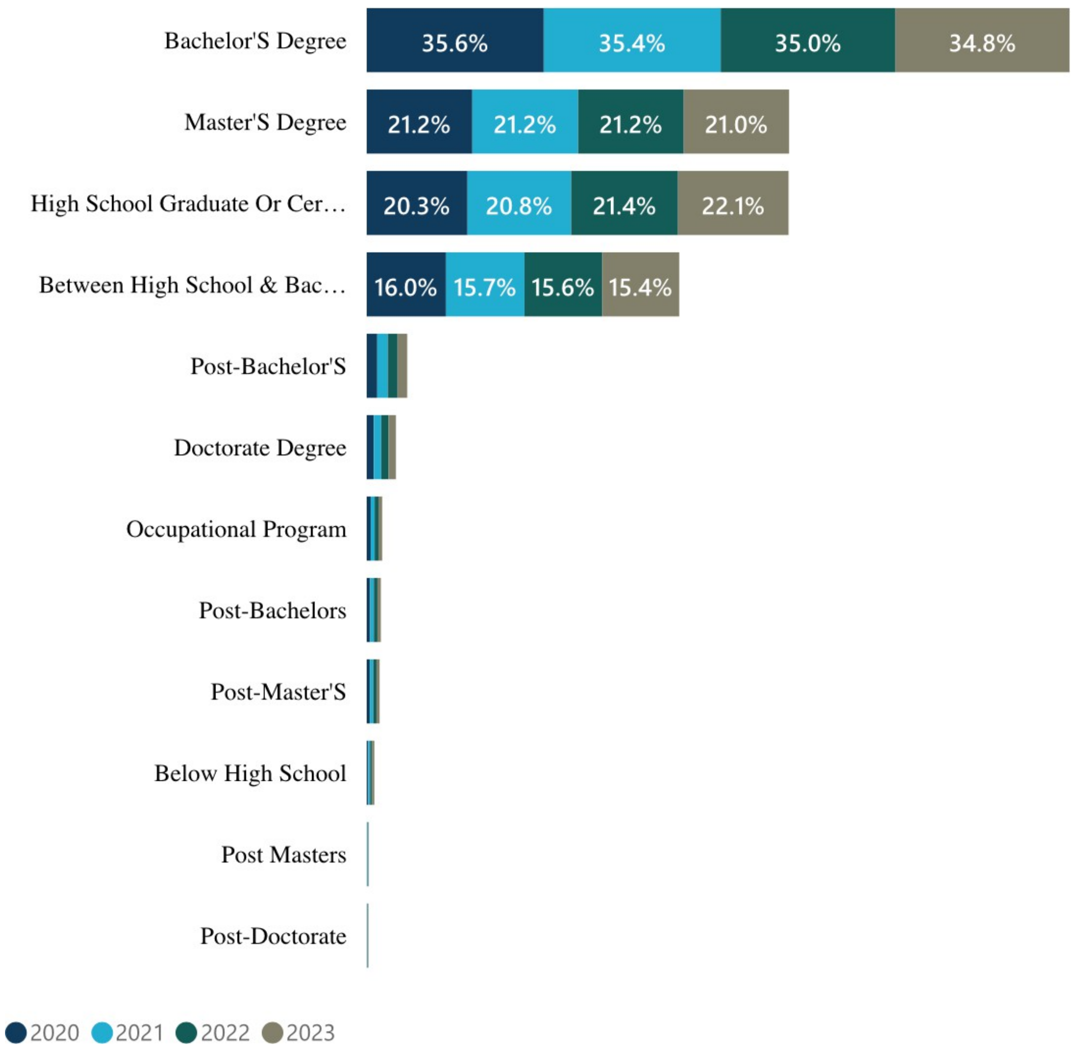


APPENDIX F: FEDERAL CYBERSECURITY WORKFORCE STATISTICS

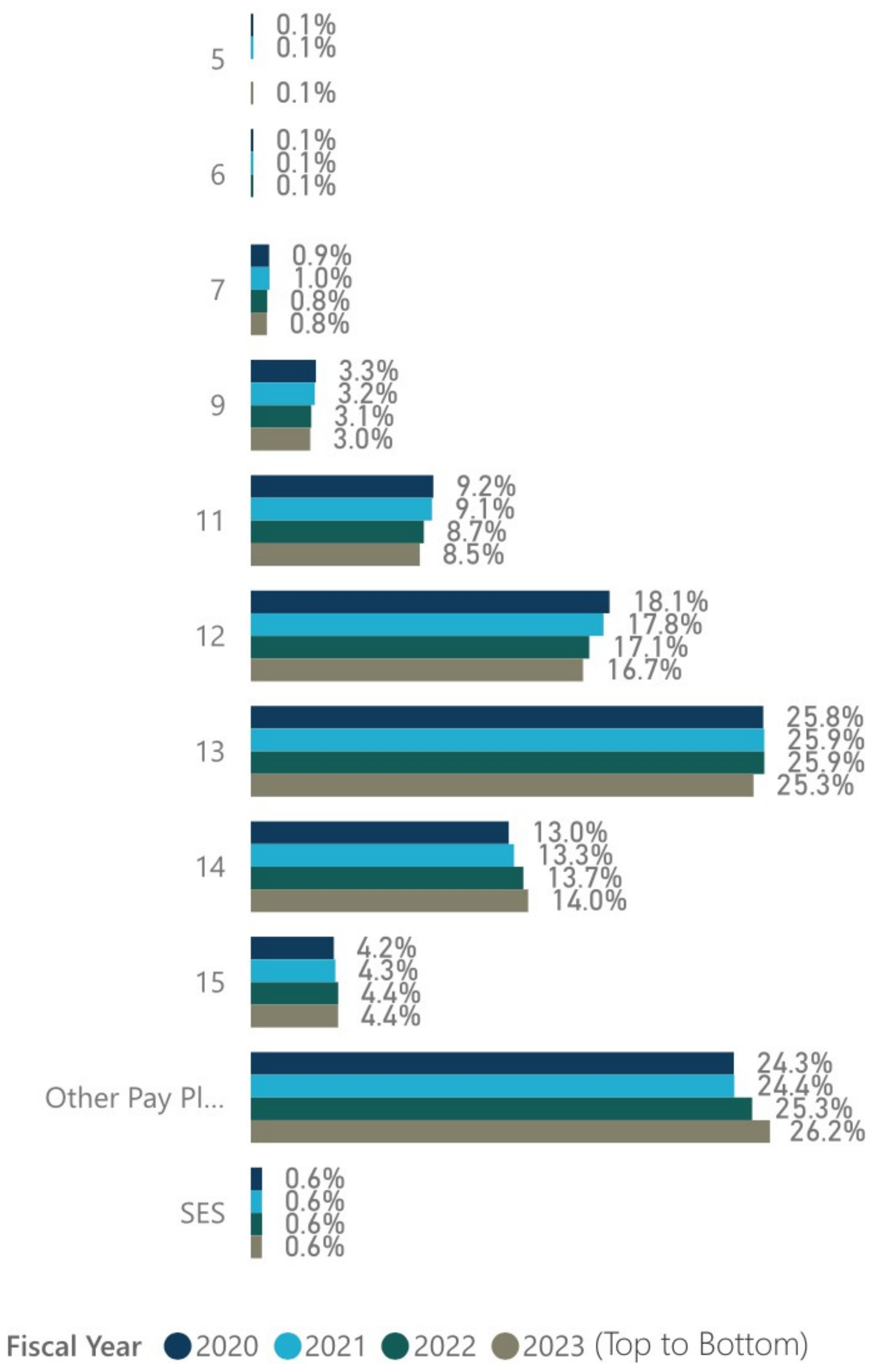
Gender



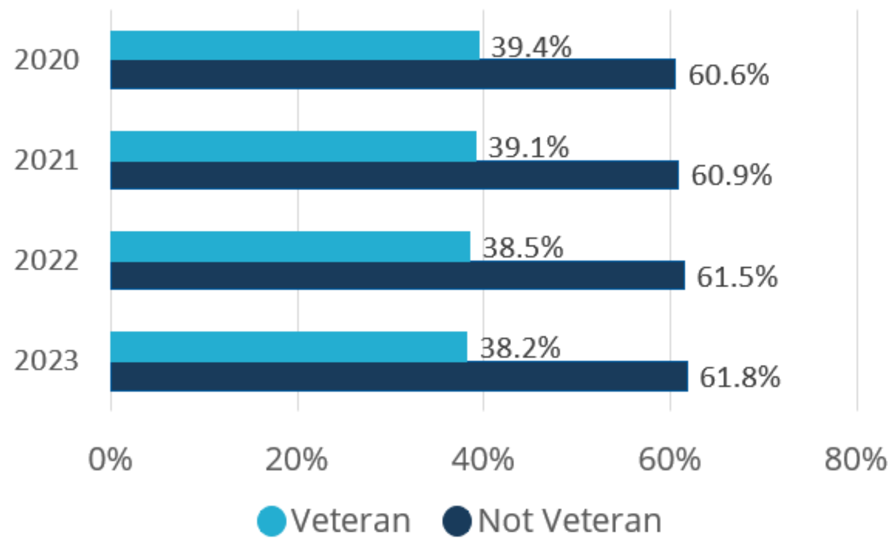
Cyber Employee Education Distribution



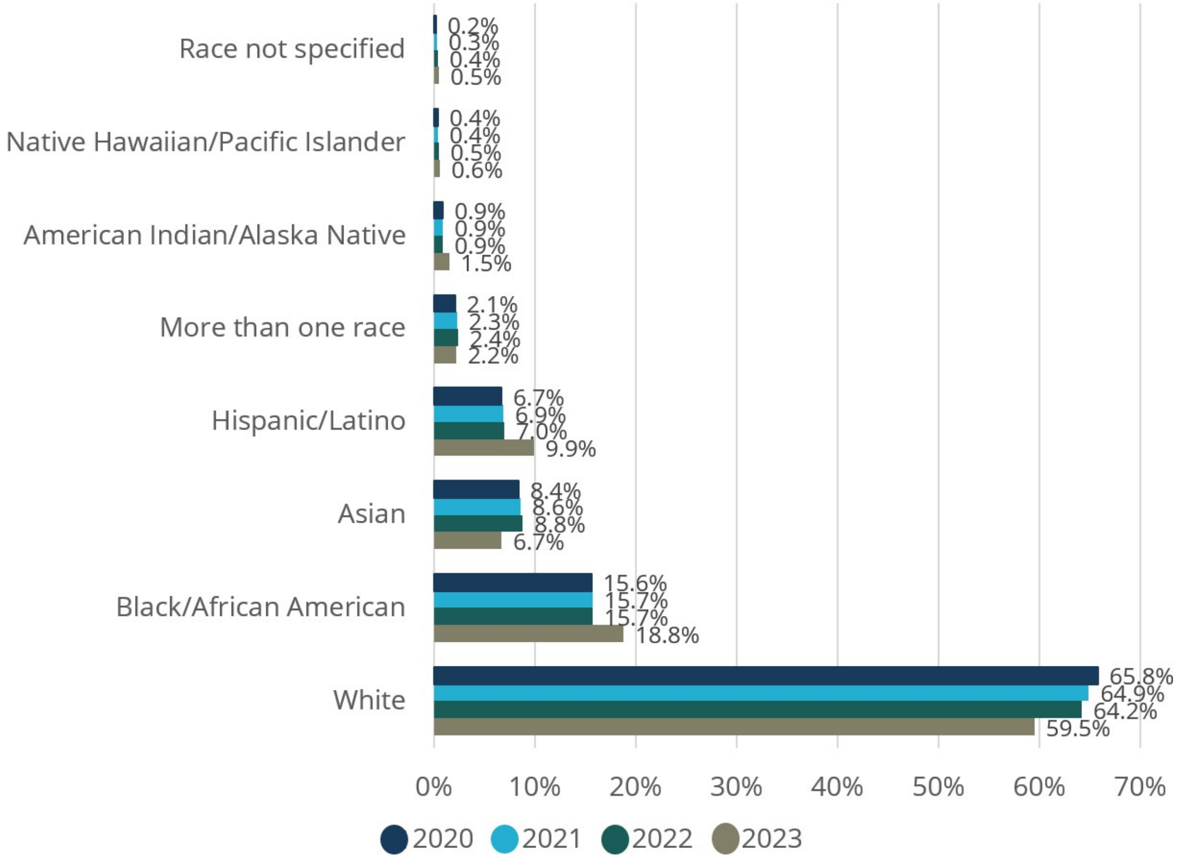
Cyber GS Grades and Executive Pay Plans



Veteran



Race/Ethnicity



APPENDIX G: LIST OF SFS SCHOOLS (ACTIVE AS OF 2023)

Alabama	Auburn University
	Tuskegee University
	University of Alabama at Birmingham
	University of Alabama in Huntsville
	University of Alabama Tuscaloosa
	University of South Alabama
Arkansas	University of Arkansas
Arizona	Arizona State University
	University of Arizona
California	Cal Poly Pomona
	California State University - Sacramento
	California State University - San Bernardino
	Naval Postgraduate School
Colorado	University of Colorado at Colorado Springs
Connecticut	University of New Haven
Delaware	University of Delaware
DC	George Washington University
	Georgetown University
Florida	Embry-Riddle Aeronautical University
	Florida Atlantic University
	Florida International University
	Florida State University
	University of Central Florida
	University of Florida
	University of South Florida
	University of West Florida
Georgia	Augusta University
	Georgia Institute of Technology
	Georgia State University
Hawaii	University of Hawaii
Idaho	Boise State University
	Idaho State University
	University of Idaho
Illinois	Loyola University Chicago
	University of Illinois at Urbana-Champaign
Indiana	Indiana University
	Indiana University Purdue University Indianapolis
	Purdue University Northwest
Kansas	Kansas State University
	University of Kansas
	Wichita State University
Kentucky	University of Louisville
Louisiana	Louisiana State University
	Louisiana Tech University
Massachusetts	Northeastern University
	University of Massachusetts Amherst
	University of Massachusetts, Dartmouth
	Worcester Polytechnic Institute
Maryland	Bowie State University
	Johns Hopkins University
	Morgan State University
	Towson University
	University of Maryland Baltimore County
	University of Maryland, College Park
Michigan	Davenport University
	Michigan Technological University
	Oakland University
Missouri	University of Missouri-Columbia
Mississippi	Mississippi State University
North Carolina	North Carolina Agricultural & Technical State University
	North Carolina State University
	University of North Carolina at Charlotte
Nebraska	University of Nebraska at Omaha
New Jersey	New Jersey Institute of Technology
	Stevens Institute of Technology
New Mexico	New Mexico Institute of Mining and Technology
	University of New Mexico
Nevada	University of Nevada, Las Vegas
	University of Nevada, Reno
New York	Binghamton University, SUNY
	Fordham University
	New York University
	Pace University
	Rochester Institute of Tech
	University at Buffalo, SUNY
Ohio	University of Cincinnati
Oklahoma	University of Tulsa
Pennsylvania	Carnegie-Mellon University
	Drexel University
	Pennsylvania State Univ University Park
	Robert Morris University
Puerto Rico	Polytechnic University of Puerto Rico
Rhode Island	University of Rhode Island
South Carolina	Citadel Military College of South Carolina
South Dakota	Dakota State University
Tennessee	Tennessee Technological University
	University of Memphis
	University of Tennessee Chattanooga
Texas	Sam Houston State University
	Texas A&M University
	University of Houston
	University of Texas at Dallas
	University of Texas at El Paso
	University of Texas at San Antonio
Utah	Brigham Young University
Virginia	Hampton University
	Marymount University
	Norfolk State University
	Old Dominion University
	Virginia Polytechnic Institute and State University
Vermont	Norwich University
Washington	University of Washington - Tacoma
Wisconsin	Marquette University

APPENDIX H: SFS EVALUATION LOGIC MODEL

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

Initiatives

SFS school staff: PIs, Co-PIs, Program Coordinators, faculty

hiring officials, recruiters, and

Planning & Risk Management

communication & coordination

Resources (e.g., Tech, faculty

counseling

- PI training & education

Intended Intermediate

Scholars

Increased:
- interest in government cyber career
- fit with program
- academic experience
- access & use of learning opportunities
- preparation for government career
- fit with internship & internship experiences
- fit with mentor & mentoring experiences
- alignment between expectations & experiences
- public service motivation

Graduates

Increased:
- placement
- sufficient job performance
- possession of technical & general competencies
- fit with agency
- goal achievement
- satisfaction with agency, job & supervisor

SFS Schools

Increased:
- knowledge of roles & responsibilities
- quality relationships with other SFS institutions
- quality & diversity of students admitted
- partnerships with agencies
- graduate placement support
- alignment with placement reqs
- relevant curriculum
- SFS visibility
- faculty

OPM SFS Program Office

Increased:
- attendance and satisfaction with virtual job fair/agency info sessions & in-person job fair
- use & satisfaction with OPM SFS website
- scholar satisfaction with access & communication

Government Agencies

Increased:
- timely placement
- workforce capacity to address emerging cyber technologies
- satisfaction with SFS interns & graduates

Recruitment of high-

Increased education

Outcomes

Unintended Outcomes

⇧

Contextual Factors

- Economy
- Job market
- Public opinion

- Cybersecurity threats/acts of terrorism
- New or emerging cybersecurity threats
- New scientific advances & technology

Private sector trends & cybersecurity issues
- Laws, legislations & mandates

82

- Agency priorities & plans
- Agency policies & budget
- Media

APPENDIX I: LIST OF SATC-EDU AWARDS (FY 2022 – 2023)

Title	Year Funded	State	Organization	Award Amount	Award Page
Collaborative Research: SaTC: EDU: Authentic Learning of Machine Learning in Cybersecurity with Portable Hands-on Labware	2021	GA	Kennesaw State University Research and Service Foundation	$279,844	2100115
Collaborative Research: SaTC: EDU: Authentic Learning of Machine Learning in Cybersecurity with Portable Hands-on Labware	2021	AL	Tuskegee University	$119,982	2100134
Collaborative Research: SaTC: EDU: A Hands-on Approach to Securing Self-Driving Networks	2021	NC	North Carolina Agricultural and Technical State University	$173,536	2113945
Collaborative Research: SaTC: EDU: A Hands-on Approach to Securing Self-Driving Networks	2021	TX	University of Texas at San Antonio	$226,438	2113981
Collaborative Research: SaTC: EDU: Security and Privacy Implications of Remote Proctoring for School Policies and Practices	2022	DC	Georgetown University	$190,737	2138078
Security and Privacy Implications of Remote Proctoring for School Policies and Practices	2022	DC	George Washington University	$309,163	2138654
Examining Pedagogy in Cybersecurity at Military Academies	2022	MD	University of Maryland Baltimore County	$262,209	2138921
Examining Pedagogy in Cybersecurity at Military Academies	2022	IL	University of Illinois at Urbana-Champaign	$176,277	2138925
Examining Pedagogy in Cybersecurity at Military Academies	2022	MN	University of Minnesota Duluth	$61,412	2138934
Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2021	NC	North Carolina Agricultural and Technical State University	$113,947	2150297
SaTC: EDU: Building a Cyber Security Enhanced Education Laboratory for Hands-on Experience Oriented Cybersecurity Education	2022	NH	University of New Hampshire	$399,999	2154606
Collaborative Research: SaTC: EDU: A Hands-on Approach to Securing Self-Driving Networks	2022	NC	University of North Carolina at Pembroke	$226,438	2203094
Pedagogical Tools for Formal Methods	2022	RI	Brown University	$499,999	2208731
Authentic Learning Modules for DevOps Security Education	2022	TN	Tennessee Technological University	$154,006	2209636
Authentic Learning Modules for DevOps Security Education	2022	AL	Tuskegee University	$119,996	2209637
Authentic Learning Modules for DevOps Security Education	2022	GA	Kennesaw State University Research and Service Foundation	$125,880	2209638
SaTC: EDU: Building an Internet Emulator for Cybersecurity Education	2022	NY	Syracuse University	$399,197	2214916
SaTC: EDU: Collaborative: Incorporating Sociotechnical Cybersecurity Learning Within Undergraduate Capstone Courses	2022	UT	University of Utah	$283,961	2221870
An Integrative Hands-on Approach to Vehicular Security Education	2022	FL	University of Florida	$500,000	2221900
Collaborative Research: SaTC: EDU: Dual-track Role-based Learning for Cybersecurity Analysts and Engineers for Effective Defense Operation with Data Analytics	2023	NY	Rochester Institute of Tech	$367,447	2228001
Collaborative Research: SaTC: EDU: Dual-track Role-based Learning for Cybersecurity Analysts and Engineers for Effective Defense Operation with Data Analytics	2023	NY	University of Rochester	$130,557	2228002

APPENDIX I: LIST OF SATC-EDU AWARDS (FY 2022 – 2023)

Title	Year Funded	State	Organization	Award Amount	Award Page
					2230609
Collaborative Research: SaTC: EDU: Adversarial Malware Analysis - An Artificial Intelligence Driven Hands-On Curriculum for Next Generation Cyber Security Workforce	2023	NC	North Carolina Agricultural and Technical State University	$200,000	2230610
Collaborative Research: SaTC: EDU: Fire and ICE: Raising Security Awareness through Experiential Learning Activities for Building Trustworthy Deep Learning-based Applications	2023	GA	Georgia State University Research Foundation, Inc.	$235,255	2244219
Collaborative Research: SaTC: EDU: Fire and ICE: Raising Security Awareness through Experiential Learning Activities for Building Trustworthy Deep Learning-based Applications	2023	TX	Texas Christian University	$220,000	2244220
Collaborative Research: SaTC: EDU: Fire and ICE: Raising Security Awareness through Experiential Learning Activities for Building Trustworthy Deep Learning-based Applications	2023	GA	Kennesaw State University Research and Service Foundation	$44,734	2244221
SaTC: EDU: Collaborative: INteractive VIsualization and PracTice basEd Cybersecurity Curriculum and Training (InviteCyber) Framework for Developing Next-gen Cyber-Aware Workforce	2023	CT	Fairfield University	$231,422	2245148
SaTC: EDU: Inculcate a culture of preparedness against AI security threats to pervasive robotic systems	2023	MS	Mississippi State University	$399,978	2246920
SaTC-EDU: Case Analysis for Security Education (CASE)	2023	MI	Michigan Technological University	$399,797	2247492
SaTC: EDU: Expanding Digital Forensics Education with Artifact Curation and Scalable, Accessible Artifact Exercises	2022	LA	Louisiana State University	$300,000	2303715
SaTC-EDU: Improving computer forensic curricula through hands-on hardware and software training and practical experience processing evidence from active criminal cases	2023	CA	San Jose State University Foundation	$498,507	2304753
SaTC: EDU: Advancing Cybersecurity and Privacy of Educational Technologies Used in K-12 schools	2022	NC	North Carolina State University	$499,971	2309400
Authentic Learning Modules for DevOps Security Education	2023	AL	Auburn University	$154,006	2310179
SaTC: EDU: Enhancing Cybersecurity Training for Next Generation Healthcare Professionals	2023	PA	Temple University	$400,000	2310298
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2023	MD	University of Maryland Baltimore County	$320,000	2317117
SaTC: EDU: Digital Safety Immersion for Elementary School Students	2023	NC	North Carolina State University	$399,999	2319015
Collaborative Research: SaTC: EDU: Creating Windows Advanced Memory Corruption Attack and Defense Teaching Modules	2023	MA	University of Massachusetts Lowell	$330,000	2325451
Collaborative Research: SaTC: EDU: Creating Windows Advanced Memory Corruption Attack and Defense Teaching Modules	2023	FL	The University of Central Florida Board of Trustees	$70,000	2325452
Collaborative Research: EAGER: SaTC-EDU: Secure and Privacy-Preserving Adaptive Artificial Intelligence Curriculum Development for Cybersecurity	2023	TX	Southern Methodist University	$30,236	2335624

APPENDIX J: SFS AND SATC-EDU AWARDS SUPPORTING CHIPS AND SCIENCE ACT PRIORITY AREAS

Advanced Communications Technologies

Title	Year Funded	State	Organization	Award Amount	Award Page
SaTC: EDU: Software Defined Radio Wars for Cybersecurity and Information Assurance Education	2016	PA	Drexel University	$299,888	1723606
Collaborative Research: SaTC: EDU: A Comprehensive Training Program of AI for 5G and NextG Wireless Network Security	2023	FL	University of South Florida	$200,000	2321270
Collaborative Research: SaTC: EDU: A Comprehensive Training Program of AI for 5G and NextG Wireless Network Security	2023	OK	University of Oklahoma Norman Campus	$200,000	2321271
SaTC: EDU: Learning Moving Target Defense Concepts: Teaching and Training Curricula Development Based on Software Defined Networking and Network Function Virtualization	2016	AZ	Arizona State University	$299,756	1723440

Aerospace

CyberCorps Scholarship for Service: High-skilled Workforce Development for the Aviation and Aerospace Cybersecurity Domains	2022	FL	Embry-Riddle Aeronautical University	$3,448,853	2146462
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2019	FL	Embry-Riddle Aeronautical University	$320,000	1956193
SaTC: EDU: Collaborative: Bolstering UAV Cybersecurity Education through Curriculum Development with Hands-on Laboratory Framework	2019	IL	University of Illinois at Chicago	$179,999	1955337
The Indiana University Space-Cybersecurity Security and Governance Program: Breaking Down Silos and Building Bridges to Raise Awareness of Opportunities, Expand, and Diversity the Space-Cybersecurity Workforce	2023	IN	Indiana University	$287,292	2332599

Artificial Intelligence (FY 2022-2023 only)

Collaborative Research: SaTC: EDU: Artificial Intelligence Assisted Malware Analysis	2021	NC	North Carolina Agricultural & Technical State University	$113,947	2150297
Collaborative Research: SaTC: EDU: Adversarial Malware Analysis - An Artificial Intelligence Driven Hands-On Curriculum for Next Generation Cyber Security Workforce	2023	TN	Tennessee Technological University	$300,000	2230609
Collaborative Research: SaTC: EDU: Adversarial Malware Analysis - An Artificial Intelligence Driven Hands-On Curriculum for Next Generation Cyber Security Workforce	2023	NC	North Carolina Agricultural & Technical State University	$200,000	2230610
SaTC: EDU: Inculcate a culture of preparedness against AI security threats to pervasive robotic systems	2023	MS	Mississippi State University	$399,978	2246920
Collaborative Research: SaTC: EDU: Dual-track Role-based Learning for Cybersecurity Analysts and Engineers for Effective Defense Operation with Data Analytics	2023	NY	Rochester Institute of Tech	$367,447	2228001
Collaborative Research: SaTC: EDU: A Comprehensive Training Program of AI for 5G and NextG Wireless Network Security	2023	FL	University of South Florida	$200,000	2321270
Collaborative Research: SaTC: EDU: A Comprehensive Training Program of AI for 5G and NextG Wireless Network Security	2023	OK	University of Oklahoma	$200,000	2321271

APPENDIX J: SFS AND SATC-EDU AWARDS SUPPORTING CHIPS AND SCIENCE ACT PRIORITY AREAS

Semiconductors

Title	Year Funded	State	Organization	Award Amount	Award Page
					1623310
EDU: Collaborative: HACE Lab: An Online Hardware Security Attack and Countermeasure Evaluation Lab	2015	FL	Florida Institute of Technology	$100,000	1623299
SaTC-EDU: PHIKS - PHysical Inspection and attacKs on electronicS	2017	FL	University of Florida	$299,999	1821780
Collaborative Research: EAGER: SaTC-EDU: Dynamic Adaptive Machine Learning for Teaching Hardware Security (DYNAMITES)	2020	NY	New York University	$150,000	2039607
Collaborative Research: EAGER: SaTC-EDU: Dynamic Adaptive Machine Learning for Teaching Hardware Security (DYNAMITES)	2020	TX	Texas A&M	$150,000	2039610
Collaborative Research: SaTC: EDU: Hardware Security Education for All Through Seamless Extension of Existing Curricula	2020	FL	University of Florida	$119,957	2114165
Collaborative Research: SaTC: EDU: Hardware Security Education for All Through Seamless Extension of Existing Curricula	2020	FL	Florida International University	$184,967	2114200

Quantum Computing

EDU: QuaSim: A Virtual Interactive Quantum Cryptography Educator-A Project-based Gamified Educational Paradigm	2016	NE	University of Nebraska at Omaha	$290,037	1623380
SaTC: EDU: A Curriculum for Quantum Security and Trust	2021	PA	Pennsylvania State Univ University Park	$400,000	2113839
Collaborative Research: SaTC: EDU: QUINTET: Quantum Internet Education and Training Synthesizer	2023	GA	Kennesaw State University Research and Service Foundation	$212,245	2324924
Collaborative Research: SaTC: EDU: QUINTET: Quantum Internet Education and Training Synthesizer	2023	NE	University of Nebraska at Omaha	$187,611	2324925

GLOSSARY

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

Deferral: An approved extension of the obligation phase.

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

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

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

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

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

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

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

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

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

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

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