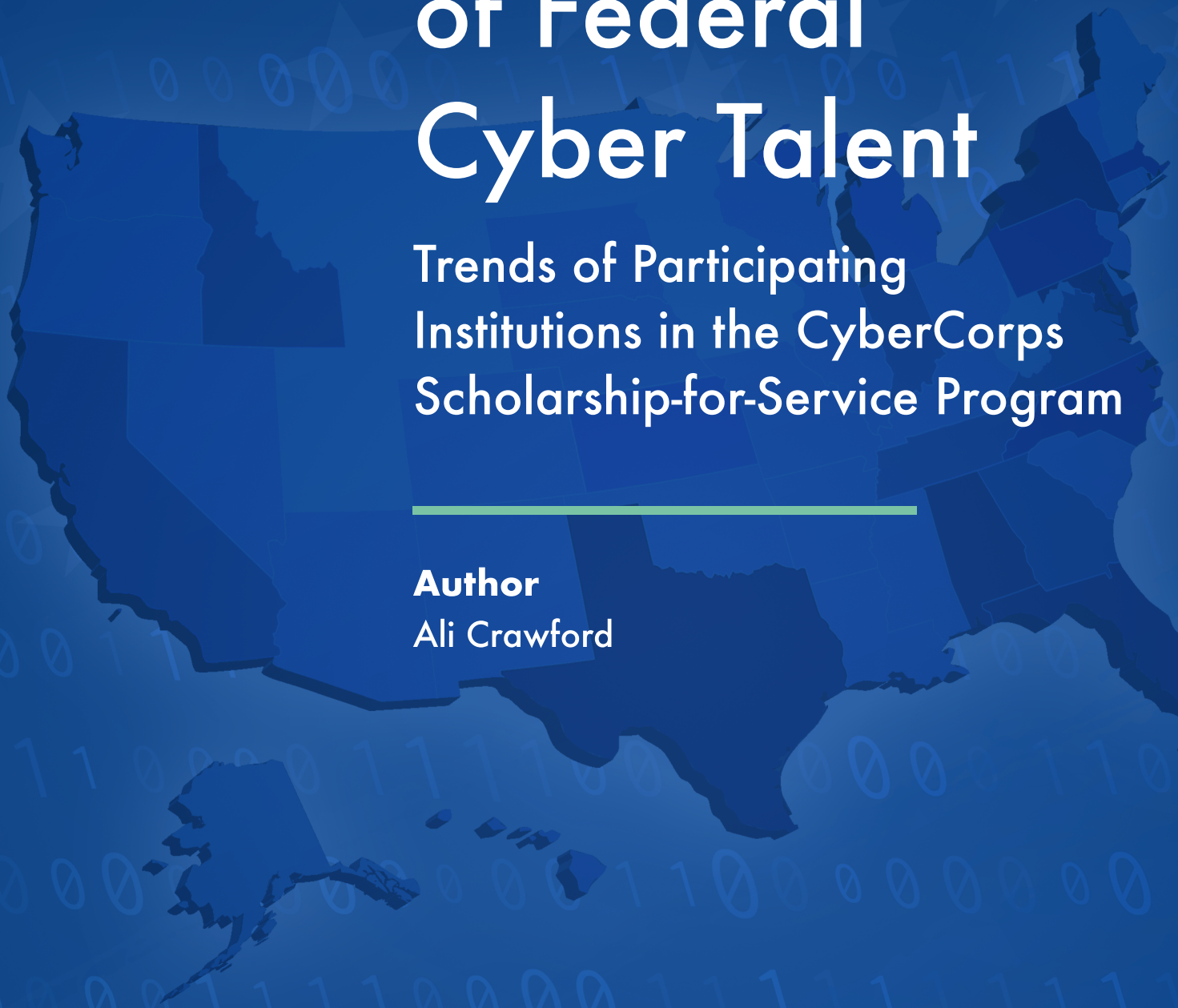
Policy Brief

The Core of Federal Cyber Talent

Trends of Participating Institutions in the CyberCorps Scholarship-for-Service Program

Author
Ali Crawford



CSET CENTER for SECURITY and EMERGING TECHNOLOGY

January 2024

Executive Summary

The National Science Foundation's (NSF) CyberCorps scholarship-for-service (SFS) program is a direct cyber talent pipeline into the federal workforce that awards grants to institutions that then provide generous scholarships to students pursuing degrees in cyber and cyber-related fields of study. In exchange, students agree to work for the federal government for the same length of time as their award. Despite its longevity, there is minimal public research about the CyberCorps program. Given recent calls for CyberCorps program expansion, this paper identifies trends found from interviews with principal investigators (PIs) from participating institutions in the CyberCorps program.* These insights may help policymakers, program decision-makers, and academic institutions to better assess how the program might expand, what factors might prevent expansion or greater participation, and ultimately how to increase the output of cyber talent into the federal workforce and beyond. Additionally, the findings and recommendations provide important observations that are relevant to the build-out of the proposed artificial intelligence (AI) federal SFS program.

This report helps to shed light on why institutions seek to be part of the program, what factors make an institution's program successful, what fields of study student recipients are pursuing, and why programs might focus on graduate students over undergraduate students—all of which inform the changes PIs would like to see in the CyberCorps program. Suggested improvements include: (1) structuring the program to allow for more PhD candidates, (2) increasing inclusion of community and technical college talent, (3) considering other metrics for program evaluation besides achieving 100% recipient placement in the federal government, and (4) streamlining the grant-renewal process for successful institutions while also considering the rising costs of tuition and living. PIs offered recommendations to improve the onboarding and retention of CyberCorps graduates within the federal government. Recommendations include addressing security clearance wait times and other federal hiring uncertainties and increasing awareness of the CyberCorps program among hiring authorities across the government.

---

* The National Security Commission on Artificial Intelligence, the Cyber Solarium Commission 2.0, and the National Cyber Workforce and Education Strategy all recommend some form of CyberCorps program expansion or improvement.

The following recommendations are based upon the assumption that the CyberCorps program's primary goal is to place cyber talent into the federal workforce:

Adding more PhD candidates to the program should be based on the federal demand for all educational levels of cyber talent. Doctorates presently make up less than 2% of the federal cyber workforce.[1] Without knowing the actual federal demand for this talent, supporting more PhD CyberCorps students might not necessarily be in the program's best interest considering the limited number of undergraduate and graduate students already being produced. However, if there is a high federal demand for PhD cyber talent, then CyberCorps could be missing an important opportunity to funnel highly educated candidates into the federal workforce.

Individuals with an education level between high school and a bachelor's degree, which we can assume is an associate's degree or similar, make up a larger 16% of the federal cyber workforce.[2] Despite this progress, community and technical college graduates might not be eligible for certain federal jobs despite demonstrating core competencies or technical skills. This is likely due to a predominant focus on four-year degrees as a minimum qualification, which limits the potential of community college talent.[3]

The CyberCorps program and the federal government should prioritize reducing hiring uncertainties and increasing retention efforts for CyberCorps recipients. If CyberCorps recipients are willing and able to enter the federal workforce, the hiring process should not dissuade them from fulfilling their obligations when they could easily turn to the private sector. Ideally, and given the amount of federal dollars invested in each candidate, recipients should be able to begin their security clearance process prior to graduation and should have specific hiring preference outside of general cyber-related special hiring authorities.

The NSF should streamline the renewal process for successful programs and consider other metrics for program evaluation. PIs expressed frustration with the renewal process despite maintaining programs that meet NSF requirements, and would like to see the cost of living and tuition taken into consideration when granting or renewing an award. Additionally, there is a sense among PIs that grants focus too much on research as a metric for program evaluation. Not every institution has the capacity or purpose to produce high-quality or experimental applied cyber research, but this does not mean that the institution isn't still producing much-needed cyber talent.

Table of Contents

Executive Summary 1
Table of Contents 3
Introduction 4
The CyberCorps Program 6
Brief program history 6
Current program analysis 7
Summary 9
Institutional Trends 10
Institutional motivations for applying to the CyberCorps program 10
Factors that make an institution's CyberCorps program successful 10
Student fields of study and degree level 11
Participation in other federal cyber scholarship-for-service programs 12
Recommended areas for program improvement 13
Challenges in federal workforce fulfillment obligations 15
Assessment of Trends and Recommendations 17
Summary 20
Implications for an AI Federal Scholarship-for-Service Program 21
Conclusion: Future Considerations for the CyberCorps Program 23
Author 24
Acknowledgments 24
Endnotes 25

Introduction

In 1998, Presidential Directive 63 created the National Plan for Information Systems Protection, which was the first major federal plan concerned with the protection and defense of America against cyber threats.[4] Among several initiatives created from this plan was the National Science Foundation's (NSF) CyberCorps scholarship-for-service (SFS) program, which was intended to increase the capacity of information technology specialists and to produce more talent for the federal workforce.[5] In 2000, four institutions received the first CyberCorps grant and produced nine graduates. Since then, the program has expanded to 135 universities and has produced roughly 4,000 graduates.

The CyberCorps program has largely been a success since its inception considering its longevity and sustained congressional funding. But the cybersecurity concerns and vulnerabilities of the early 2000s are still very real threats today—including a pressing need for more cyber talent. Both the Cyber Solarium Commission 2.0 and the National Security Commission on Artificial Intelligence (NSCAI) recommend expanding CyberCorps to produce significantly more graduates.[6] The more recent National Cyber Workforce and Education Strategy (NCWES) also provides objectives for supporting CyberCorps expansion.

However, the NCWES highlights that the demand for skilled cyber workers is outpacing supply.[7] Studies cited in the report estimate a demand for 411,000 cybersecurity workers, and data from CyberSeek (a National Initiative for Cybersecurity Education partner) indicates there are more than 600,000 cyber vacancies across public and private sectors.[8] Therefore, calls for expansion of the CyberCorps program seem both warranted and necessary amid increasing needs. Understanding how CyberCorps programs are growing at each institution, or what is preventing growth, can inform how CyberCorps could expand.

Presently, there is a lack of public comprehensive research on the CyberCorps program, making it difficult to assess expansion. Limited data from two important sources informs this work: a Government Accountability Office (GAO) report, which outlines actions needed to improve the CyberCorps program, and the NSF's 2021 Biennial Report on the CyberCorps program.[9] Yet, important knowledge gaps remain. This paper addresses these by distilling trends from structured interviews with principal investigators (PIs) from institutions that participate in the CyberCorps program. Out of 135 institutions contacted, a total of 25 responded to interview requests. The interviews have been anonymized and aggregated.

Specifically, this paper examines how participating institutions are recruiting students, maintaining their programs, and placing their graduates. This analysis also includes trends in institutional best practices, expansion recommendations, and challenges, with the goal of elevating the program for the continued production of cyber talent for the federal workforce and beyond.

The scope of this paper is limited to current participating institutions in the CyberCorps program. Some institutions do participate in similar cyber SFS programs, such as the CySP or SMART programs through the Department of Defense (DOD), but this paper focuses specifically on CyberCorps because it is arguably the most public-facing federal cyber-specific scholarship program. It also has a broad reach, allowing scholarship recipients to fulfill their obligations through service in a variety of federal, state, local, tribal, and academic positions.

Lastly, this paper is motivated by the recent passage of the CHIPS and Science Act, which directs the NSF to explore the feasibility of setting up a separate AI federal SFS.[10] While this feasibility study is currently ongoing, observations and best practices presented in this paper can help inform how an AI SFS can be most impactful by understanding the federal government's specific talent needs, what challenges prevent institutions from producing more talent, and where program improvements can be made.

The CyberCorps Program

Brief program history

The NSF's CyberCorps program provides participating institutions with scholarship funding for students studying computer science, cybersecurity, and other cyber-related fields of study.[11] In exchange, students are required to work in a cyber or cyber-related position for the federal government for the same length of time as their scholarship. In some cases, students may be able to fulfill their workforce obligations within state, local, or tribal governments; federally funded research and development centers; or academia. In practice, there are placement caps on where students can and cannot go: 70% can secure placement in the executive branch; 20% in state, local, or tribal government positions or federally funded research institutions; and 10% as educators at other SFS institutions.[12]

CyberCorps was initially established in 1998 and has since been amended by the Cybersecurity Enhancement Act of 2014 and the National Defense Authorization Acts of 2018 and 2021.[13] The program is authorized by Congress and funding is appropriated through fiscal year 2026.[14] Funding for FY2024 and FY2025 is $78 million and $84 million, respectively. Awarded scholarships are designed to support up to three years of tuition and related costs. Undergraduate students receive $27,000 and graduate students receive $37,000 in additional stipends. An allowance of $6,000 per academic year is provided for the annual job fair in Washington, D.C., and for other expenses like travel, conferences, research materials and supplies, books, professional training, and certifications.[15] Students must be full-time and either U.S. citizens or lawful permanent residents, and they have 18 months after completing their degree program to find acceptable employment. Students who fail to fulfill their workforce obligations—meaning they pursue employment outside of the acceptable pathways—are required to repay the amount of the scholarship award received or the award may be converted into a direct unsubsidized loan.[16] Students are also required to take an internship during their funding duration.

Education institutions apply to receive CyberCorps funding from the NSF. Proposals must first provide clearly documented evidence of a strong academic program in cybersecurity, such as an Accreditation Board for Engineering and Technology accreditation in cybersecurity, a designation as a National Center of Academic Excellence (NCAE), or equivalent evidence documenting a strong program in cybersecurity.[17] The NSF proposal merit review process evaluates all proposals based

on criteria established by the National Review Board.[†] In addition to these criteria, CyberCorps proposals specifically are evaluated on (1) quality and availability of cyber education and research, including research opportunities; (2) quality of experiential learning; (3) quality of and extent to which students are engaged in cyber-related extracurricular activities; and (4) evidenced-based inclusion initiatives.[18]

If an institution is selected, it has full authority over the recipient selection process and the administration of scholarship funding over the five-year grant period. After this period ends, an institution must apply for renewal. Until 2017, there were two funding tracks: the scholarship track and the capacity-building track. The latter merged with the cross-agency Secure and Trustworthy Cyberspace program in 2018 to fund proposals for projects that align with national strategies to increase the U.S. ability to produce cyber talent and bolster workforce development.[19]

Current program analysis

As of 2023, there are 135 active participating institutions that have collectively produced over 4,000 CyberCorps graduates since the program's inception.[20] Eight community colleges participate as part of the Community College Cyber Pilot Program where CyberCorps grants are awarded directly to community colleges. There are 28 additional community colleges that participate as partners with an active program at a four-year university.[21] As shown in Figure 1, states with the most active participating institutions are Texas (11), Alabama (10), New York (9), Maryland (9), and Florida (8). Currently, 11 states do not have an active CyberCorps program.[‡] Anecdotally, we learned that some schools choose not to apply to the CyberCorps program because they see the administrative burden of participating as outweighing the benefit. One PI suggested that a rationale for this is that graduates will "probably be recruited into these kinds of jobs anyways."

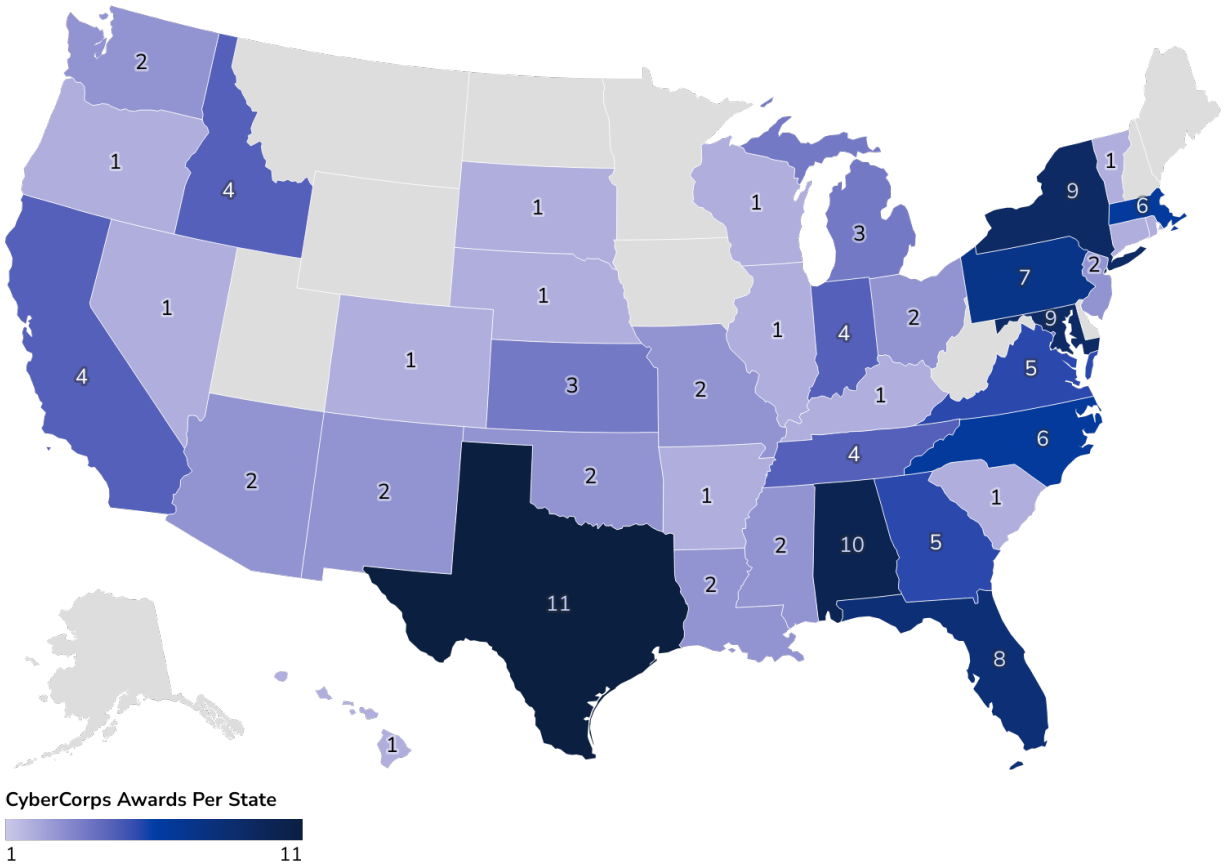
About 75% of CyberCorps institutions are designated as National Centers of Academic Excellence in Cyber. The NCAE-C is a consortium of over 400 postsecondary institutions that apply to receive this designation from the National Security Agency

[†] These criteria include: (1) to what extent the proposal suggests and explores creative, original, or potentially transformative concepts; (2) if it's well-reasoned, well organized, and based on sound rationale; and (3) if the team is well qualified to carry out the proposal.

[‡] Alaska, Delaware, Iowa, Maine, Minnesota, Montana, New Hampshire, North Dakota, Utah, West Virginia, and Wyoming.

(NSA). Institutions must meet high academic standards to be eligible for the program. In 2020, NCAE-C institutions produced 50% of all cyber and cyber-related bachelor's degrees in the United States.[22]

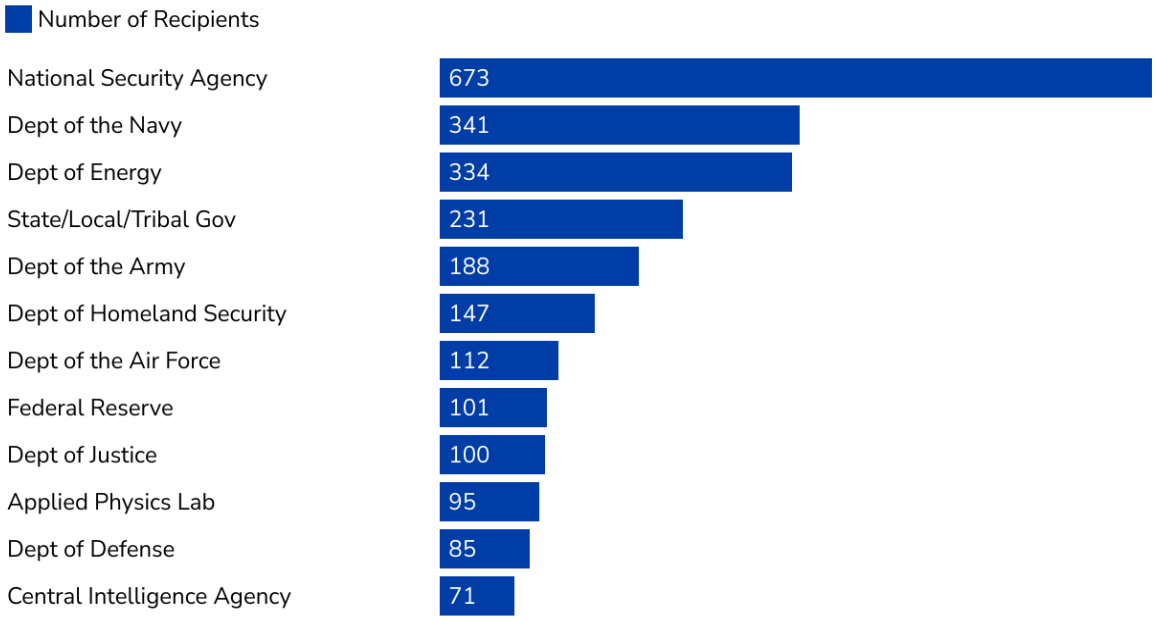
Figure 1. Institutions with CyberCorps Awards per State as of 2023



Source: National Science Foundation.[23]

Figure 2 shows the top placement agencies of CyberCorps students over the last two decades.[24] The NSA received the most CyberCorps graduates, about 30%, while 14% of graduates fulfilled their workforce obligations with the Department of the Navy and 14% percent with the Department of Energy.

Figure 2. Top Federal Agency Placements Of CyberCorps Recipients, 2001-2021



Source: National Science Foundation.[25]

Summary

Federal cyber occupations such as computer science, computer engineering, and intelligence saw negative growth in new hires over the last two years.[26] Therefore, calls for expansion of the CyberCorps program seem both warranted and necessary amid increasing needs for cyber talent both in the federal workforce and beyond. Understanding how CyberCorps programs are growing at each institution, or what is preventing growth, will inform how CyberCorps should consider expanding and how best to implement the recommendations from bodies like the Cyber Solarium Commission in the future.

Institutional Trends

To gain a deeper understanding of the CyberCorps program, we spoke with 25 PIs from participating institutions to determine and assess trends in best practices, challenges, barriers to workforce entry for students, institutional characteristics, and areas where the CyberCorps program could expand or change. Interview questions are categorized below into themes and are aggregated to reflect general trends in responses from interviewed PIs.

Institutional motivations for applying to the CyberCorps program

Most of the interviewed PIs acknowledged that the federal government is in serious need of cyber talent. Because of this, PIs were motivated to apply for a CyberCorps grant to provide students with scholarships that are tied to public service—especially if the institution is located in an area with a high federal footprint. Also, the prestige of the CyberCorps program and the potential to establish a working relationship with the federal government were important incentives. Being a recipient of a highly selective federal scholarship program is an attractive marketing and recruitment tool.

Factors that make an institution's CyberCorps program successful

In our interviews with the PIs, the following factors came up consistently as making for a successful CyberCorps program. PIs believe that a successful program is defined by grant renewals, achieving 100% student placement, or program growth. During the grant application process, institutions focus on their individual strengths in additional areas, such as:

- **Proximity to federal employment opportunities:** As noted by one PI, competitive proposals to the NSF are ones that have definitive plans to put students into federal jobs. While not every institution is close to Washington, D.C., some are situated in regions across the country with a high federal footprint. For these institutions, the job opportunities for students post-graduation could be relatively close to home. This creates an ecosystem where local federal demand for cyber talent is met through the supply of CyberCorps graduates. Local federal opportunities might also include institutes or research centers either inside or outside the university that collaborate with federal departments or agencies.
- **Established mentorship networks:** Six of the PIs specifically mentioned using mentorship networks as a program strength. Mentorship varies across

institutions, but generally scholarship recipients are paired with one or more student, faculty, or industry mentor. In some cases, institutions have close relationships with their CyberCorps alumni who also provide mentorship and counsel. Reliance on alumni is particularly helpful for students navigating their federal job searches after graduation.

- **Education and extracurriculars:** Seven PIs specifically emphasized how student participation in extracurricular activities like cybersecurity competitions is an important part of their program. Extracurriculars are often hands-on or applied learning experiences that enhance a student's cybersecurity education. As the next section will discuss further, nine PIs mentioned their program's focus on cross- or multi-disciplinary cyber education. Additionally, there is a major emphasis on research opportunities for CyberCorps students. Twenty-three of the institutions we spoke with specifically mention access to high-quality research opportunities in their respective NSF proposals.

Student fields of study and degree level

According to the NSF's 2021 Biennial Report, CyberCorps students are mostly majoring in computer science.[27] In reality, recipients are pursuing diverse fields of study and concentrations. PIs report students studying computer science with concentrations in areas such as engineering, cybersecurity, and software development. While some schools continue to focus on technical fields of study for their recipients, other schools are increasingly recruiting from different colleges across their respective campuses. Other PIs reported students studying business, law, political science, and criminal justice, where they are concentrating in areas like cybersecurity, cyber operations, digital forensics, network security, and management of information systems and security. As noted by one PI, "The graduates of these programs are employable across a variety of federal agencies and not just the NSA."

According to the NSF's Biennial Report, the most common degree among CyberCorps students is a master's (53%), followed by a bachelor's (39%), PhD (4%), and associate's (4%).[28] This breakdown is relatively similar to that of the institutions interviewed but with important additional context. Based on the interviews, some programs focus mainly on the recruitment of undergraduate or graduate students and recruit at different levels for different reasons.

PIs might focus on undergraduates for these reasons:

- Limited master's or doctoral programs at a particular institution in cyber or cyber-related fields of study (e.g., only a bachelor's in computer science but no master's program in computer science).
- A larger applicant pool at the undergraduate level because, in some instances, there are fewer U.S. citizens at the graduate level.[§] CyberCorps recipients must be U.S. citizens or lawful permanent residents. Even then, some federal jobs require U.S. citizenship.
- Greater familiarity among PIs and selection committees with potential recipients, their academic aptitude, and their interest in the field if they have been studying at the same institution during their undergraduate career.

PIs might focus on graduates for these reasons:

- Students qualify for more federal positions, often with slightly higher salaries, with a graduate degree. A prospective employee with a master's degree typically starts as a higher level in the General Schedule for the federal government, which is usually a GS-9, compared to a GS-7 for applicants with a bachelor's degree.[29]
- Graduate students in cyber and cyber-related fields have demonstrated their commitment to the field and might better understand the conditions of their scholarship.

Participation in other federal cyber scholarship-for-service programs

Fifteen of the institutions we spoke with either had or currently have active student participants in the DOD's CySP or SMART program, but these are often administered by different faculty members or departments. The DOD's CySP program operates very similarly to CyberCorps, but CySP recipients are limited to fulfilling their workforce obligations specifically within the DOD. Beyond these restrictions, we learned that

[§] Stanford's 2023 "AI Index Report" indicates that 65.2% of computer science master's degree graduates and 68.6 percent% of computer science doctoral degree graduates are international students. Nestor Maslej et al., "The AI Index 2023 Annual Report" (Institute for Human-Centered AI, Stanford University, 2023), https://aiindex.stanford.edu/wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

there are other unique differences between CyberCorps and CySP that are helpful when considering how CyberCorps could expand in the future.

The NSF awards CyberCorps grants to institutions for the PI to administer to selected students. For CySP, eligible students apply directly to the DOD program office; to be eligible, students must attend an institution with an NCAE-C designation that has a preexisting relationship as a cooperating partner with the CySP program office. The institution must apply to the CySP program, alongside the student applicant, if there is no established relationship.

Recipients are extended employment offers if they are accepted into the CySP program, meaning that they can start their clearance process while they are finishing their studies. This can significantly reduce the time the student has to wait to begin their job, as well as employment uncertainty. The CySP program has two other scholarship tracks. Accepted institutions with accepted students can apply for capacity-building grants. These grants can be utilized for purposes such as faculty professional development or research infrastructure. There is also a retention scholarship that can be awarded to DOD civilians, military officers, and enlisted personnel who want to pursue a master's or doctoral degree in cyber-related fields of study. These program characteristics are relevant when considering some of the CyberCorps administrative challenges mentioned by PIs.

Recommended areas for program improvement

The PIs collectively agree that the CyberCorps program is a useful way to incentivize cyber talent into the federal workforce. However, there are areas where the PIs feel that the program could improve or expand to reach more institutions or to produce more graduates.

- **More support for PhD students:** The current CyberCorps program is not necessarily structured to support PhD students. Half of the PIs we spoke with strongly believe that the return on investment for PhD students benefits both academia and the federal government. Presently, CyberCorps funding is capped at three years, which complicates fully funding PhD candidates since it often takes five years or more to complete degree requirements.

  To work with PhD candidates, PIs must find additional funding streams before or after the three-year cap is reached. In some cases, PhD candidates will receive CyberCorps funding for the three-year allotment and "fulfill" their workforce obligations by teaching at their respective institutions while finishing their

program. This does not mean that the program does not produce PhD graduates, but they represent a small number of total recipients. Only 4% of CyberCorps graduates are PhDs, or roughly 150 graduates since the start of the program.[30]

Research opportunities and output are the main factors by which an institution is evaluated when applying or renewing. But some PIs point out that more impactful cyber research occurs at the PhD level, suggesting that not having more doctoral candidates means that less cyber research can be funded.

- **Increased community and technical college inclusion:** PIs would also like to see more community and technical college participation, but students at community colleges can face unique challenges. According to the PIs we spoke with, students with degrees from community colleges are generally not "qualified" for federal jobs despite graduating with demonstrable competency in cyber skills, or the jobs for which they are qualified tend to start at lower GS scales and are not particularly attractive.

  Around 4% of total CyberCorps recipients graduated with an associate's degree, which is also about 150 graduates since the beginning of the program.[31] The federal cyber workforce could benefit from hiring graduates from community and technical colleges, and the NSF could be a real champion for understanding and promoting the value of cyber and technical associate's degrees, certifications, and short-term programs—another core tenant of the NCWES.[32] Additionally, program costs per student at these institutions are likely lower and would enable more output, providing an excellent return on investment for the CyberCorps program and the federal government.

- **Streamlining the renewal process and award increases:** When institutions seek a grant renewal from the NSF, they must still undergo a competitive process even when a program has a demonstrated history of success. Renewals are primarily based on a program's ability to place all CyberCorps recipients into the federal government or other acceptable areas of employment. As noted by one PI, "If you don't reach these placement requirements it can count against your renewal." As such, this metric plays an outsize role in whether an institution is renewed. Where students ultimately end up fulfilling their workforce obligations is largely outside of a PI's control, and uncertainties surrounding the federal hiring process are outside of both the student's and the PI's control.

The emphasis on student placement becomes especially salient when there are only a limited number of CyberCorps recipients that an institution can produce each year. On average, participating institutions graduate four or five CyberCorps students per year and 20 to 25 CyberCorps students per grant. Therefore, one or two students reneging on their obligation can significantly impact an institution's chances of renewing its grant.

PIs would also like to see NSF consider increased cost of living and tuition when granting or renewing an award. As these costs continue to rise, PIs worry that the number of CyberCorps students they can support will decrease.

- **Capacity-building and faculty development funding:** PIs would also like to see funding streams for faculty or research development similar to the capacity-building grants awarded by the DOD's CySP program. Some PIs note that administrative burdens prevent their program from expanding because they do not have the human or financial capital bandwidth to provide more specific classes, research opportunities, or mentorship. Until 2017, there were two funding tracks: the scholarship track and the capacity-building track. The latter merged with the cross-agency Secure and Trustworthy Cyberspace program in 2018.[33] It is unclear if PIs were not aware that there used to be a capacity-building funding stream or if they simply wish to bring it back.

Challenges in federal workforce fulfillment obligations

Though PIs are not necessarily struggling to meet student placement requirements, the process is not without complication. Challenges that come with entering the federal workforce are largely outside the control of both students and PIs, and yet fulfilling the federal workforce obligation is a major requirement for both. PIs felt that broad federal hiring uncertainties and a lack of awareness among federal agencies regarding the CyberCorps program are challenges for students attempting to enter the federal workforce.

- **Federal hiring uncertainties:** Ten PIs suggested that the biggest challenge their students face is wait time and uncertainty related to security clearance processing. In the CyberCorps program, students do not begin the security clearance process until after they complete their program of study. They are also responsible for securing their own employment. Other federal hiring uncertainties can complicate this process. It is not entirely uncommon to be

turned down for a security clearance, face unexpected job closures, or wait through federal hiring freezes—each with little to no prior warning.

Such uncertainties can cause students to fulfill their workforce obligations outside of the executive branch despite the caps on those channels, or to make the rare decision to abandon their obligations altogether. These uncertainties also place burdens on PIs that are largely outside of their control and yet directly affect their CyberCorps grant. For example, if a student decides to forgo his or her obligation, for many potential reasons, the institution may be "penalized" for not placing the students.

Anecdotally, we learned that slow security clearance processing has cost students their first-choice internships or jobs, or students have had industry offers to repay their CyberCorps debt to release them from their federal obligation. As noted by one PI, waiting six months to a year is tough when students know they could instead pursue lucrative industry careers.

- **Awareness:** More concerning, we found that being a CyberCorps recipient doesn't necessarily improve a student's hiring prospects with federal agencies and departments. Students have reported to their respective PIs that some hiring managers are not even familiar with the CyberCorps program. There is a shared sentiment among PIs that the agencies receiving the most CyberCorps students, like the NSA, are just more aware of the CyberCorps program and the kinds of cyber talent it produces and are therefore more involved in the program.

Assessment of Trends and Recommendations

Our research into the CyberCorps program found that institutions value participating in the program due to a deep belief in and commitment to public service, the opportunity to provide scholarships for students, and the prestige from partnering with the federal government. Overall, institutions would like to see some form of CyberCorps expansion with minor improvements.

For some PIs, this expansion means restructuring the program somewhat to support more PhD candidates. Such an expansion is challenging given the three-year cap for scholarships. Another factor preventing expansion is an institution's own faculty or staff shortages in computer science departments, which further emphasize the need for more PhD candidates. For other interviewees, expansion means increased community and technical college participation.

In addition, the grant renewal process for institutions already in the program can be burdensome. Program "success" seems to have an overdependence on an institution's ability to place 100% of its CyberCorps students into the federal workforce. Given federal hiring uncertainties, this factor is largely outside of both PI and student control. However, there really isn't a suitable replacement metric.

Based on our interviews and research into the program, we offer the following recommendations:

1. Any initiatives to expand the CyberCorps program should begin with an assessment of the federal demand for all levels of cyber talent. Expanding the program to produce more graduates is a key recommendation from the Cyber Solarium Commission 2.0.[34] Some PIs strongly believe that the CyberCorps program should restructure to be more inclusive of PhD students, and other PIs would like to see more community college participation. PhD and associate's graduates together only make up 8% of CyberCorps graduates. Before considering expanding the program to be more inclusive of either PhD or community college students, the NSF must conduct an assessment of the federal demand for these types of cyber talent.

1a. PhDs make up less than 2% of the federal cyber workforce.[35] What's unknown is if this number is small because there is not much of a federal demand, because the education system is not producing enough PhD graduates, or because of competition with the private sector for these highly skilled workers. Without knowing the actual federal demand for this talent and the government's ability to attract and retain this talent, supporting more PhD CyberCorps students might not necessarily be in the

program's best interest considering the limited number of undergraduate and graduate students already being produced. The risk is that fully funding more PhD students would decrease the overall number of yearly graduates given the longer completion times for PhD candidates and the increased overall expense.

However, if there is a high federal demand for PhD cyber talent, particularly in basic or applied research, then CyberCorps could be missing an important opportunity to funnel highly educated talent into the federal workforce, as suggested by the NCWES.[**] To produce more PhD CyberCorps professionals, the NSF would need to raise the scholarship funding duration caps to enable institutions to support more PhD candidates. The NCWES recognizes this challenge. Strategic Objectives 2.3.4 and 2.4.3 advocate for increasing participation in advanced degree programs to expand cyber faculty and to increase participation of students and teachers in cyber scholarship programs, respectively. The strategy contends that the White House and Congress will work together to enable scholarship recipients pursuing doctoral degrees to be eligible for five years of funding. This would result in more cyber and cyber-related expertise with research experience funneled into the federal government.

1b. Additionally, a few PIs expressed that both their CyberCorps and degree programs are not able to expand or grow due to cyber and computer science faculty shortages. The GAO acknowledges this as a serious risk for the CyberCorps program and an overarching problem for the U.S. education system.[36] To partly address this gap, the FY2021 National Defense Authorization Act expanded authorized employment options for CyberCorps recipients to include placement as an educator in the field of cybersecurity at universities participating in the program. The NCWES also wants to increase the participation of students and teachers in CyberCorps to create more cyber educators.[37] But PIs face pressure to achieve 100% federal placement, making the academia pathway less promising because of the 10% cap. A potential solution is to remove the 10% cap on the academia pathway, as well as to increase scholarship funding durations so that more PhD students can become educators in computer science or cyber fields.

1c. Community colleges are already being recognized for their cyber programs. There are 117 public two-year institutions and nine private two-year institutions with NCAE-C designations.[38] Despite this progress, community or technical college graduates might not be eligible for certain federal jobs despite demonstrating core competencies

[**] The NCWES states that the federal government requires a cyber research and development workforce with advanced degrees.

or technical skills. This is likely due to a predominant focus on four-year degrees as a metric for qualification that limits the potential of community college talent.[39] The Cyber Solarium Commission 2.0 notes that degree-based hiring requirements are unnecessarily constraining the federal cyber workforce, as the cyber industry is one where associate's degrees, industry certifications, and informal education are common and valued.[40]

2. Because participating institutions only graduate a small number of CyberCorps students each year, the program should prioritize reductions in hiring uncertainties and promote retention efforts for CyberCorps recipients. PIs are not necessarily struggling to place their students into the federal workforce or other acceptable jobs. But given the small number of CyberCorps graduates produced each year, there are always concerns about what might prevent 100% placement.

2a. The NCWES recognizes how delays in onboarding and processing can deter talent.[41] If CyberCorps recipients are willing and able to enter the federal workforce, this process should not dissuade them from fulfilling their obligations when they could easily turn to the private sector. CyberCorps graduates should be fast-tracked into federal service to more quickly employ and retain the high-caliber cyber talent coming out of the program. The NSCAI also recommends fast-tracking by beginning the security clearance process at least one year prior to graduation.[42] In some cases, this is mitigated if a student's required internship is with a federal agency where some level of clearance may have been granted. In comparison, the CySP program extends employment offers to recipients upon acceptance into the program. This means that recipients are able to start the clearance process while they are finishing their studies. This theoretically reduces wait time and uncertainty, but recipients don't have much say in their final placement.

2b. Retention is a critical component considering the significant investment that CyberCorps makes in its recipients. Based on limited retention data from the NSF, it does appear that a majority of recipients tend not to stay within the federal government past their obligations.[43] For example, only 11 out of 153 survey respondents have been employed by a federal agency for at least ten years. Moreover, out of 175 respondents who are no longer with their hiring organization, 60 individuals stayed only two years.[44] The GAO reaches similar conclusions in its 2022 report, arguing that a lack of consistent data on recipients, including how long they stay in the government after fulfilling their obligation, makes it difficult to assess if the CyberCorps program is achieving its stated goals.[45]

2c. Anecdotally, we learned that some students have reported no real preference in hiring due to their status as a CyberCorps recipient, and others have experienced a lack of awareness about the program from hiring managers. Given the federal investment into these students, they must be prioritized in all hiring decisions. Again, the GAO assessed that some federal agencies do not fully leverage the flexibility of appointing recipients directly into the excepted service and noncompetitively converting them to full-time positions, without going through a formal application process, once they have completed their program postgraduate work service obligation.[46]

2d. The NSF does work to mitigate some of these hiring challenges. Agencies can recruit scholarship recipients directly by registering as an agency official through the scholarship-for-service and the Office of Personnel Management website. There are also two hiring events specifically for the SFS students to give agencies an opportunity to interview and even hire SFS students on the spot. Congressional special hiring authorities allow federal organizations to noncompetitively appoint CyberCorps graduates.[47] Upon fulfillment of their service term, these graduates may be converted noncompetitively to a term, career-conditional, or career appointment. If converted to a term appointment, an agency may later noncompetitively convert such an employee to a career-conditional or career appointment before the term appointment expires.[48]

3. The NSF should streamline the renewal process for successful programs and consider other metrics for program evaluation. PIs expressed frustration with the renewal process despite maintaining programs that meet NSF requirements. One PI has "found it very competitive to get the renewal grant despite having a good placement record and quality of the program." For programs that have a demonstrated history in achieving student placement outcomes and few to no deferrals, PIs would like to see something similar to an automatic renewal. In addition, PIs would like to see accurate costs of living taken into consideration when granting or renewing an award. PIs worry that the number of CyberCorps students they can support will decrease due to rising costs.

Summary

As the demand for cyber talent rises, there are increasing calls for program expansion from both external organizations and individual institutions. In sum, it is important to note that the CyberCorps program's longevity and consistent congressional funding should be considered a testament to its necessity and usefulness. Our recommendations provide some consideration on how to expand or augment the existing CyberCorps program that can function as a stepping stone for a future AI federal scholarship-for-service program.

Implications for an AI Federal Scholarship-for-Service Program

The CHIPS and Science Act of 2022 required a report on the need and feasibility of an AI SFS program, which would potentially run tangential to the existing CyberCorps program. While the AI SFS feasibility study is ongoing, there are factors from the CyberCorps SFS that can inform how to structure an AI SFS.

- **Clearly define the program structure.** Though the legislation authorizes the NSF to establish a federal AI SFS, it is not entirely clear how this potential scholarship program might be structured. If the program is to operate similarly to CyberCorps, then it is imperative that program managers decide upon the program's goals and purpose to avoid duplication. AI as a distinct college major is a relatively new academic pursuit at many institutions, but previous CSET research finds that degrees in engineering and computer science are among the top fields of study for technical AI occupations.[49] These fields of study are obviously not differentiated from CyberCorps fields of study, so there is likely going to be overlap between the two programs.

  It will be important to establish the primary goal of an AI SFS program: placing AI talent directly into the federal workforce or developing a broad domestic AI workforce. This goal will drive the types of scholarships that institutions should pursue and at what academic level. For example, if there is more federal demand for AI talent with master's or doctoral degrees, then the AI SFS program should be structured to support graduate scholars with longer funding durations. Program managers must also consider what metrics might be used to evaluate institutional program successes. Achieving 100% student placement in the federal government, research output, and no deferrals are current examples of how institutional CyberCorps programs are evaluated.

- **Use the NSF AI Research Institutes as a starting point for model institutions and fields of study.** The NSF's AI Research Institutes offer a promising place to germinate a potential AI SFS program because of the institutes' specific focus on AI applications for a variety of fields and their existing relationships with the federal government. There are 23 institutes across the country with the NSF designation, nine have an active CyberCorps program, and 12 are designated as NCAE-C.

- **Minimize the wait times or hiring uncertainties.** Future AI SFS recipients should have the opportunity to begin the onboarding or security clearance process prior

to graduation to reduce the potential wait time or other federal hiring uncertainties, especially when AI talent is in high demand. CySP is able to reduce these uncertainties because CySP recipients are going to a specific U.S. department. Initially, perhaps, it would make sense to assess what federal departments or agencies are in critical need of AI talent and develop the AI SFS pipeline for those specific departments.

Conclusion: Future Considerations for the CyberCorps Program

For two decades, the NSF's CyberCorps scholarship-for-service program has been a direct talent pipeline into the federal workforce and beyond. Acknowledging the success of the program, recent recommendations from the NCWES, the Cyber Solarium Commission 2.0, and the NSCAI have advocated for the CyberCorps program to grow, expand, or change in some way, with the ultimate goal of producing more cyber talent.

The CyberCorps program's stated long-term goals are (1) increasing the number of qualified and diverse cybersecurity candidates for federal positions; (2) improving the national capacity for the education of cybersecurity professionals; (3) hiring, monitoring, and retaining CyberCorps graduates; and (4) strengthening partnerships between institutions and federal, state, local, and tribal governments.[50] It is fair to say that the program continues to meet these goals. However, CyberCorps has seemed to swell beyond these goals as the program tries to satisfy increasing needs and pathways for more cyber talent. This is not necessarily bad, and it is certainly an indication that some form of expansion is needed, but it does perhaps require a revisitation or reassessment of future and immediate federal cyber needs so that grant awarding, renewals, and employment pathways can be clearly defined.

This paper provides three contributions to conversations surrounding program expansion: (1) insight from PIs at participating institutions in the CyberCorps program, (2) recommendations for how the CyberCorps program might expand or improve based on trends from PI insight, and (3) recommendations for how the federal government might improve its uptake of CyberCorps recipients. Additionally, the findings and recommendations presented in this paper will inform how a future AI federal SFS program might be structured and how the NSF AI Research Institutes are a starting point for model institutions and fields of study.

Author

Ali Crawford is a research analyst working on the CyberAI Project at the Center for Security and Emerging Technology, where she focuses on cyber talent, education, and workforce issues.

Acknowledgments

For iterative feedback and support, I am grateful to John Bansemer, Dr. Jenny Jun, Ronnie Kinoshita, Cherry Wu, Maggie Wu, Dr. Mike Ham, Dr. Catherine Aiken, Dr. Clay Shields, and Dr. Matthias Oschinski. I am especially thankful to the principal investigators for your participation. I would also like to thank the folks at the NSF for their insight throughout this project. Finally, I would like to thank CSET's external affairs team and Liz Dana for their polishing final touches on this project and shepherding this paper to publication.

Document Identifier: doi: 10.51593/2023CA001

Endnotes

[1] Office of Personnel Management, Cyber Workforce Dashboard, demographic trends, accessed July 20, 2023, www.opm.gov/data/data-products/cyber-workforce-dashboard/. Actual totals of PhDs in the federal cyber workforce are not publicly shared.

[2] Office of Personnel Management, Cyber Workforce Dashboard, demographic trends. Actual totals of associate's or similar degree holders in the federal cyber workforce are not publicly shared.

[3] Diana Gehlhaus and Luke Koslosky, "Training Tomorrow's AI Workforce" (Center for Security and Emerging Technology, April 2022), https://doi.org/10.51593/20210022.

[4] Office of Personnel Management, "History/Overview," CyberCorps, accessed August 8, 2023, https://sfs.opm.gov/About/History.

[5] CyberCorps and SFS may be used interchangeably throughout this paper as a way to refer to the NSF's CyberCorps program.

[6] Eric Schmidt et al., "Final Report" (National Security Commission on Artificial Intelligence, 2021), 367, www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf; Laura Bate and RADM (Ret.) Mark Montgomery, "Workforce Development Agenda for the National Cyber Director" (Cyberspace Solarium Commission 2.0, June 2022), https://cybersolarium.org/wp-content/uploads/2022/05/CSC2.0_Report_WorkforceDevelopmentAgenda_FullText.pdf.

[7] Office of the National Cyber Director, "National Cyber Workforce and Education Strategy: Unleashing America's Cyber Talent" (White House, July 2023), www.whitehouse.gov/wp-content/uploads/2023/07/NCWES-2023.07.31.pdf.

[8] CyberSeek, "Cybersecurity Supply/Demand Heat Map," accessed August 8, 2023, www.cyberseek.org/heatmap.html.

[9] Government Accountability Office, "Actions Needed to Improve CyberCorps Scholarship for Service Program," GAO Highlights, September 2022, www.gao.gov/assets/gao-22-105187-highlights.pdf; National Science Foundation, "2021 Biennial Report—Scholarships for Service CyberCorps," 2021, www.nsf.gov/ehr/Materials/2021SFSBiennialReport.pdf.

[10] CHIPS and Science Act, H.R. 4346, 117th Cong., Sec. 10313 (2022), www.congress.gov/bill/117th-congress/house-bill/4346.

[11] National Science Foundation, "Program Solicitation," NSF 21-580, accessed April 3, 2023, www.nsf.gov/pubs/2021/nsf21580/nsf21580.htm.

[12] National Science Foundation, "2021 Biennial Report."

[13] National Science Foundation, "2021 Biennial Report."

[14] National Science Foundation for the Future Act, H.R. 2225, 117th Cong., sec. 4 (2021), www.congress.gov/bill/117th-congress/house-bill/2225. FY2022 for $70 million, FY2023 for $72 million, FY2024 for $78 million, FY2025 for $84 million, and FY2026 for $90 million.

[15] Government Accountability Office, "Actions Needed to Improve."

[16] Federal Register, "NSF Federal Cyber Scholarship-for-Service Program (CyberCorps® SFS)," July 15, 2022, 87 FR 42431, www.federalregister.gov/documents/2022/07/15/2022-14328/nsf-federal-cyber-scholarship-for-service-program-cybercorps-sfs.

[17] National Science Foundation, "Program Solicitation," NSF 21-580.

[18] National Science Foundation, "CyberCorps Scholarship-for Service: Program Solicitation," NSF 23-574," accessed August 10, 2023, www.nsf.gov/pubs/2023/nsf23574/nsf23574.pdf.

[19] National Science Foundation, "2021 Biennial Report," 3.

[20] National Science Foundation, "2021 Biennial Report."

[21] National Science Foundation, "2021 Biennial Report," 4.

[22] Luke Koslosky, Ali Crawford, and Sara Abdulla, "Building the Cybersecurity Workforce Pipeline" (Center for Security and Emerging Technology, June 2023), https://doi.org/10.51593/20220005.

[23] National Science Foundation, "CyberCorps Scholarship for Service Active Awards," accessed August 2023, www.nsf.gov/awards/award_visualization.jsp?org=NSF&pims_id=504991&ProgEleCode=1668&from=fund.

[24] National Science Foundation, "2021 Biennial Report," 6.

[25] National Science Foundation, "2021 Biennial Report," 6.

[26] Office of Personnel Management, Cyber Workforce Dashboard, top 10 cyber occupations, accessed July 20, 2023, www.opm.gov/data/data-products/cyber-workforce-dashboard/.

[27] National Science Foundation, "2021 Biennial Report."

[28] National Science Foundation, "2021 Biennial Report."

[29] USA Jobs, "How Many Years of Experience Do I Need to Qualify for a Job?" accessed June 8, 2023, www.usajobs.gov/Help/faq/application/qualifications/experience/.

[30] National Science Foundation, "2021 Biennial Report."

[31] National Science Foundation, “2021 Biennial Report.”

[32] NCyTE Center, “CyberCorps Scholarship for Service Program: The Expanding Role of Community Colleges,” (National Science Foundation, 2022), 28–37, www.ncyte.net/home/showpublisheddocument?id=271.

[33] National Science Foundation, “2021 Biennial Report,” 3.

[34] Bate and Montgomery, “Workforce Development Agenda.”

[35] Office of Personnel Management, Cyber Workforce Dashboard, demographic trends.

[36] Government Accountability Office, “Actions Needed to Improve.”

[37] Bate and Montgomery, “Workforce Development Agenda,” 17.

[38] Koslosky, Crawford, and Abdulla, “Building the Cybersecurity Workforce Pipeline.”

[39] Gehlhaus and Koslosky, “Training Tomorrow’s AI Workforce.”

[40] Bate and Montgomery, “Workforce Development Agenda.”

[41] Office of the National Cyber Director, “National Cyber Workforce and Education Strategy,” 33.

[42] Schmidt et al., “Final Report,” 367.

[43] National Science Foundation, “2021 Biennial Report,” 16.

[44] National Science Foundation, “2021 Biennial Report,” 16.

[45] Government Accountability Office, “Actions Needed to Improve.”

[46] Government Accountability Office, “Actions Needed to Improve.”

[47] Cybersecurity Enhancement Act, P.L. 113–274, 113th Cong., sec. 302(e) (2014).

[48] Federal Register, “NSF Federal Cyber Scholarship-for-Service Program.”

[49] Diana Gehlhaus and Santiago Mutis, “The U.S. AI Workforce: Understanding the Supply of AI Talent” (Center for Security and Emerging Technology, January 2021), https://doi.org/10.51593/20200068.

[50] National Science Foundation, “2021 Biennial Report,” 4–5.