United States Government Accountability Office

Report to Congressional Requesters

September 2022

CYBERSECURITY WORKFORCE

Actions Needed to Improve CyberCorps Scholarship for Service Program

Accessible Version

GAO-22-105187

GAO Highlights

Highlights of GAO-22-105187, a report to congressional requesters

September 2022

CYBERSECURITY WORKFORCE

Actions Needed to Improve CyberCorps Scholarship for Service Program

Why GAO Did This Study

GAO has previously reported that federal agencies faced challenges in ensuring that they have an effective cybersecurity workforce. What is now known as the CyberCorps® Scholarship for Service Program—operated by NSF in conjunction with OPM and the Department of Homeland Security (DHS)—was established in 2000 to increase the supply of new government cybersecurity employees. Since its inception, NSF reports that the program has awarded about $621 million in scholarships to over 4,707 recipients.

GAO was asked to review the Scholarship for Service Program. GAO determined the extent to which (1) NSF and OPM are complying with program legal requirements, and (2) NSF has identified, analyzed, mitigated, and reported on program risks.

GAO assessed program documentation and processes against legal requirements and industry best practices. Further, GAO interviewed NSF, OPM, and DHS officials as well as personnel from selected institutions of higher education participating in the program.

What GAO Recommends

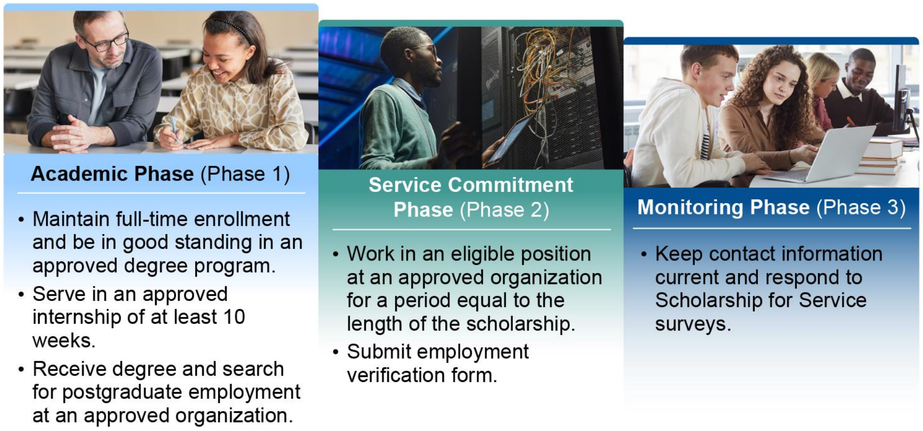
GAO is making three recommendations to NSF and two to OPM to comply with legal requirements and implement a risk management strategy. Both agencies agreed with AO's recommendations.

View GAO-22-105187. For more information, contact David B. Hinchman at (214) 777-5719 or HinchmanD@gao.gov.

What GAO Found

The CyberCorps® Scholarship for Service Program provides participating institutions of higher education with scholarships to students in approved IT and cybersecurity fields of study. As a condition of receiving scholarships, students are required to enter agreements to work in qualifying full-time jobs upon graduation for a period equal in length to their scholarship. See the figure below for how recipients progress through the program.

Scholarship Recipients Progress through Three Phases in the CyberCorps® Program



Academic Phase (Phase 1)
• Maintain full-time enrollment and be in good standing in an approved degree program.
• Serve in an approved internship of at least 10 weeks.
• Receive degree and search for postgraduate employment at an approved organization.
Service Commitment Phase (Phase 2)
• Work in an eligible position at an approved organization for a period equal to the length of the scholarship.
• Submit employment verification form.
Monitoring Phase (Phase 3)
• Keep contact information current and respond to Scholarship for Service surveys.

Source: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program data; images: Seventyfour/stock.adobe.com. | GAO-22-105187

Text of Scholarship Recipients Progress through Three Phases in the CyberCorps® Program

Academic Phase 1

- Maintain full-time enrollment and be in good standing in an approved degree program.
- Serve in an approved internship of at least 10 weeks.
- Receive degree and search for postgraduate employment at an approved organization.

Service Commitment Phase (Phase 2)

- Work in an eligible position at an approved organization for a period equal to the length of the scholarship.
- Submit employment verification form.

Monitoring Phase (Phase 3)

- Keep contact information current and respond to Scholarship for Service surveys.

Source: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program data; images: Seventyfour/stock.adobe.com. | GAO-22-105187

GAO identified 19 selected legal requirements on how National Science Foundation (NSF) and the Office of Personnel Management (OPM) are to manage the program. GAO found that NSF and OPM fully complied with 13 of the requirements and partially complied with six. The partially complied with requirements include the following:

- Scholarship recipients are required to provide OPM with annual verifiable documentation of post-award employment. OPM officials acknowledge that recipients provide verifiable employment documentation and up-to-date contact information only at the beginning and end of the service commitment period, rather than annually as required by law.
- NSF is required to periodically report on program performance, including how long scholarship recipients stay in the positions they enter after graduation. OPM attempts to answer this by surveying recipients. However, recipient response rates ranging from 32 to 50 percent do not yield reliable and complete results.

NSF did not implement a risk management strategy and process to effectively identify, analyze, mitigate, and report on program risks and challenges. Absent such a strategy, NSF is not in a position to mitigate the adverse effects of risk events that do occur, which could negatively impact the accomplishment of program goals.

Contents

Tables

Figures

Abbreviations

CMMI-SVC	Capability Maturity Model® Integration for Services
DHS	Department of Homeland Security
FFRDC	Federally Funded Research and Development Centers
FY	Fiscal Year
IPA	Intergovernmental Personnel Act
NDAA	National Defense Authorization Act
NICE	National Initiative for Cybersecurity Education
NPRM	Notice of Proposed Rulemaking
NSF	National Science Foundation
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PI	Principal Investigator
ROTC	Reserve Officers' Training Corps
SFS	Scholarship for Service

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

441 G St. N.W.
Washington, DC 20548

September 29, 2022

The Honorable Margaret Wood Hassan
Chair
Subcommittee on Emerging Threats and Spending Oversight
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Kirsten Gillibrand
United States Senate

A resilient, well trained, and dedicated cybersecurity workforce is essential to protecting federal IT systems and networks. The ability to secure federal systems depends on the knowledge, skills, and abilities of the federal and contractor workforce that uses, implements, secures, and maintains these systems. We and other organizations have previously reported that federal agencies face challenges in ensuring that they have an effective cybersecurity workforce.[1] Specifically, we have also stated that building and maintaining the federal government's IT and cybersecurity workforce through addressing mission-critical skills gaps is one of federal government's most important challenges.[2]

One method the federal government has established to increase the supply and quality of IT and cybersecurity personnel is through the use of undergraduate and graduate scholarship programs. In 2000, the Executive Office of the President established what is now known as the CyberCorps® Scholarship for Service (SFS) Program to attract and retain technical personnel.[3] The SFS Program—operated by the National

[1] GAO, *Information Technology: Biannual Scorecards Have Evolved and Served As Effective Oversight Tools*, GAO-22-105659 (Washington, D.C.: Jan. 20, 2022); *Federal Management: Selected Reforms Could be Strengthened By Following Additional Planning, Communication, and Leadership Practices*, GAO-20-322 (Washington, D.C.: April 23, 2020); National Academy of Public Administration, *A Call to Action – The Federal Government's Role in Building a Cybersecurity Workforce for the Nation* (Washington D.C.: January 2022); and Cyberspace Solarium Commission, *Workforce Development Agenda for the National Cyber Director* (June 2022).

[2] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[3] The White House, *National Plan for Information Systems Protection* (Washington, D.C.: 2000). SFS was created under the Federal Cyber Service Training and Education Initiative, a component of the *National Plan for Information Systems Protection*.

Science Foundation (NSF) in conjunction with the Office of Personnel Management (OPM) and the Department of Homeland Security (DHS)—was established to increase the supply of new government cybersecurity employees.[4] Specifically, the program provides participating institutions of higher education or universities with scholarships for selected students in approved IT and cybersecurity fields of study.[5] As a condition of receiving the scholarships, students are required to enter into agreements to work in qualifying full-time jobs upon graduation for a period equal in length to their scholarship.

You asked us to review the CyberCorps® Scholarship for Service (SFS) Program. Our specific objectives were to (1) determine what actions, if any, did NSF and OPM take to comply with the SFS requirements, and (2) determine the extent to which NSF has identified, analyzed, mitigated, and reported risks on the SFS Program.

To address the first objective, we reviewed the Cybersecurity Enhancement Act of 2014 and identified legal requirements related to the SFS Program.[6] Of these legal requirements, we identified and selected the 19 requirements of the law that related to how NSF and OPM managed, monitored, and tracked the SFS Program.[7] We classified the SFS Program's legal requirements into three categories: recipient responsibilities, scholarship forfeitures, and administrative responsibilities. We then analyzed NSF and OPM's SFS Program policies, procedures, and related documentation, and compared them to the SFS Program's legal requirements to determine the extent to which the legal requirements were met.

To address the second objective, we analyzed NSF's SFS Program risk documentation such as the SFS Program Solicitation and NSF's data analytics and assurance to determine the extent to which NSF had a risk

[4] The three agencies have different roles. NSF is responsible for the financial management of the program, OPM helps NSF administer the program, and DHS is to promote and help with workforce development for the program.

[5] In this report, we use the terms institutions of higher education and universities interchangeably.

[6] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

[7] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

management process in place for the SFS program.[8] We then compared NSF's SFS Program risk documentation to risk management best practices to determine the extent which NSF identified, analyzed, mitigated, and reported risks on the SFS Program. Because NSF had not identified, analyzed, mitigated, or reported any risks associated with the SFS Program, we undertook an effort to identify them by analyzing documents and by interviewing NSF and OPM officials, as well as program officials from the top five universities receiving awards. We developed a list of risks and challenges identified by NSF, OPM and officials from selected universities during our interviews as well as actions taken to mitigate some of the risks and challenges. We identified 14 program risks and challenges, which we grouped into the five categories below.

1. SFS Program administrative overhead resulting from SFS Program policies and procedures that inherently impose a greater workload on OPM's SFS Program Office, OPM Human Resource Solutions, as well as SFS Principal Investigators (PI);
2. postgraduate work service employment impacted by federal law and other provisions that imposed difficulty for recipients, PIs, and recipient employers;
3. student eligibility impacted by requirements on recipients that are not U.S. citizens;
4. ineffective tracking of scholarship recipients for up to 8 years following the completion of their postgraduate work service obligation; and
5. the COVID-19 pandemic.

For each objective, we supplemented our analyses with interviews with officials in NSF's Program, OPM's Program, and DHS's Program management offices. We also interviewed representatives from the five universities participating in the SFS Program that received the most SFS Program award funding between fiscal years 2016 and 2020.[9] We conducted these interviews to obtain perspectives on the program's legal

[8] The NSF SFS Program Solicitation, contains information on the SFS Program including: proposal preparation and submission instructions for universities; proposal processing and review procedures; award administration information; revision notes, program requirements; and program evaluation.

[9] Universities refer to all institutions of higher education that participate in the CyberCorps® Scholarship for Service Program, including community colleges.

requirements, cost, challenges, and risk mitigation strategies. For more information on our scope and methodology, see appendix I.

We conducted this performance audit from April 2021 to September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

The IT systems and networks supporting the federal government are at increasing risk from cybersecurity threats and attacks. These systems and networks are often interconnected with other internal and external systems and networks, including the internet. With this greater connectivity, threat actors are increasingly willing and capable of conducting cyberattacks on federal agencies' IT systems that could be disruptive and destructive.

In 1997, we designated the security of federal information systems as a government-wide high-risk area and cited the shortage of information security personnel with technical expertise required to manage controls in these systems.[10] In the 2017 update to our high-risk list, we reported that the federal government continued to face challenges in addressing mission critical skills gaps, including cybersecurity skills gaps.[11]

In addition, in September 2018, we reported that effective cybersecurity workforce management was a critical action for addressing cybersecurity challenges facing the nation.[12] That same year, the federal government released an updated National Cyber Strategy designed to strengthen the

[10] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[11] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: February 2017).

[12] GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation,* GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

nation's cybersecurity capabilities and secure it from cyber threats.[13] Specifically, the strategy seeks to promote American prosperity by developing a superior U.S. workforce through the recruitment and retention of highly qualified cybersecurity professionals.

In 2021, we updated our high-risk list again regarding this issue.[14] Specifically, we stated that building and maintaining the federal government's IT and cybersecurity workforce through addressing mission-critical skills gaps is one of federal government's most important challenges.[15]

As previously stated, the SFS Program was established to increase the supply of new government cybersecurity employees. The SFS Program's long-term goals published generally align with the National Cyber Strategy to develop a superior cybersecurity workforce, and include:[16]

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 SFS graduates in federal government employment; and
4. Strengthen partnerships between institutions of higher education and federal, state, local, and tribal governments.

[13] The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

[14] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[15] GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas,* GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[16] The White House, *National Cyber Strategy of the United States of America* (Washington, D.C.: September 2018).

SFS Program Requirements

The SFS Program is governed by a series of legal requirements as established by the Cybersecurity Enhancement Act of 2014,[17] as amended by the fiscal year 2018[18] and the fiscal year 2021 National Defense Authorization Acts.[19] These legal requirements define how NSF and OPM are to manage, monitor, and track the program and what recipients are responsible for while in the SFS Program. Scholarship recipients are required to be enrolled in an academic degree or specialized program in the IT or cybersecurity field and agree to work in an approved government-related position after graduation.[20] See table 1 for a list of the 19 selected legal requirements that relate to how NSF and OPM manage, monitor, and track the SFS Program. Each requirement is categorized in the following table as being related to oversight of recipient responsibilities, oversight of scholarship forfeitures, or administrative responsibilities.

[17] Pub. L. No. 113-274, § 302, 128 Stat. 2971, 2982 (2014), codified as amended at 15 U.S.C. § 7442.

[18] National Defense Authorization Act (NDAA) for Fiscal Year 2018, Pub. L. No. 115-91, div. A, title XVI, subtitle C, part II, § 1649B, 131 Stat. 1283, 1754-55 (2017).

[19] William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021, Pub. L. No. 116-283, div. H, title XCIV, subtitle A, §§ 9403-9404,, 134 Stat. 3388, 4810-12 (2021)

[20] After graduation, scholarship recipients are authorized to work in the cybersecurity mission of an executive agency, a legislative or interstate agency, a state, local, or tribal government, or a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure, and as educators in the field of cybersecurity at qualified universities that provide SFS scholarships.

Table 1: The 19 Selected Legal Requirements That Relate to How the NSF and the OPM Manage, Monitor, and Track the CyberCorps® Scholarship for Service Program

Category	Selected 19 Legal Requirements
Oversight of Recipient Responsibilities	• The recipient must be a citizen or lawful permanent resident of the United States. • The recipient must demonstrate a commitment to a career in improving the security of information technology. • The recipient must have demonstrated a high level of competency in relevant knowledge, skills, and abilities, as defined by the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.[a] • The recipient must be a full-time student in an eligible degree program at a qualified institution of higher education, or be a student in a community college pursuing a degree on a less than full-time basis, but not less than half-time basis. • The recipient must agree to work for a period equal to the length of the scholarship, following receipt of their degree, in the cybersecurity mission of: an executive agency; Congress, including any agency, entity, office, or commission established in the legislative branch; an interstate agency; a state, local, or tribal government; a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure; and a qualified institution of higher education. • The recipient must agree to provide OPM and their qualified universities with annual verifiable documentation of post-award employment and up-to-date contact information.
Oversight of Forfeiture of Scholarship	• The recipient shall be liable to repay the scholarship if they fail to maintain an acceptable level of academic standing at the applicable institution of higher education. • The recipient shall be liable to repay the scholarship if they are dismissed from the applicable institution of higher education for disciplinary reasons. • The recipient shall be liable to repay the scholarship if they withdraw from the eligible degree program before its completion. • The recipient shall be liable to repay the scholarship if they declare that they do not intend to fulfill the post-award employment obligation under this section. • The recipient shall be liable to repay the scholarship if they fail to maintain or fulfill any of the post-graduation or post-award obligations or requirements.

Category	Selected 19 Legal Requirements
Administrative Responsibilities	• The Director of NSF, in coordination with the Director of OPM, shall continue a federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments. • The SFS Program shall provide scholarships through qualified universities, including community colleges, to students who are enrolled in programs of study at universities leading to degrees or specialized program certifications in the cybersecurity field. • The SFS Program shall provide scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the federal information technology and cybersecurity workforce. • The SFS Program shall prioritize the placement of scholarship recipients fulfilling the post-award employment obligation to ensure that not less than 70 percent are placed in an executive agency, and not more than 20 percent are placed in a legislative or interstate agency, a state, local, or tribal government, or a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure, and not more than 10 percent are placed as educators in the field of cybersecurity at qualified universities that provide SFS scholarships. • As a condition of participating in the program, a qualified university shall enter into an agreement with the Director NSF, to monitor the compliance of scholarship recipients with respect to their post-award employment obligations. • The Director of NSF, in coordination with the Director of OPM, shall periodically evaluate and make public information on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector cybersecurity workforce, including information on: (A) placement rates; (B) where students are placed, including job titles and descriptions; (C) salary ranges for students not released from obligations under this section; (D) how long after graduation students are placed; (E) how long students stay in the positions they enter upon graduation; (F) how many students are released from obligations; and (G) what, if any, remedial training is required. • The Director of NSF, in coordination with OPM, shall submit to congressional committees, not less frequently than once every 2 years, a report, including: (A) the results of the evaluation described above; (B) the disparity in any reporting between scholarship recipients and their respective universities; and (C) any recent statistics regarding the size, composition, and educational requirements of the federal cyber workforce. • The Director of NSF, in coordination with the Director of OPM, shall provide consolidated and user-friendly online resources for prospective scholarship recipients, including, to the extent practicable searchable, up-to-date, and accurate information about participating institutions of higher education and job opportunities related to the field of cybersecurity; and a modernized description of cybersecurity careers.

Legend: NSF = National Science Foundation; OPM = Office of Personnel Management; SFS = Scholarship for Service

Source: GAO analysis of CyberCorps® Scholarship for Service Program documentation and guidance. | GAO-22-105187

[a]The National Initiative for Cybersecurity Education (NICE) Workforce Cybersecurity Framework is the foundation for increasing the size and capability of the U.S. cybersecurity workforce. NICE is a component of the National Institute of Standards and Technology. The purpose of the framework is to provide a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks. National Institute of Standards and Technology, Workforce Framework for Cybersecurity (NICE Framework), Special Publication 800-181 revision 1 (Gaithersburg, MD: November 2020).

Federal Agencies and Universities Participate in the SFS Program

The SFS Program established a process to manage, monitor, and track scholarships that involves both federal agencies and universities. The process begins when NSF publishes the annual program solicitation. Interested universities respond by submitting their program solicitation proposals to NSF. As part of a university's solicitation proposal, they identify a university employee called a Principal Investigator (PI) to manage the program. NSF is to use a merit review process to evaluate and select universities to receive the SFS Program awards.

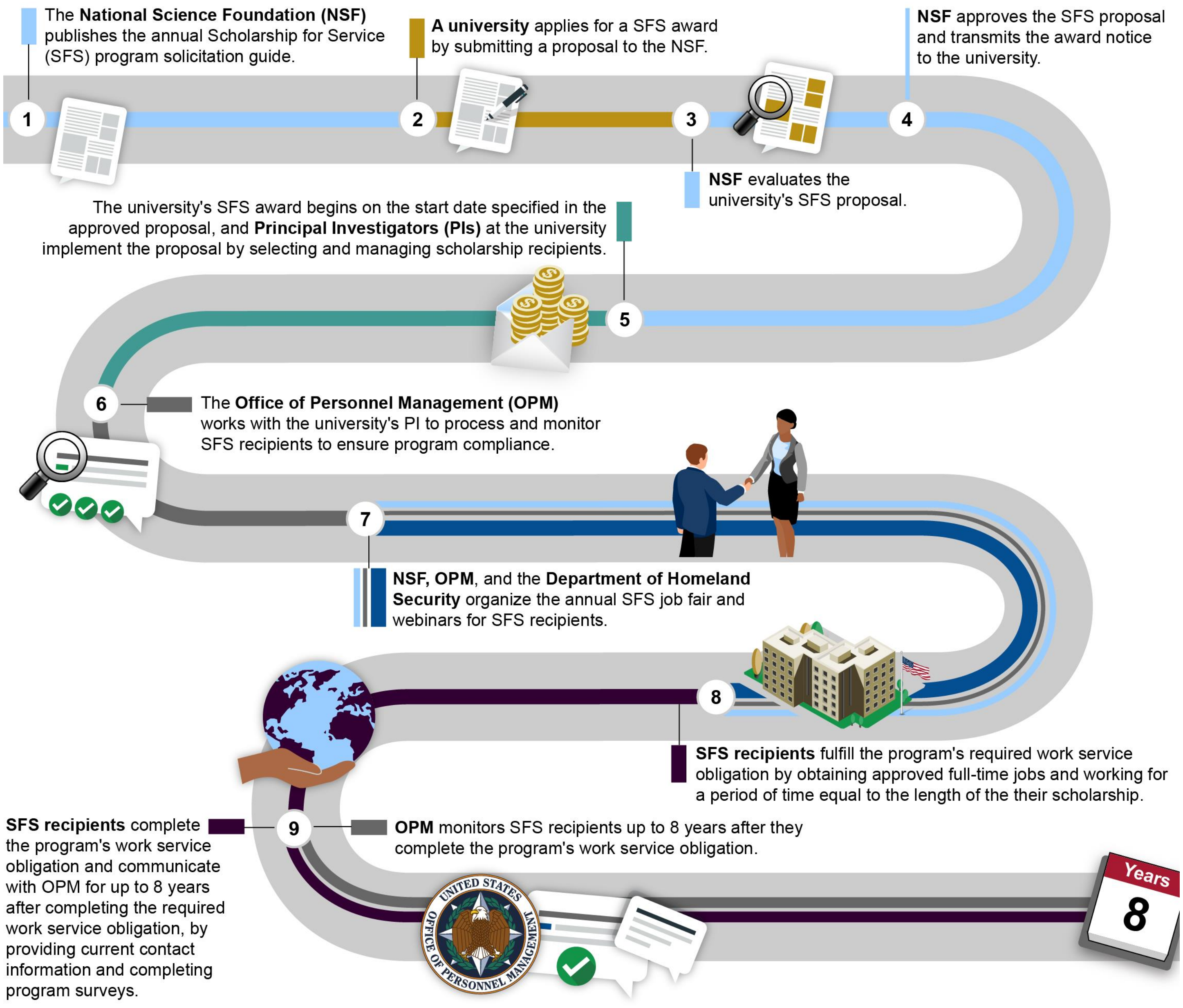
Once a university is selected for a program award, it assumes responsibility to execute the award as described in the solicitation proposal. The process continues with the university PI designing, developing, and establishing the program based on their funded proposal. Key PI program responsibilities are to:

- Serve as the SFS Program administrator of the award.
- Serve as the primary point of contact between the university, NSF, and OPM.
- Identify, evaluate, and select students to become scholarship recipients.
- Design, develop, and implement the SFS Program to enrich scholarship recipients' education and skills.
- Guide the scholarship recipients throughout the SFS lifecycle, including academics, internship, and postgraduate work service requirements.

OPM is to work with the university PI to process and monitor the recipients, and to ensure program compliance with the program's rules and regulations. The scholarship supports up to three years of stipends, tuition, and allowances for students in the general area of cybersecurity. Specifically, the scholarships provide annual stipends for living expenses of $25,000 per year for undergraduate students and $34,000 per year for graduate students. In addition, SFS scholarships cover expenses normally incurred by full-time students, including tuition and education related fees. A professional allowance of $6,000 per academic year is provided for the SFS job fair and other expenses such as, among other things, travel, conferences, research materials and supplies, a laptop, books, professional training, and certifications.

Recipients complete program requirements by obtaining full-time jobs in qualifying positions for a period equal in length to their scholarship, not to exceed three years. Finally, the OPM SFS Program office is to monitor and track the recipients for up to 8 years after they complete their required work service obligation through surveys intended to determine long-term retention of the recipients as government employees. Figure 1 provides an overview of the SFS Program and the process to be followed in administering it.

Figure 1: The CyberCorps® Scholarship for Service (SFS) Program Process



1 The **National Science Foundation (NSF)** publishes the annual Scholarship for Service (SFS) program solicitation guide.

2 **A university** applies for a SFS award by submitting a proposal to the NSF.

3 **NSF** evaluates the university's SFS proposal.

4 **NSF** approves the SFS proposal and transmits the award notice to the university.

5 The university's SFS award begins on the start date specified in the approved proposal, and **Principal Investigators (PIs)** at the university implement the proposal by selecting and managing scholarship recipients.

6 The **Office of Personnel Management (OPM)** works with the university's PI to process and monitor SFS recipients to ensure program compliance.

7 **NSF, OPM**, and the **Department of Homeland Security** organize the annual SFS job fair and webinars for SFS recipients.

8 **SFS recipients** fulfill the program's required work service obligation by obtaining approved full-time jobs and working for a period of time equal to the length of the their scholarship.

9 **SFS recipients** complete the program's work service obligation and communicate with OPM for up to 8 years after completing the required work service obligation, by providing current contact information and completing program surveys.

OPM monitors SFS recipients up to 8 years after they complete the program's work service obligation.

Source: GAO analysis of NSF and OPM CyberCorps® Scholarship for Service program documentation; images: toonsteb/stock.adobe.com, Logvin art/stock.adobe.com. | GAO-22-105187

Text of Figure 1: The CyberCorps® Scholarship for Service (SFS) Program Process

1. The National Science Foundation (NSF) publishes the annual Scholarship for Service (SFS) program solicitation guide.
2. A university applies for a SFS award by submitting a proposal to the NSF.
3. NSF evaluates the university's SFS proposal.
4. NSF approves the SFS proposal and transmits the award notice to the university.
5. The university's SFS award begins on the start date specified in the approved proposal, and Principal Investigators (PIs) at the university implement the proposal by selecting and managing scholarship recipients.
6. The Office of Personnel Management (OPM) works with the university's PI to process and monitor SFS recipients to ensure program compliance.
7. NSF, OPM, and the Department of Homeland Security organize the annual SFS job fair and webinars for SFS recipients.
8. SFS recipients fulfill the program's required work service obligation by obtaining approved full-time jobs and working for a period of time equal to the length of the their scholarship.
9. SFS recipients complete the program's work service obligation and communicate with OPM for up to 8 years after completing the required work service obligation, by providing current contact information and completing program surveys.
   OPM monitors SFS recipients up to 8 years after they complete the program's work service obligation.

Source: GAO analysis of NSF and OPM CyberCorps® Scholarship for Service program documentation; images: toonsteb/stock.adobe.com, Logvin art/stock.adobe.com. |

Scholarship Recipients Proceed through Three Phases

SFS scholarship recipients proceed through three phases: an academic phase, the service commitment phase, and the monitoring phase. During the academic phase, recipients must remain enrolled at a participating university on a full-time basis and must maintain good academic standing in an approved program of study.[21]

The service commitment phase begins when a recipient graduates from their approved program of study. Recipients have 18 months to secure a qualifying position of employment. The OPM SFS Program Office may grant an extension to the 18-month requirement to secure employment in a qualifying position. If a recipient has not secured a qualifying position within 18 months of graduation, or by the end of the granted extension, the recipient will be indebted to the federal government for their scholarship and may be required to reimburse the program.

There are further constraints on the types of employment a scholarship recipient must obtain. For example, as amended through 2021, the Cybersecurity Enhancement Act of 2014 requires that scholarship recipients be placed in one of the following types of entities, subject to the indicated minimum and maximum placement percentages[22]:

- An executive agency (at least 70 percent of recipients must be placed in such entities);[23]
- Congress, including any agency, entity, office, or commission established in the legislative branch; an interstate agency; a state, local, or tribal government; or a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure (at most 20 percent of recipients may be placed in all such entities combined); and
- Qualifying institutions of higher education that participate in the SFS Program, with recipients serving as educators in the field of cybersecurity (at most 10 percent of recipients may be placed in such entities).
- As another example, the Cybersecurity Enhancement Act requires scholarship recipients to agree to work "in the cybersecurity mission" of the same types of entities.[24] Additional provisions of the statute

[21] An exception to this is a student who is enrolled in a community college may be a student pursuing a degree on a less than full-time basis, but not less than half-time basis.

[22] 15 U.S.C. § 7442(b).

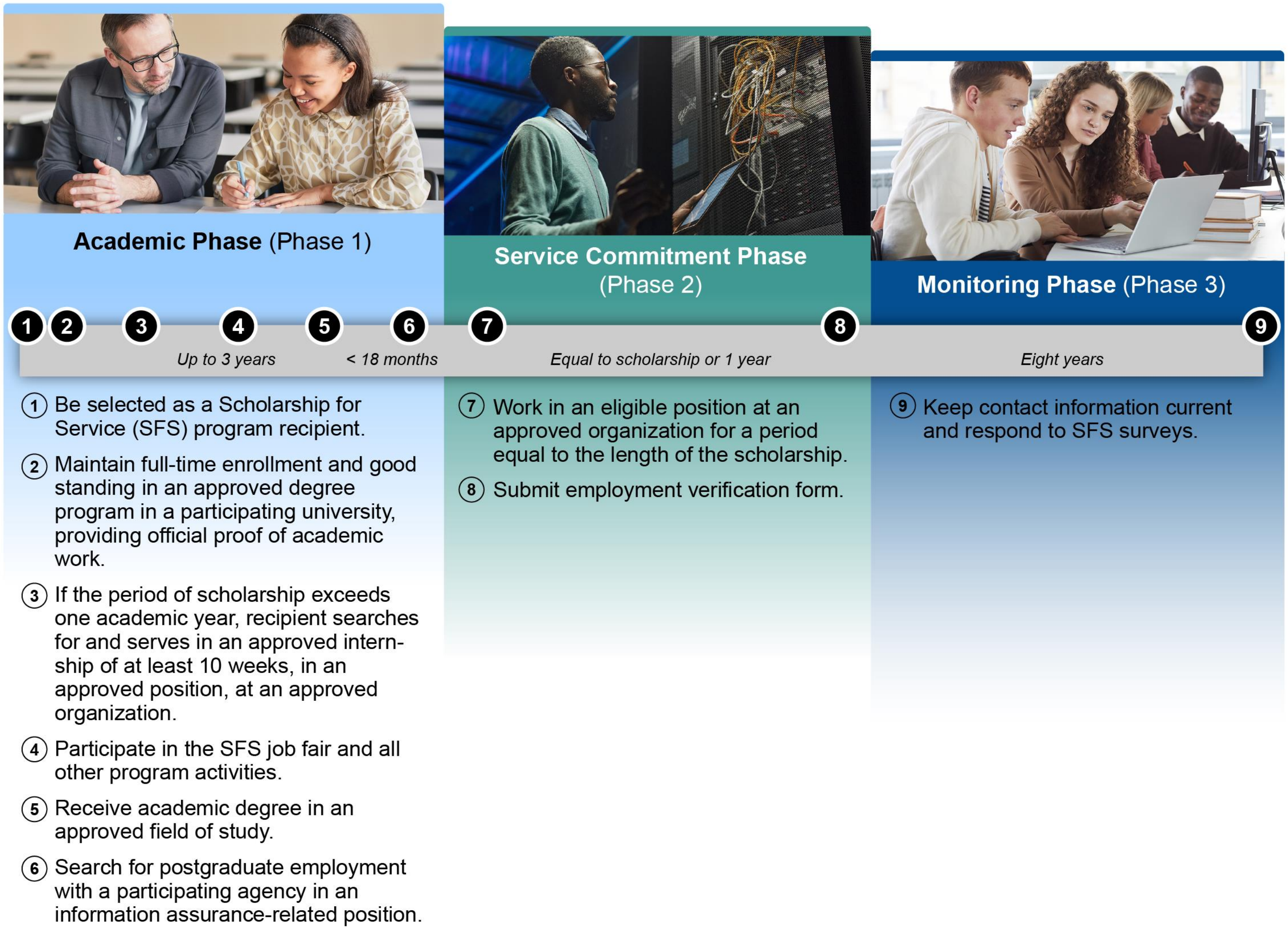
[23] 5 U.S.C. § 105 defines an executive agency as an executive department, a government corporation, and an independent establishment.

[24] 15 U.S.C. § 7442(d).

may also be relevant to the types of employment a recipient must obtain.

The program's third phase, the monitoring phase, is focused on retention of scholarship recipients as government employees. During this phase, OPM's SFS Program Office monitors the recipient's employment status for up to 8 years after their required work service commitment ends. An overview of the program's three phases is shown in figure 2.

Figure 2: Scholarship Recipients Progress through Three Phases in the CyberCorps® Scholarship for Service (SFS) Program



Academic Phase (Phase 1)

1. Be selected as a Scholarship for Service (SFS) program recipient.
2. Maintain full-time enrollment and good standing in an approved degree program in a participating university, providing official proof of academic work.
3. If the period of scholarship exceeds one academic year, recipient searches for and serves in an approved internship of at least 10 weeks, in an approved position, at an approved organization.
4. Participate in the SFS job fair and all other program activities.
5. Receive academic degree in an approved field of study.
6. Search for postgraduate employment with a participating agency in an information assurance-related position.

Service Commitment Phase (Phase 2)

7. Work in an eligible position at an approved organization for a period equal to the length of the scholarship.
8. Submit employment verification form.

Monitoring Phase (Phase 3)

9. Keep contact information current and respond to SFS surveys.

Source: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program data; images: Seventyfour/stock.adobe.com. | GAO-22-105187

Text of Figure 2: Scholarship Recipients Progress through Three Phases in the CyberCorps® Scholarship for Service (SFS) Program

Academic Phase (Phase 1)

1. Be selected as a Scholarship for Service (SFS) program recipient.
2. Maintain full-time enrollment and good standing in an approved degree program in a participating university, providing official proof of academic work.
3. If the period of scholarship exceeds one academic year, recipient searches for and serves in an approved internship of at least 10 weeks, in an approved position, at an approved organization.
4. Participate in the SFS job fair and all other program activities.
5. Receive academic degree in an approved field of study.
6. Search for postgraduate employment with a participating agency in an information assurance-related position.

Service Commitment Phase (Phase 2)

7. Work in an eligible position at an approved organization for a period equal to the length of the scholarship.
8. Submit employment verification form.

Monitoring Phase (Phase 3)

9. Keep contact information current and respond to SFS surveys.

Source: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program data; images: Seventyfour/stock.adobe.com. | GAO-22-105187

SFS Program Costs over the Past 5 Fiscal Years

From fiscal year 2016 through fiscal year 2021, NSF reported receiving a total of about $330 million in congressional appropriations for the program (on average, about $55 million annually).[25] NSF reported spending the majority of the appropriations on awards to universities participating in the program, totaling about $320 million (on average, about $53 million

[25] Expenditure figures are in nominal terms.

annually).[26] These awards to universities included recipient costs such as scholarships for tuition and stipends for living expenses. NSF reported spending about $1.92 million on personnel expenditures for the program salaries, including those for two rotating Intergovernmental Personnel Act (IPA) assignees.[27] NSF officials reported they spent the remaining amount, about $7.14 million on program non-personnel administrative expenditures.[28] The breakdown of the program costs from fiscal years 2016 through 2021 are shown in table 2.

[26] Direct costs do not include the opportunity cost associated with the SFS Program, such as the cost of resources used, measured by the return to those resources in their most productive application elsewhere.

[27] NSF's Intergovernmental Personnel Act (IPA) program provides assignments to or from federal agencies and the following: state and local governments; private and public colleges and universities; Indian tribal governments; federally funded research and development centers; and qualified non-profit organizations involved in public management. IPA assignees are usually detailed to NSF and remain on their home institution's payroll (for both salary and benefits) in an active pay status while assigned to NSF. IPA assignees are not federal employees, but are subject to provisions of law governing the ethics and conduct of federal employees.

[28] NSF's SFS Program fiscal year 2021 final data are not reported publicly until the release of NSF's SFS Program fiscal year 2023 congressional request.

Table 2: National Science Foundation's CyberCorps® Scholarship for Service (SFS) Program Expenditures, Fiscal Year 2016 through Fiscal Year 2021

SFS Program expenditures	Expenditure description	Total amount (dollars in millions)
Program expenditures	Expenditures of awards directly to universities participating in the SFS Program	**$319.75**
Personnel expenditures	Expenditures such as salaries for Intragovernmental Personnel Assignment assignees	**$1.92**

Non-personnel expenditures	Expenditure description	Total amount (dollars in millions)
Review Process	Expenditures associated with reviews of university proposals	**$0.44**
Quality Monitoring System[a]	Expenditures for IT system used to manage program data	**$0.20**
Office of Personnel Management (OPM) SFS Program office operations	Expenditures for contract costs paid to OPM to manage and administer the SFS Program	**$5.60**
Job fair contribution[b]	Expenditures for SFS Program job fair	**$0.83**
Travel and outreach	SFS Program travel and outreach	**$0.07**
Total expenditures	Includes total program, non-personnel, and personnel expenditures	**$328.81**

Source: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program budget and cost data. | GAO-22-105187

[a] NSF reported that additional funds were provided in fiscal years 2018 and 2019 by the NSF evaluation/monitoring program. These additional funds totaled $412,128 in fiscal year 2018 and $1,499,000 in fiscal year 2019.

[b] The Department of Homeland Security (DHS) reported that, per the memorandum of agreement between DHS and NSF, DHS and the Cybersecurity and Infrastructure Security Agency (an operational component under DHS oversight) provided $1.93 million of funding to NSF in fiscal year 2016 through fiscal year 2021 to support the SFS Program and related job fairs.

In addition, SFS scholarship funds were distributed to universities in a large number of U.S. states. See appendix II for SFS scholarships distributed between fiscal years 2016 through 2021.

The SFS Program Has Awarded Thousands of Scholarships Since 2001

In January 2022, NSF reported that since the first cohort of 31 students in 2001, the SFS Program has provided about $621 million SFS Program awards to universities participating in the program. NSF reported that of the total 4,707 scholarship awarded to recipients, 3,430 recipients (or 73 percent) had completed the academic phase, entered the service commitment phase, and placed in an approved position to begin postgraduate work.

Scholarship Recipients Worked for a Variety of Employers

Of the 3,426 recipients from the beginning of the program in 2001 to October 2021, NSF reported that these recipients entered the following organizations:

- 2,191 (64 percent) were placed in federal executive government agencies;
- 810 (24 percent) were placed in a federally funded research and development center (FFRDC) or national laboratory;
- 286 (8 percent) were placed in federal legislative branch government agencies or state, local, or tribal governments; and
- 139 (4 percent) were placed in organizations that are not identified as falling in the categories above.

Table 3 displays the top 10 employers of recipients as reported by NSF from the inception of the program through October 2021.

Table 3: NSF Reported Top 10 Employers of CyberCorps® Scholarship for Service (SFS) Recipients from 2001 Program Inception through October 2021

National Security Agency	678
Department of Navy	345
MITRE Corporation (i.e., a federally funded research and development center)[a]	285
State/local/tribal government	235
Department of the Army	189
Sandia National Laboratories	153
Department of Homeland Security	148
Department of Air Force	116
Department of Defense	115
University Affiliated Research Center/John Hopkins University - Applied Physics Laboratory	98

Legend: NSF = National Science Foundation

Source: National Science Foundation CyberCorps® SFS Program documentation. | GAO-22-105187

[a] MITRE Corporation is not the only federally funded research and development center (FFRDC) employer of scholarship recipients; however, it has hired the most scholarship recipients.

OPM is Working to Expand the Diversity of Scholarship Recipients

Since 2015, OPM has requested voluntary gender, ethnicity, and race data from every student entering the SFS Program. See table 4 for a summary of program diversity data as reported by OPM.

Table 4: CyberCorps® Scholarship for Service (SFS) Program Diversity from 2015 through July 2021

Gender of scholarship recipients	
Male	72 percent
Female	26 percent
Did not disclose gender	2 percent
Ethnicity of scholarship recipients	
Not Hispanic or Latino	85 percent
Hispanic or Latino	10 percent
Did not disclose ethnicity	5 percent

Race of scholarship recipients[a]	
White	71 percent
Black or African American	11 percent
Asian	11 percent
American Indian or Alaskan Native	1 percent
Native Hawaiian or Pacific Islander	>1 percent
Did not disclose race	6 percent

Source: National Science Foundation CyberCorps® SFS documentation. | GAO-22-105187

[a] Percentages might not exactly total 100 percent due to rounding.

Additionally, according to OPM officials, they collected data on recipient disability through surveys. The statistics based on an aggregate of OPM's 2016-2020 survey results indicate that disability was reported by 3.5 percent of scholarship recipients.[29]

In an effort to increase the diversity of the cybersecurity workforce, NSF officials reported that starting in 2015, the program began investing in two cybersecurity initiatives involving kindergarten-through-12th-grade schools:

- The GenCyber program provides summer cybersecurity camp experiences for students and teachers at the kindergarten-through-

[29] According to NSF officials, OPM survey results indicating disability may not be confined to physical disability.

12th-grade level. In 2019, there were 123 GenCyber camps; 89 were student camps and 34 were teacher camps. These camps were held in 38 different states, and Puerto Rico and were developed and delivered by 73 educational institutions. The attendance was 3,035 students and 778 teachers, for a total enrollment of 3,813 individuals. In 2019, GenCyber camps had 52.5 percent female participants, and 51.9 percent non-white participants.

- Air Force Junior Reserve Officers' Training Corps (ROTC) Cyber Academies are modeled after the Air Force Flight Academy. The demographics of the Junior ROTC population includes: 500,000 Junior ROTC cadets attending 3,400 high schools (with more than 50 percent being Title I schools), with 55 percent of participating students identified as minorities, and 40 percent identified as female.

NSF and OPM Have Complied with Most SFS Requirements but Need to Address Employment Retention

Of 19 selected and identified SFS Program legal requirements, NSF and OPM fully complied with 13 requirements and partially complied with 6. See table 5 for the 19 selected program legal requirements and an assessment of whether NSF and OPM complied with these requirements.

Table 5: Assessment of NSF and OPM Compliance with 19 Selected Legal Requirements for the CyberCorps® Scholarship for Service (SFS) Program

	SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
Oversight of Recipient Requirements	The recipient must be a citizen or lawful permanent resident of the United States.	Fully Complied	The NSF SFS Program Solicitation[a] states that an eligible recipient must be a citizen or lawful permanent resident of the United States. OPM officials and Principal Investigators (PIs) at universities participating in the program stated that PIs request proof of U.S. citizenship or lawful permanent resident status from prospective scholarship recipients before they are accepted into the program. Once a prospective scholarship recipient is accepted into the program, the PI communicates the recipient's citizenship or lawful permanent resident status to the OPM SFS Program Office. OPM records this information in the recipient's profile in the Master Roster system's 'Citizen/Permanent Resident' data field.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The recipient must demonstrate a commitment to a career in improving the security of information technology.	Fully Complied	NSF's SFS Program Solicitation states that an eligible recipient must demonstrate a commitment to a career in cybersecurity. OPM officials and PIs at universities participating in the program stated that PIs confirm the academic major of prospective recipients before they are accepted into the program, thus ensuring their commitment to a career in improving IT security. Once a prospective recipient is accepted into the program, the PI communicates the recipient's academic major to OPM's SFS Program Office. OPM records this information in the recipient's profile in the Master Roster system's 'Major' data field.
The recipient must have demonstrated a high level of competency in relevant knowledge, skills, and abilities, as defined by the National Initiative for Cybersecurity Education (NICE) Workforce Cybersecurity Framework.	Fully Complied	NSF's SFS Program Solicitation states that an eligible scholarship recipient must have demonstrated a high level of competency in relevant knowledge, skills, and abilities, as defined by the NICE Cybersecurity Workforce Framework. OPM officials and PIs at universities participating in the program stated that PIs evaluate prospective scholarship recipients for their ability to demonstrate a high degree of competency in relevant knowledge, skills, and abilities, as defined by the NICE Cybersecurity Framework before they are accepted into the program. Once a prospective scholarship recipient is accepted into the program, the PI communicates the results of the scholarship recipient's evaluation to OPM's SFS Program Office.
The recipient must be a full-time student in an eligible degree program at a qualified institution of higher education, or be a student in a community college pursuing a degree on a less than full-time basis, but not less than half-time basis.	Fully Complied	NSF's SFS Program Solicitation states that an eligible recipient must be a full-time student in a formal academic program that is focused on cybersecurity at a university participating in the program. OPM officials stated that they ensured that recipients are full-time students through verification with the university PIs and by reviewing scholarship recipient transcripts and relevant information in the SFS System.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The recipient must enter into an agreement to work for a period equal to the length of the scholarship, following receipt of their degree, in the cybersecurity mission of: an executive agency; Congress, including any agency, entity, office, or commission established in the legislative branch; an interstate agency; a state, local, or tribal government; a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure; or a qualified institution of higher education.	Partially Complied	OPM requires each recipient to sign an SFS Student Agreement that requires the recipient to agree to work full-time in a qualifying position at an approved organization for a period commensurate with the length of the scholarship or one year, whichever is longer, following the completion of the recipient's academic degree requirements. To address the ability of recipients to work at a qualified institution of higher education, in September 2021, OPM provided a memorandum to PIs informing them of a 2021 change in the SFS Program statute adding qualified institutions of higher education as authorized employers for recipients. OPM officials stated that they verified that recipients are working in a full-time qualifying position at an approved organization through communication with the PIs from the institutions of higher education and by reviewing employment documentation provided by recipients and relevant information in the SFS System. In addition, NSF's SFS Program Solicitation states that up to 20 percent of scholarship recipients may be placed at entities including National Laboratories or Federally Funded Research and Development Centers (FFRDCs). As amended through 2021, the SFS Program statute addresses requirements relating to scholarship employment placements and scholarship recipients. GAO is currently evaluating these requirements to assess whether they authorize scholarship recipients to work in cybersecurity positions at FFRDCs. GAO will be addressing these matters separately.

	SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
	The recipient must agree to provide OPM and their qualified institutions of higher education with annual verifiable documentation of post-award employment and up-to-date contact information	Partially Complied	OPM's SFS Program Office requires recipients to complete (1) an online form when they first begin postgraduate employment and (2) submit a verification form at the completion of their required postgraduate work service obligation. However, the Office does not verify employment and ensure current recipient contact information on an annual basis. Specifically, OPM officials stated that recipients provide verifiable employment documentation and up-to-date contact information only at the beginning and end of the service commitment period rather than annually as required by law. However OPM reported that NSF, in consultation with the Department of Education (Education) developed a Notice of Proposed Rulemaking (NPRM) that it asserts would address this deficiency. The proposed rule requires recipients to provide documentation within 30 days of the beginning of the service and upon completion of each year of work service obligation. In July 2022, NSF reported that this NPRM was submitted to the Federal Register on June 30, 2022, was published on July 15, 2022, and all comments are due by September 2022. However the final rule has not yet been promulgated by NSF.[b] While OPM asserts that this rule would address the deficiency in obtaining annual information from scholarship recipients, neither OPM nor NSF have provided a time frame for developing a process related to this issue. Specifically, a process does not exist that ensures scholarship recipients provide OPM and their institutions of higher education with verifiable documentation of post-graduation employment and up-to-date contact information on at least an annual basis. Until OPM and NSF verifies employment and ensures current recipient contact information on an annual basis, they will be unable to verify that recipients are meeting the SFS Program legal requirements.
Oversight of Scholarship Forfeiture	The recipient shall be liable to repay the scholarship if they fail to maintain an acceptable level of academic standing at the applicable institution of higher education.	Fully Complied	OPM's SFS Student Agreement that is signed by each scholarship recipient requires recipients to agree to maintain good academic standing, as defined by their university, in an approved program of study. OPM officials stated that they verified recipients' academic standing through communication with the university PIs and identified recipients as liable to repay the scholarship if they failed to maintain an acceptable level of academic standing.
	The recipient shall be liable to repay the scholarship if they are dismissed from the applicable institution of higher education for disciplinary reasons.	Fully Complied	OPM's SFS Student Agreement that is signed by each recipient requires recipients to agree to maintain enrollment at a participating university participating on a full-time basis. OPM officials stated that they verified recipients' enrollment status through communication with the university PIs and identified recipients as liable to repay the scholarship if they are dismissed from the universities for disciplinary reasons.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The recipient shall be liable to repay the scholarship if they withdraw from the eligible degree program before its completion.	Fully Complied	OPM's SFS Student Agreement that is signed by each recipient requires participants to agree to maintain enrollment at a participating university in an approved program of study. OPM officials stated that they verified that recipients were liable to repay the scholarship if they withdrew from the eligible degree program by verifying the information with the PIs. OPM officials stated that they verified recipients' status in an approved program of study through communication with the university PIs and identified recipients as liable to repay the scholarship if they withdraw from the eligible degree program before its completion.
The recipient shall be liable to repay the scholarship if they declare that they do not intend to fulfill the post-award employment obligation under this section.	Fully Complied	OPM's SFS Student Agreement that is signed by each recipient requires recipients to agree to work full-time in a qualifying position at a participating agency for a period commensurate with the length of the scholarship or one year, whichever is longer. OPM officials stated that they verified that recipients were liable to repay the scholarship if they declared that they did not intend to fulfil the post-award employment obligation by verifying the information with the PIs. OPM officials stated that they verified recipients' intention to fulfill the post-award employment obligation through communication with the university PIs and identified recipients as liable to repay the scholarship if their intentions change.
The recipient shall be liable as specified by law to repay the scholarship if they fail to maintain or fulfill any of the post-graduation or post-award obligations or requirements.	Partially Complied	OPM's SFS Student Agreement that is signed by each recipient states that a recipient who fails to comply with any program requirement established under the service agreement will be indebted to the federal government and must immediately reimburse the program. OPM's SFS Program Office requires recipients to complete (1) an online form when they first begin postgraduate employment and (2) submit a verification form at the completion of their required postgraduate work service obligation. However, the Office does not verify employment and ensure current recipient contact information on an annual basis. Specifically, OPM officials stated that recipients provide verifiable employment documentation only at the beginning and end of the service commitment period. Moreover, the Student Agreement requires program participants to complete periodic surveys as requested by the SFS Program Office (usually annually), from the recipients' initial entrance into the program through their completion of the work service obligation period.[c] According to OPM officials, recipient response rates varied from 32 percent to 50 percent between 2014 and 2019. Despite these low response rates, in August 2021, OPM officials stated that they do not take any action if a student fails to respond to these surveys, and that it was not clear what actions would be appropriate to address survey non-respondents. Until NSF and OPM can ensure the collection of complete and consistent data that relate to the fulfillment of all post-award obligations or requirements, NSF and OPM will not be able to effectively know if recipients are maintaining and fulfilling post-award obligations or requirements.

	SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
Administrative Responsibilities	The Director of NSF, in coordination with the Director of OPM, shall continue a federal cyber scholarship-for-service program to recruit and train the next generation of information technology professionals, industrial control system security professionals, and security managers to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments.	Fully Complied	NSF's SFS Program Solicitation states that the goals of the program are: (1) to increase the quantity of new entrants to the government cyber workforce; (2) to increase the national capacity for the education of cybersecurity professionals; (3) to increase national research and development capabilities in critical information infrastructure protection; and (4) to strengthen partnerships between institutions of higher education and relevant employment sectors.
	The SFS Program shall provide scholarships through qualified universities, including community colleges, to students who are enrolled in programs of study at universities leading to degrees or specialized program certifications in the cybersecurity field.	Fully Complied	NSF's SFS Program Solicitation states that the program proposals may only be submitted by universities and sub-awardee community colleges partnering with four-year institutions participating in the program. Additionally, a proposing university must provide clearly documented evidence of a strong existing program in cybersecurity. The SFS Program Solicitation also states that to be eligible for consideration for a scholarship, a student must be a full-time student in a formal program that is focused on cybersecurity at an awardee institution (a) with sophomore standing in an associate's degree program; or (b) with junior or senior standing in a bachelor's degree program; or (c) enrolled in a master's degree program; or (d) enrolled in a research-based doctoral program. OPM officials stated that they verified recipients were enrolled in programs of study at universities leading to degrees or specialized program certifications in the cybersecurity field through communications with the university PIs and by reviewing recipient information in the SFS System.
	The SFS Program shall provide scholarship recipients with summer internship opportunities or other meaningful temporary appointments in the federal information technology and cybersecurity workforce.	Fully Complied	NSF, OPM, and the Department of Homeland Security (DHS) have a joint working group that organizes SFS job fairs. Handouts provided at these job fairs include lists of the attending organizations offering program internships. NSF and OPM verified that scholarship recipients obtained program-approved internships through communications with the university PIs and by reviewing recipient information in the SFS System.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The SFS Program shall prioritize the placement of scholarship recipients fulfilling the post-award employment obligation to ensure that at least 70 percent are placed in a federal executive agency; and not more than 20 percent are placed in a federal legislative branch agency; an interstate agency; a state, local, or tribal government; or a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure; and no more than 10 percent are placed as educators in the field of cybersecurity at qualified institutions of higher education that provide SFS scholarships.	Partially Complied	NSF's SFS Program Solicitation states that at least 70 percent of recipients are placed in a federal executive agency; no more than 20 percent are placed in a federal legislative branch agency; an interstate agency; a state, local, or tribal government; or a state, local, or tribal government-affiliated non-profit considered to be critical infrastructure; and no more than 10 percent are placed as educators in the field of cybersecurity at qualified institutions of higher education that provide SFS scholarships. OPM officials stated that they verified that recipients are working in a full-time qualifying position at an approved organization through communication with the PIs from institutions of higher education and by reviewing employment documentation provided by recipients and relevant information in the SFS System. In addition, NSF's SFS Program Solicitation states that up to 20 percent of scholarship recipients may be placed at entities including National Laboratories or FFRDCs. As amended through 2021, the SFS Program statute addresses requirements relating to scholarship employment placements and scholarship recipients. GAO is currently evaluating these requirements to assess whether they authorize scholarship recipients to work in cybersecurity positions at FFRDCs. GAO will be addressing these matters separately.
As a condition of participating in the program, a qualified university shall enter into an agreement with the Director of NSF, to monitor the compliance of scholarship recipients with respect to their post-award employment obligations.	Fully Complied	While universities participating in the program do not directly monitor the compliance of recipients during the second phase of the program, they are able to view recipient profiles in the SFS System to monitor ongoing compliance of recipients with respect to their post-award employment obligations. OPM's SFS Program Office complied with the requirement for recipients to complete an employment verification form to assist participating universities in meeting the requirement to verify recipient employment obligations.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The Director of NSF, in coordination with the Director of OPM, shall periodically evaluate and make public information on the success of recruiting individuals for scholarships under this section and on hiring and retaining those individuals in the public sector cybersecurity workforce, including information on- (A) placement rates; (B) where students are placed, including job titles and descriptions; (C) salary ranges for students not released from obligations under this section; (D) how long after graduation students are placed; (E) how long students stay in the positions they enter upon graduation; (F) how many students are released from obligations; and (G) what, if any, remedial training is required.	Partially Complied	NSF publicly reported the SFS Program information dating from 2016-2021, including placement rates, student placement locations, job titles, salary ranges, and recommendations for additional training. In a separate data release, NSF publicly reported the number of recipients released from their program obligations. However, the program information that NSF publicly released from 2016 to 2021 did not include information on (D) how long after graduation students (recipients) were placed; and (E) how long students (recipients) stay in the positions they enter upon graduation. Furthermore, NSF delivered its 2021 Biennial SFS Report to Congress on May 12, 2022, that contained information on placement rates, student placement locations, job titles, salary ranges, and recommendations for additional training. However, this report stated that data illustrating (E) how long students stay in the positions they enter upon graduation is not available. In addition, OPM administers surveys to recipients for a total of up to 8 years after the completion of their required work service obligation. Currently, the surveys are the only method used by OPM to evaluate recipient retention. However, the survey data OPM collected were insufficient to calculate how long recipients remain in government positions due to low survey response rates. According to OPM officials, recipient response rates varied from 32 percent to 50 percent between 2014 and 2019. NSF and OPM SFS Program officials stated that they do not enforce the requirement for scholarship recipients to respond to these annual postgraduate surveys. Officials reported that it was not clear what actions would be appropriate to address survey non-respondents. Further, according to the law, there are no penalties for non-respondents who have already completed their service obligation. Additionally, while OPM officials have access to alternate ways to collect information, including government-wide hiring data, they stated that they have not used these data to date because of their limitations. However, the legal requirement still states that NSF and OPM need to determine how long students stay in the positions they entered upon graduation. Until NSF, in coordination with OPM evaluates and makes public data on how long students stay in the positons they enter upon graduation, NSF will be unable to determine the long-term benefits of the SFS Program.

SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
The Director of NSF, in coordination with OPM, shall submit to congressional committees, a report at least once every 3 years. After the deadline for the submission of the initial report, the law was amended to require NSF to submit an expanded report not less frequently than once every 2 years.	Partially Complied	The National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2018, enacted into law on December 12, 2017, amended the Cybersecurity Enhancement Act of 2014 to require the Director of NSF to submit a report to Congress at least once every 3 years. The NDAA for FY 2021, enacted into law on January 1, 2021, subsequently amended the reporting requirement to expand the scope of the report and require that the Director of NSF submit the report to Congress at least once every 2 years. In February 2022, NSF officials stated they had conducted a two-year evaluation of the SFS Program from 2018 to 2020, with most of the program data being collected by October 2020. NSF cited missing the December 12, 2020, reporting deadline established by the NDAA for FY 2018 due to COVID-19. NSF officials stated that three weeks after the December 2020 deadline, the NDAA for FY 2021 amended the Cybersecurity Enhancement Act of 2014 reporting requirement again, this time requiring NSF in coordination with OPM to include information on the disparity in reporting between scholarship recipients and their respective institutions of higher education, and also requiring NSF to submit the report every two years instead of every three years. NSF officials stated that the amendment in the NDAA for FY 2021 overwrote the pre-existing requirement to report by December 12, 2020. As a result, NSF officials stated they delivered a 2021 Biennial SFS Program Report to Congress on May 12, 2022, and will strive to deliver a 2023 Biennial Report in January 2024. In August 2022, NSF indicated that they do not intend to submit a report in satisfaction of the 3-year requirement to report by December 12, 2020, even though that report was required to be submitted to Congress prior to the January 1, 2021, amendment to the Cybersecurity Enhancement Act of 2014. With respect to the contents of the 2021 Biennial SFS Program Report, it does not contain information on how long students stay in the positions they enter upon graduation, which is information required to be included in both the triennial and biennial reports. Until NSF and OPM provide Congress with required SFS Program information in a timely manner, Congress will not have all the information it needs to make effective decisions regarding the program.

	SFS Program Legal Requirements	Evaluation	Assessment of NSF and OPM Compliance
SFS Program Legal Requirements	The Director of NSF, in coordination with the Director of OPM, shall provide consolidated and user-friendly online resources for prospective scholarship recipients, including, to the extent practicable searchable, up-to-date, and accurate information about participating institutions of higher education and job opportunities related to the field of cybersecurity; and a modernized description of cybersecurity careers.	Fully Complied	The OPM's SFS Program website includes pages that list all universities participating in the program and a student resources page that includes links to a website listing cybersecurity job opportunities. It also has a frequently-asked-questions page that provides a description of cybersecurity careers where students can fulfil their work service obligation.

Legend: NSF = National Science Foundation; OPM = Office of Personnel and Management

● Fully Complied = SFS Program documentation and activities addressed all aspects of the legislative requirement;
◐ Partially Complied = SFS Program documentation and activities addressed some, but not all, aspects of the legislative requirement;
○ Not Complied = SFS Program documentation and activities did not address any aspect of the legislative requirement.

Source: GAO analysis of CyberCorps® Scholarship for Service Program Obligations and Guidance. | GAO-22-105187

[a] The NSF SFS Program Solicitation Guide, found on the NSF website, contains information on the SFS Program including: proposal preparation and submission instructions for universities; proposal processing and review procedures; award administration information; revision notes related to changes to the program, program requirements; and program evaluation requirements.

[b] 45 CFR Part 620, NSF Federal Cyber Scholarship-for-Service Program (CyberCorps® SFS), RIN: 3145-AA64, Notice of Proposed Rulemaking

[c] SFS recipients' obligation to repay their scholarship ends upon the completion of their work service obligation period.

While NSF and OPM have complied with most of the 19 selected and identified program legal requirements, they have not fully addressed all of them. The agencies are not always verifying employment and current recipient contact information on an annual basis, collecting complete and consistent data that relate to the fulfillment of all post-award obligations or requirements, reporting how long recipients stay in the positions they enter upon graduation, or providing Congress with required information in a timely manner. Until NSF and OPM ensure that they comply with all program legal requirements and that the SFS Program guidance is consistently enforced, the program will be at risk of not achieving its goal of attracting and retaining high-quality graduates in the public sector cybersecurity workforce. Moreover, the SFS Program may fall short of supporting the U.S. government's strategy to develop a superior cybersecurity workforce.

NSF Did Not Always Effectively Identify, Analyze, Mitigate, and Report SFS Program Risks

According to Carnegie Mellon University's Software Engineering Institute, risk management is an important part of program management.[30] It is defined as a continuous, forward-looking process that should address issues that could endanger achievement of critical program objectives. Therefore, risk-handling activities can be planned and remediated as needed to mitigate adverse impacts on achieving program objectives. SEI's CMMI-SVC, Office of Management and Budget (OMB) Circular No. A-123,[31] *Management's Responsibility for Enterprise Risk Management and Internal Control,* and GAO's *Standards for Internal Controls in the Federal Government* identify risk management best practices.[32] Specific risk management principles from these three sources include management's responsibility for effectively identifying, analyzing, mitigating, and reporting on risks. Additionally, these activities should be documented in, and align with, an organization's strategic plan or in a separate risk management strategy.

NSF officials stated that they follow OMB Circular No. A-123 and the Standards for Internal Controls for risk management. Specifically, NSF officials provided documentation outlining NSF's approach to an enterprise risk management by addressing three approaches: university award management, scholarship recipient support and monitoring, and program outcome controls.

University award management: NSF described its risk-based framework for evaluating the SFS Program solicitation proposals from universities prior to issuance of a program award. The framework includes, but is not limited to, considering the university's record of how it

[30] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Services (CMMI-SVC)*, version 1.3, CMU/SEI-2010-TR-034 (Pittsburg, Pa: November 2010).

[31] Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control,* Circular No. A-123 (July 2016).

[32] GAO, *Standards for Internal Controls in the Federal Government* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

has managed past and current awards, and leveraging the NSF systems to identify any ongoing issues.

Scholarship recipient support and monitoring: NSF described its role in verifying that OPM's SFS Program Office is tracking all the scholarship recipients. NSF performs this verification through ongoing interaction with OPM, including contacting the SFS Program Office several times a week, conducting bi-weekly meetings with OPM in addition to having formal briefings, and monthly Management Board meetings.

Program outcome controls: NSF provided documentation regarding program outcome control measures, which NSF stated it used to measure the program's performance towards achieving goals. NSF identified several program components with defined outcome measures NSF used to identify, analyze, and respond to risks.

However, NSF officials did not provide any documents or a risk management strategy related to how they were identifying, analyzing, mitigating, and reporting SFS program risks and challenges. NSF officials stated that their approach to risk management is performed at the enterprise level. Accordingly, they do not document or track risks specific to SFS. Without a risk management strategy to document risks and challenges, NSF is not in a position to mitigate the adverse effects of risk events that do occur. As a result, this could cause damage to the program.

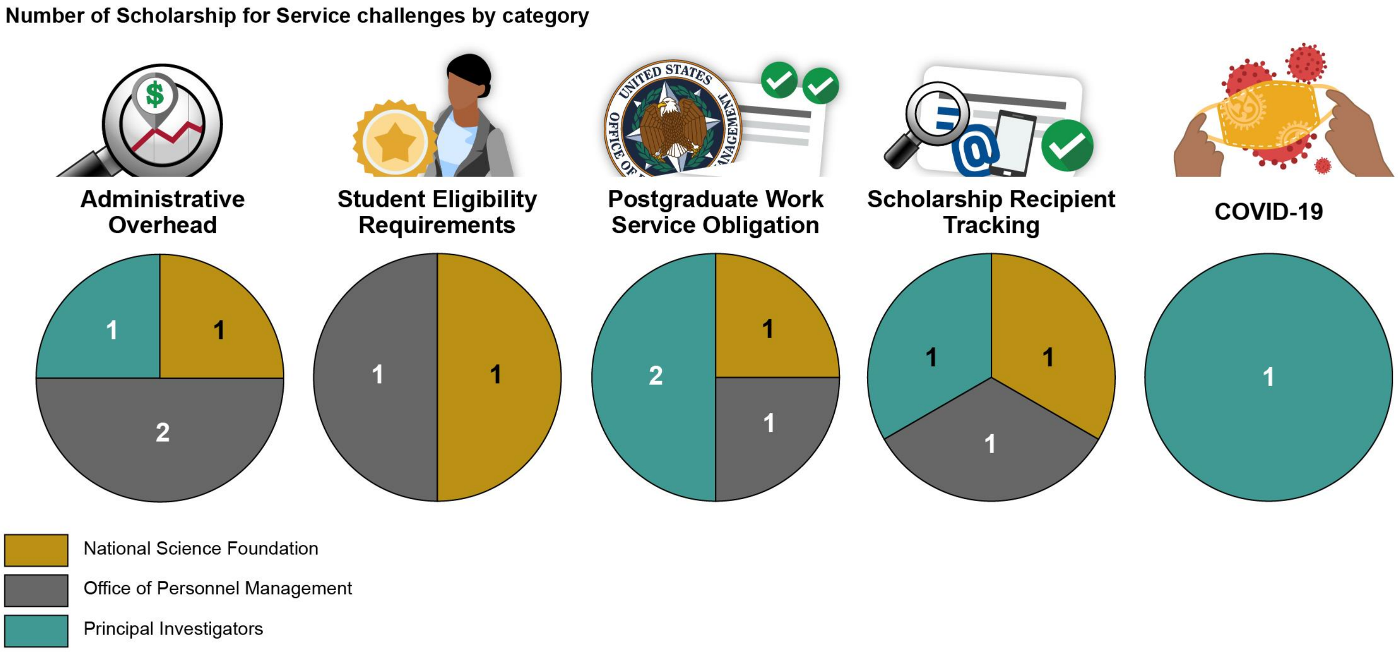
Because the agency had not identified, analyzed, mitigated, and reported on any documented SFS Program risks, we undertook an effort to identify them by analyzing documents and through interviewing NSF and OPM program officials, and PIs from the top five universities receiving awards. We identified 14 key risks and challenges and presented them to the NSF and OPM. The agencies concurred with the risks and challenges and discussed with us possible mitigations that were planned or underway. Based on our analysis, we grouped the 14 risks and challenges for the SFS Program into five areas.

1. SFS Program administrative overhead resulting from SFS Program policies and procedures that inherently impose a greater workload on OPM's SFS Program Office, OPM Human Resource Solutions, as well as SFS PIs;

2. postgraduate work service employment impacted by federal law and other provisions that imposed difficulty for recipients, PIs, and recipient employers;
3. student eligibility impacted by requirements on recipients that are not U.S. citizens;
4. ineffective tracking of scholarship recipients for up to 8 years following the completion of their postgraduate work service obligation; and
5. the COVID-19 pandemic.

Figure 3 shows the number of risks and challenges we identified and organized in each of these five categories. A detailed description of the selected risks and challenges are provided in table 6. In discussing these risks and challenges with the agencies, officials responded by providing us with information on actions that they have taken to mitigate some of these risks and challenges. Although the actions orally noted by officials were not documented and tracked, we included them in table 6 to reflect the officials' views.

Figure 3: Number of CyberCorps® Scholarship for Service (SFS) Program Risks and Challenges by Category



Source: GAO analysis of National Science Foundation, Office of Personnel Management, and University Principal Investigator CyberCorps® Scholarship for Service data; images: toonsteb/stock.adobe.com. | GAO-22-105187

Data for Figure 3: Number of CyberCorps® Scholarship for Service (SFS) Program Risks and Challenges by Category

Administrative Overhead:

- National Science Foundation = 1
- Office of Personnel Management = 2
- Principal Investigators = 1

Student Eligibility Requirements

- National Science Foundation = 1
- Office of Personnel Management = 1

Postgraduate work service obligation

- National Science Foundation = 1
- Office of Personnel Management = 1
- Principal Investigators = 2

Scholarship Receipt Tracking

- National Science Foundation = 1
- Office of Personnel Management = 1
- Principal Investigators = 1

Covid 19

- Principal Investigators = 1

Source: GAO analysis of National Science Foundation, Office of Personnel Management, and University Principal Investigator CyberCorps® Scholarship for Service data; images: toonsteb/stock.adobe.com. |

Table 6: Selected CyberCorps® Scholarship for Service (SFS) Program Risks and Challenges and Steps Taken to Mitigate Them, as of March 2022

	Source of Risks and Challenge	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
Administrative Overhead Risks and Challenges	NSF	A small percentage of recipients who fail to fulfill their work service obligation create a significant workload for OPM's SFS Program Office. The office has to arrange and monitor repayments or to refer the cases for U.S. Treasury collection.	NSF reported that they have been working in consultation with OPM and the Department of Education to develop a Notice of Proposed Rule Making (NPRM) that would govern the process of converting scholarships to student loans if the recipients fail to fulfil their work service obligations. In July 2022, NSF reported that this NPRM was submitted to the Federal Register on June 30, 2022, was published on July 15, 2022, and all comments are due by September 2022. However the final rule has not yet been promulgated by NSF.[a]
	OPM	From a human resources perspective, it is difficult for the SFS Program to keep up with the increasingly high demand among federal government agencies for the program graduates.	OPM officials stated that its Human Resource Solutions department continues to track program progression, and is adding staff to OPM's SFS Program Office team to support the program's ongoing and future growth.
		The OPM SFS System was not designed to capture and determine the percentage of recipients hired by agencies in specific branches of the federal government.	OPM plans to implement future IT system modifications, such as one that that would allow it to retroactively determine the percentage of recipients hired at each branch of the federal government before October 2020.
	PIs	In July 2021, the program changed the per-recipient administrative expenses to a flat rate of $10,000 per recipient. This change resulted in a challenge for certain universities, and raises the risk that the program will not be sustainable due to a mismatch in administrative costs and funding provided.	NSF officials reported that the previous methodology to manage per-recipient administrative expenses capped these costs as a percentage of the overall student recipient expense. However, the capped per-recipient administrative expense as compared to rising costs is resulting in a challenge for certain universities. NSF officials reported that the new methodology uses a per-capita methodology, thus attempting to treat universities equally.
Student Eligibility Requirement Risks and Challenges	NSF, OPM	Current law stipulates that non-U.S. citizens who are permanent residents can become scholarship recipients; however, most federal agencies, as well as state, local, and tribal government agencies, will not hire recipients who are not US citizens. This makes it difficult for non-U.S. citizens to complete their postgraduate work service obligation.	In November 2018, NSF studied the impact of this challenge and made a series of program recommendations. In addition, OPM, in conjunction with the universities, defined a series of remediation efforts to address this issue, such as requiring the university to discuss with the recipient the difficulty of securing postgraduate employment as a non-U.S. citizen. The university then establishes a plan to support the recipient's future success, such as recipients becoming U.S. citizens near their graduation date or focusing on state or local government employment opportunities.
Postgraduate Work Service Obligation Risks and Challenges	NSF	Most universities participating in the program are not able to expand capacity of their programs due to a severe shortage of cybersecurity faculty.	The William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 amended 15 U.S.C. § 7442 and expanded recipient employment opportunities to include placement as an educator in the field of cybersecurity at universities participating in the program. NSF updated the SFS Program Solicitation,[b] NSF 21-580, to reflect the statutory change.

	Source of Risks and Challenge	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
	OPM	Some federal government agencies do not fully leverage the flexibility of appointing recipients directly into the excepted service, and non-competitively convert them to full-time positions, without going through a formal application process, once they have completed their program postgraduate work service obligation.	OPM officials market to federal agencies the opportunity to non-competitively convert, and directly hire, recipients through the provisions in the Cybersecurity Enhancement Act of 2014 in order to streamline the hiring process. Additionally, OPM provides guidance to federal agencies who request their assistance in the process of directly hiring recipients.
	PIs	Some PIs described the legislation that defines and categorizes federal government branch agencies as unclear. As a result, it can be challenging for PIs to approve recipient postgraduate work service employment.	NSF and OPM officials explained that the process for PIs to review and make recommendations on recipient employment opportunities has been streamlined. For example, PIs are only required to review and recommend approval or disapproval for commitments reported by recipients that fall in the non-executive branch federal agency and educator categories.
		The amount of time for recipients to obtain a security clearance for eligible federal government executive branch positions is very long. For example, it could take up to two years for a recipient to get a top-secret security clearance.	NSF is providing guidance to recipients with expectations for the security clearance process, the types of information that will be needed, and to prepare by gathering required information early. Recipients are also urged by NSF and OPM to begin their postgraduate employment search early. Additionally, NSF and OPM are urging agencies to recruit and make tentative offers of employment early in order for the security clearance process to be started earlier.
Scholarship Recipient Tracking Risks and Challenges	NSF, OPM, PIs	Tracking SFS recipients from entry into the program for 8 years following the completion of their postgraduate work service obligation is a challenge. NSF and OPM reported having limitations in tracking recipients beyond their postgraduate work service obligation, in particular for recipients who work in the intelligence community. Additionally, PIs who track their recipients after graduation, stated it is difficult to continue in their role as an advisor to recipients who are employed in the intelligence community, due to similar issues.	OPM is continuing to explore solutions to this challenge. In December 2021, OPM officials stated that remediation efforts taken by OPM include allowing recipients to submit their postgraduate SFS Program employment verification via fax, mail, or by phone, in lieu of reporting it online in the SFS system.

	Source of Risks and Challenge	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
COVID-19 Risks and Challenges	PIs	The success of the program at the university level was based on in-person interactions that provide community support. Without the ability to conduct program activities in-person, PIs stated that many of their recipients were adversely impacted. COVID-19 made it more difficult for PIs to monitor scholarship recipients and determine when the recipients needed support. In addition, COVID-19 made it more difficult for recipients to obtain support from their peers. Additionally, a PI explained that due to COVID-19, the 2020 and 2021 SFS job fairs were conducted virtually instead of in person. This change made it more difficult for recipients to obtain the required SFS Program summer internship and secure program-approved postgraduate employment.	NSF and OPM SFS Program officials provided pandemic guidance to PIs, allowed additional time for the recipients to search for postgraduate positions, and made exceptions to allow recipients to complete internship requirements at organizations that would normally be non-approved. In addition, NSF established the 2020 SFS Summer Experience to substitute cancelled internships with research and professional development summer activities. Specifically, NSF organized 30 summer projects in lieu of mandatory internships, and created provisions for additional COVID-19 related stipends for the recipients. NSF officials plan to hold the January 2023 SFS job fair in-person.

Legend: NSF = National Science Foundation; OPM = Office of Personnel Management, PI = Principle Investigator

Source: GAO analysis of CyberCorps® Scholarship for Service program data. | GAO-22-105187

[a] NSF required that interested parties should submit written comments on or before September 13, 2022 to be considered in the formation of the final rule.

[b] The NSF SFS Program Solicitation, contains information on the SFS Program including: proposal preparation and submission instructions for universities; proposal processing and review procedures; award administration information; revision notes, program requirements; and program evaluation.

For additional details of all 14 risks and challenges and steps taken to mitigate some of the risks and challenges, see appendix IV.

Conclusions

The CyberCorps® SFS Program plays an important role in addressing the federal government's IT and cybersecurity workforce needs. As the organizations responsible for managing CyberCorps®, NSF and OPM have complied with most of SFS's governing legal requirements. However, the agencies do not verify employment and current recipient contact information on an annual basis, collect complete and consistent data that relate to the fulfillment of all post-award obligations or requirements, report how long recipients stay in the positions they enter upon graduation, or provide Congress with all required information in a timely manner. While the agencies are aware of the issue, they have yet to establish a timeframe and process to collect this information. Further, NSF has not consistently reported data on scholarship recipients, specifically on how long students stay in the positon they enter upon graduation. As a result, it is not clear whether the SFS Program is achieving its goal of attracting and retaining long-term employees in the public sector cybersecurity workforce. Furthermore, NSF has not provided Congress with all required information in a timely manner so that it can make informed decisions regarding the program. Until NSF and OPM ensure that they comply with all program legal requirements, the program will be at risk that it will fall short of developing a superior cybersecurity workforce.

NSF did not implement a risk management strategy and process to effectively identify, analyze, mitigate, and report on program risks and challenges. Without a risk management strategy, NSF is not in a position to mitigate the adverse effects of risk events that do occur, which could negatively impact the accomplishment of program goals.

Recommendations for Executive Action

We are making a total of five recommendations, including three to NSF and two to OPM. Specifically:

The Director of the National Science Foundation, in coordination with the Director of the Office of Personnel Management, should periodically evaluate and make public, information on how long CyberCorps® Scholarship for Service Program scholarship recipients stay in the positions they enter upon graduation. (Recommendation 1)

The Director of the National Science Foundation should provide Congress with all required information in a timely manner for the CyberCorps® Scholarship for Service Program so Congress can use this information to make informed decisions regarding the SFS Program. (Recommendation 2)

The Director of the National Science Foundation should develop and implement a risk management strategy that includes a process to effectively identify, analyze, mitigate, and report CyberCorps® Scholarship for Service Program risks and challenges. (Recommendation 3)

The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should establish a time frame for implementing a process to ensure that all CyberCorps® Scholarship for Service Program scholarship recipients provide their institutions of higher education and the Office of Personnel Management (in coordination with the National Science Foundation) with annual verifiable documentation of post-award employment and up-to-date contact information for a period of at least through the end of their work service obligation. (Recommendation 4)

The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should ensure the collection of complete and consistent data that relate to the fulfillment of all post-award obligations or requirements pursuant to the CyberCorps® Scholarship for Service Program. (Recommendation 5)

Agency Comments

We provided a draft of this report to the National Science Foundation (NSF), Office of Personnel Management (OPM), and the Department of Homeland Security (DHS) for their review and comment. NSF and OPM concurred with our recommendations. DHS told us they did not have any comments on the draft.

In NSF's written comments, reproduced in appendix V, the agency concurred with our three recommendations and described the steps planned or under way to address them. For example, in response to our first recommendation, NSF stated that it was in the final stage of promulgating a new regulation to help with the management of the CyberCorps® Scholarship for Service (SFS) Program. This includes improvement in gathering required data and in converting the SFS scholarships to loans in the event that SFS recipient fail to complete their service obligation. NSF noted that these SFS Program enhancements are being conducted in collaboration with OPM, DHS, and the Department of Education. In response to our second and third recommendations, NSF discussed additional actions the agency plans to take. These include working with OPM to provide Congress and the public with all SFS Program required information on a biennial basis, and to implement a risk management strategy for the program. NSF also provided technical comments, which we have incorporated as appropriate.

In OPM's written comments, reproduced in appendix VI, it concurred with our two recommendations and described the steps planned or under way to address them. For example, in response to our first recommendation, OPM stated that it is working with NSF to establish a timeline and implement changes related to SFS recipients providing their institutions of higher education and OPM with annual verifiable documentation of post-award employment and up-to-date contact information. In response to our second recommendation, OPM stated it is working with NSF to ensure the collection of complete and consistent data that relate to the fulfillment of all post-award obligations or requirements pursuant to the SFS Program. We have updated this report to reflect these comments.

We are sending copies of this report to appropriate congressional committees, the Director of the National Science Foundation, the Director of the Office of Personnel Management, and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

If you have any questions regarding this report, please contact me at (214) 777-5719 or HinchmanD@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VII.

David B Hinchman

David B. Hinchman
Acting Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our specific objectives were to (1) identify what actions, if any, did the National Science Foundation (NSF) and the Office of Personnel Management (OPM) take to comply with the CyberCorps® Scholarship for Service Program (SFS) requirements, and to what extent does their process track whether scholarship recipients have remained employed by the government after completing the program; and (2) determine the extent to which NSF has identified, analyzed, mitigated, and reported risks on the SFS program.

To address these two objectives, our scope of work included interviews with the NSF Program officials, OPM Program and human capital officials, DHS Program officials, as well as Principal Investigators (PI) from a sample of five universities participating in the program.[1] We selected the five universities that received the most program award funding between fiscal year (FY) 2016 and FY 2020. To identify these universities, we performed a search in NSF's online award database for both active and expired program awards, which returned 613 total awards. These results were refined to only include the SFS Program's scholarship track for FY 2016 through FY 2020 and universities that received a total of $3 million or more in funding during these fiscal years.[2] The top five universities that met our criteria included Tennessee Technological University, University Enterprises Corporation at California State University (at San Bernardino), Georgetown University, University of Alabama (at Huntsville), and Florida State University.

To address the first objective, we reviewed the Cybersecurity Enhancement Act of 2014 and identified 35 legal requirements related to

[1] Universities refer to all institutions of higher education that participate in the CyberCorps® Scholarship for Service Program, including community colleges.

[2] Beginning with the 2018 SFS Program solicitation, the SFS Program's Capacity Building track was merged with the National Science Foundation's Education Designation of the cross-agency Secure and Trustworthy Cyberspace program, and removed from the SFS Program, thus the only SFS program track remaining was the Scholarship track.

the SFS Program.[3] Of these 35 legal requirements, we identified and selected the 19 requirements of the law that related to how NSF and OPM managed, monitored, and tracked the program. These three categories include: (1) the recipients' eligibility and responsibilities (recipient responsibilities); (2) conditions under which the recipient forfeits their scholarship (forfeiture of scholarship); and (3) NSF and OPM's administrative responsibilities related to the recipients (administrative responsibilities). We then analyzed NSF and OPM's SFS Program policies and procedures as well as the program documentation,[4] and compared them to the 19 identified and selected legal requirements to determine the extent to which NSF and OPM were in compliance.[5]

We determined whether NSF and OPM's actions related to how they managed, monitored, and tracked the program had fully complied, partially complied, or not complied with each of the 19 identified and selected legal requirements. In addition, we analyzed program documentation and conducted interviews with NSF and OPM Program officials.

To address the second objective, we analyzed NSF's SFS Program risk documentation such as the SFS Program Solicitation and NSF's data analytics and assurance to determine the extent to which NSF had a risk management process in place.[6] We also interviewed NSF officials to understand their enterprise risk management process. We then compared NSF's SFS Program risk documentation to risk management best practices to determine the extent which NSF identified, analyzed,

[3] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (2014).

[4] Documentation reviewed included the SFS Student Service Agreement and corresponding guidance document, the SFS Program Solicitation, Amendment to Memorandum of Agreement between NSF and OPM, meeting minutes, and other program documentation.

[5] Scholarship recipients are students who, as a condition of receiving a scholarship under the SFS program, enter into an agreement under which the recipient, upon receipt of their academic degree, agrees to work for a period equal to the length of the scholarship in the cybersecurity mission of an executive agency, a legislative or interstate agency, a state, local, or tribal government, or a state, local, or tribal government-affiliated non-profit that is considered to be critical infrastructure, and as educators in the field of cybersecurity at qualified institutions of higher education that provide SFS scholarships.

[6] The NSF SFS Program Solicitation, contains information on the SFS Program including: proposal preparation and submission instructions for universities; proposal processing and review procedures; award administration information; revision notes, program requirements; and program evaluation.

mitigated, and reported risks on the SFS Program. Specially, we reviewed best practices such as OMB Circular No. A-123,[7] *Management's Responsibility for Enterprise Risk Management and Internal Control,* GAO's *Standards for Internal Controls in the Federal Government* identify risk management best practices,[8] and by the Software Engineering Institute's Capability Maturity Model® Integration for Services (CMMI-SVC).[9] Because NSF had not identified, analyzed, mitigated, or reported any risks associated with the SFS Program, we undertook an effort to identify them by analyzing documents and by interviewing NSF and OPM officials, well as program PIs from the top five universities receiving awards. We developed a list of 14 risks and challenges identified by NSF, OPM and PIs, and presented them to the agencies. NSF and OPM concurred with risks and challenges, and discussed with us possible mitigations that were planned or underway. We grouped the 14 risks and challenges into five categories based on the program area affected.

1. SFS Program administrative overhead resulting from SFS Program policies and procedures that inherently impose a greater workload on OPM's SFS Program Office, OPM Human Resource Solutions, as well as SFS PIs;
2. postgraduate work service employment impacted by federal law and other provisions that imposed difficulty for recipients, PIs, and recipient employers;
3. student eligibility impacted by requirements on recipients that are not U.S. citizens;
4. ineffective tracking of scholarship recipients for up to 8 years following the completion of their postgraduate work service obligation; and
5. the COVID-19 pandemic.

We conducted this performance audit from April 2021 to September 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our

[7] Office of Management and Budget, *Management's Responsibility for Enterprise Risk Management and Internal Control,* Circular No. A-123 (Washington, D.C.: July 2016).

[8] GAO, *Standards for Internal Controls in the Federal Government* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[9] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model® Integration for Services (CMMI-SVC)*, version 1.3, CMU/SEI-2010-TR-034 (Pittsburgh, Pa: November 2010).

findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: SFS Program Awards by Location, Fiscal Year 2016 through Fiscal Year 2021

Universities in a variety of states obtained funding for CyberCorps® Scholarship for Service (SFS) Program scholarships.[1] Universities in Alabama received the most in program awards (about $22 million) and universities in South Carolina were awarded the least (about $1 million).[2] Universities in several states, including Maine, Iowa, and Oregon, did not receive any scholarship funds. The states without awards either did not have any universities within that state apply for the program awards, or the National Science Foundation (NSF) did not select universities within that state for the program awards. Figures 4 and 5 display fiscal year (FY) 2016 through FY 2021 program award amounts made to universities by state.

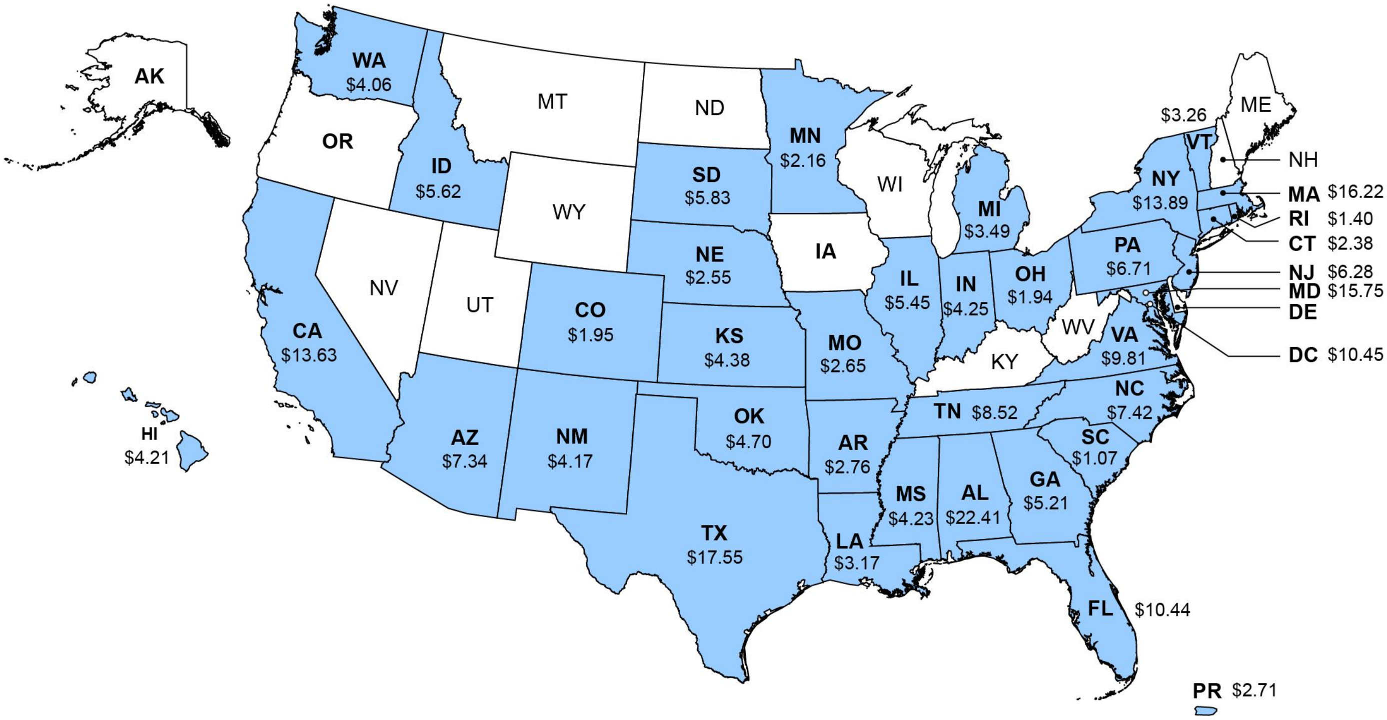
[1] Universities refer to all institutions of higher education that participate in the CyberCorps® Scholarship for Service Program, including community colleges.

[2] Award amount figures are in nominal terms.

Appendix II: SFS Program Awards by Location, Fiscal Year 2016 through Fiscal Year 2021

Figure 4: Fiscal Year 2016 through Fiscal Year 2021 CyberCorps® Scholarship for Service (SFS) Program Awards by Location

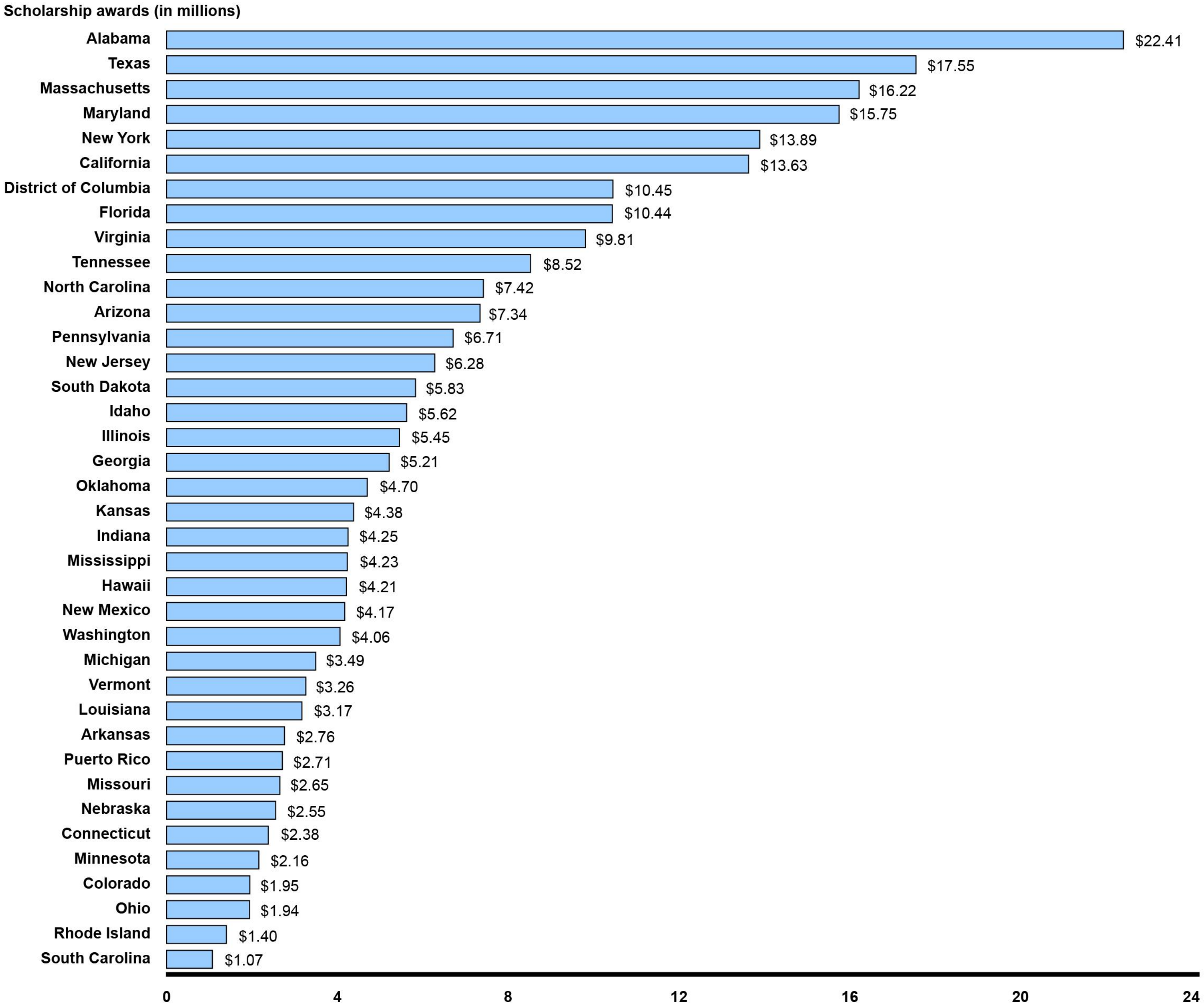
Scholarship awards (in millions)



Sources: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program award data. | GAO-22-105187

Appendix II: SFS Program Awards by Location, Fiscal Year 2016 through Fiscal Year 2021

Figure 5: Fiscal Year 2016 through Fiscal year 2021 CyberCorps® Scholarship for Service (SFS) Program Awards by Location



Sources: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program award data. | GAO-22-105187

Data table for Figure 5: Fiscal Year 2016 through Fiscal year 2021 CyberCorps® Scholarship for Service (SFS) Program Awards by Location

State	SFS Award amount ($ in millions)
Alabama	22.41
Texas	17.55
Massachusetts	16.22
Maryland	15.75
New York	13.89
California	13.63
District of Columbia	10.45
Florida	10.44
Virginia	9.81
Tennessee	8.52
North Carolina	7.42
Arizona	7.34
Pennsylvania	6.71
New Jersey	6.28
South Dakota	5.83
Idaho	5.62
Illinois	5.45
Georgia	5.21
Oklahoma	4.7
Kansas	4.38
Indiana	4.25
Mississippi	4.23
Hawaii	4.21
New Mexico	4.17
Washington	4.06
Michigan	3.49
Vermont	3.26
Louisiana	3.17
Arkansas	2.76
Puerto Rico	2.71
Missouri	2.65
Nebraska	2.55
Connecticut	2.38
Minnesota	2.16
Colorado	1.95

State	SFS Award amount ($ in millions)
Ohio	1.94
Rhode Island	1.4
South Carolina	1.07

Appendix III: SFS Program Agency and University Responsibilities

To implement the CyberCorps® Scholarship for Service (SFS) Program's goals, the National Science Foundation (NSF), Office of Personnel Management (OPM), and the Department of Homeland Security (DHS), and the university Principal Investigators (PIs) have various key SFS Program responsibilities, as outlined in tables 7-11.

Table 7 outlines NSF's key SFS Program responsibilities.

Table 7: Key National Science Foundation CyberCorps® Scholarship for Service (SFS) Program Responsibilities

Financially manage the SFS Program.
Create and distribute the annual program solicitation to prospective universities.[a]
Evaluate the program solicitation proposals from the universities using an established merit review process and issues the three to five year awards to selected universities.
Represent the program through relationships with organizations that hire recipients such as federal agencies and other organizations within the academic/scientific communities.

Source: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program documentation and interview. | GAO-22-105187

[a] Universities refer to all institutions of higher education that participate in the CyberCorps® Scholarship for Service Program, including community colleges.

Table 8 outlines OPM's key SFS Program responsibilities.

Table 8: Key Office of Personnel Management CyberCorps® Scholarship for Service (SFS) Program Responsibilities

Facilitate the registration and tracking of all recipients and their program commitments, from entry into the program until 8 years following the completion of their post-graduation commitment.
Respond to general inquiries from prospective students, current/former scholarship recipients, universities, and agencies.
Review and approve recipient employment offers.
Coordinate the collection and transmission of information for repayments and waiver requests to the National Science Foundation.
Participate in planning the annual in-person job fair.
Draft, review, update, and distribute program service agreements, program policy, guidance documents, and other program documentation, including the distribution and tracking of surveys.
Coordinate and host multiple virtual events such as quarterly zoom sessions with recipients, agency information sessions, and virtual job fairs.

Source: GAO analysis of Office of Personnel Management CyberCorps® Scholarship for Service program documentation. | GAO-22-105187

Table 9 outlines NSF and DHS's key SFS Program responsibilities.

Table 9: Joint Key National Science Foundation (NSF) and Department of Homeland Security (DHS) CyberCorps® Scholarship for Service (SFS) Program Responsibilities

Promote an interchange of expertise between the NSF and DHS workforce development.
Promote U.S. higher education information assurance through the program.
Participate in an annual SFS Program meeting.
Designate program administrators to serve as the primary points of contact within their respective agencies to be responsible for tracking any matters of joint concern or potential developments, which could be of importance to the SFS Program.
Conduct an annual program review to determine program effectiveness and determine a need for adjustments.

Source: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program documentation. | GAO-22-105187

Table 10 outlines DHS's individual key SFS Program responsibilities.

Table 10: Key Department of Homeland Security CyberCorps® Scholarship for Service (SFS) Program Responsibilities

Participate as a member of the annual review board for the program.
Participate in National Science Foundation-led information security training and education conference, symposia, and working groups.

Source: GAO analysis of National Science Foundation CyberCorps® Scholarship for Service program documentation. | GAO-22-105187

In addition to federal agency support, the SFS Program is supported by university Principal Investigators (PI). Table 11 outlines key university PI SFS Program responsibilities.

Table 11: Key Principal Investigator CyberCorps® Scholarship for Service (SFS) Program Responsibilities

Serve as the SFS Program administrator of the award.
Serve as the primary point of contact between the university, the National Science Foundation, and the Office of Personnel Management.
Identify, evaluate, and select students to become scholarship recipients.
Design, develop, and implement the program to enrich the recipient education and skills.
Guide the recipients throughout the SFS lifecycle, including academics, internship, and postgraduate work service requirements.

Source: GAO analysis of CyberCorps® Scholarship for Service program documentation and interview. | GAO-22-105187

Appendix IV: Risks and Challenges within the SFS Program, and What Steps NSF and OPM Have Taken to Mitigate Them

Because the National Science Foundation (NSF) had not identified, analyzed, mitigated, or reported any risks associated with the CyberCorps® Scholarship for Service (SFS) Program, we undertook an effort to identify them by analyzing documents and by interviewing NSF and Office of Personnel Management (OPM) officials, well as program Principal Investigators (PIs) from the top five universities receiving awards.[1] We identified 14 key risks or challenges and presented them to the NSF and OPM. In discussing these risks and challenges with the agencies, officials responded by providing us with information on actions that they have taken to mitigate some of these risks and challenges. Although the actions orally noted by officials were not documented and tracked, we included them in table 12 below to reflect the officials' views.

[1] Universities refer to all institutions of higher education that participate in the CyberCorps® Scholarship for Service Program, including community colleges.

Table 12: CyberCorps® Scholarship for Service (SFS) Program Risks and Challenges and Steps Taken to Mitigate Them as of March 2022

	Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
Administrative Overhead Risk and Challenges[a]	NSF	According to agency officials, a small percentage of recipients who fail to fulfil their program postgraduate work service obligation create a significant workload for the program to arrange and monitor repayments or to refer the cases for U.S. Treasury collection. According to 15 U.S.C. § 7442,b scholarship recipients are financially liable to the United States if the individual fails to fulfill the post-award employment obligation, among other things. Failure to satisfy the program requirements results in forfeiture of the scholarship award, which must either be repaid or reverted by the university to a student loan with repayments pro-rated to reflect partial service completed.	NSF officials stated that since April 2021, they have been working in consultation with OPM and the Department of Education to develop a proposed rule that would govern the process of converting the scholarships to student loans. Specifically, the first step of the rulemaking process is to submit a Notice of Proposed Rulemaking (NPRM). In July 2022, NSF reported that this NPRM was submitted to the Federal Register on June 30, 2022, was published on July 15, 2022, and all comments are due by September 2022. However the final rule has not yet been promulgated by NSF.[b]
	OPM	OPM officials stated that it is a challenge to prepare the program for growth from a human resources perspective. Specifically, it is difficult to keep up with the increasingly high demand among federal government agencies for the program graduates.	To address this challenge, OPM officials stated that OPM's Human Resource Solutions department continues to track program demand, and in response, is adding staff to OPM's SFS Program Office team to support ongoing and future program growth.
		The OPM SFS System was not designed to capture and determine the percentage of scholarship recipients hired by agencies in specific branches of the federal, state, local, or tribal government. 15 U.S.C. § 7442 requires that at least 70 percent of SFS scholarship recipients secure employment in a federal government executive branch agency. However, the SFS System was designed before this requirement was established and is unable to capture and determine the percentage of recipients employed at agencies in specific branches of the federal government.	To address this challenge, OPM modified the two components it used to manage the program, specifically the SFS System, as well as the electronic spreadsheet, Master Roster and Placement Log. According to OPM officials, the modification to both IT components allows OPM to easily determine, for those recipients employed by federal government agencies, their respective type of federal government branch. Additionally, the modification allows OPM to retroactively determine the percentage of recipients hired at each branch of the federal government, dating back to October 2020. OPM plans to implement future IT system modifications, such as one that that would allow them to retroactively determine the percentage of recipients hired at each branch of the federal government before October 2020.

Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
PIs	In February 2006, the SFS Program changed administrative expenses related to each individual recipient. Prior to the change, PIs could request up to 15 percent of their total award budget as partial reimbursement of indirect costs to address the management and administrative costs directly associated with operating the program. In addition, PIs had the ability to request up to 5 percent of their total award budget as partial reimbursement of direct or indirect costs of the total budget to address curriculum, laboratory, and faculty development in support of the program.[c] However, in July 2021, the program changed the per recipient administrative expense to a flat rate of $10,000 per recipient, per year. This change resulted in a challenge, particularly for universities that charge high tuition rates, thereby resulting in a lower number of recipients to receive scholarships at these particular universities.	In response to this challenge, NSF officials explained that the previous methodology capped indirect, administrative costs at a percentage of the support for student recipients. Examples of activities supported by these indirect costs are administrative tasks and student mentoring. This allowed universities that charged higher tuition to benefit from a larger operational budget while those universities that charged lower tuition were disadvantaged, compromising the extent to which they could support administration of the SFS Programmatic elements such as administrative tasks and student mentoring. NSF officials stated that the new methodology uses a per capita methodology so that universities are treated equally. However, the capped per-recipient administrative expense as compared to rising costs is resulting in a challenge for certain universities.

	Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
Student Eligibility Legislation Risks and Challenges[d]	NSF, OPM	Most federal, state, local, and tribal government agencies will not hire recipients who are not U.S. citizens, impacting postgraduate employment possibilities. The Cybersecurity Enhancement Act of 2014, [e] expanded recipient eligibility requirements to include lawful permanent residents of the U.S. However, NSF and OPM reported that most federal government agencies, as well as most state, local, and tribal government agencies, will not hire recipients who are not U.S. citizens. According to NSF and OPM officials, recipients who are lawful permanent residents and not U.S. citizens have a difficult time fulfilling their required postgraduate work service obligation.	To address this challenge, NSF officials stated that in November 2018, OPM's SFS Program Office examined the impact of the Cybersecurity Enhancement Act of 2014[f] on the program. Specifically the SFS Program Office analyzed the likelihood that a lawful permanent resident of the U.S. could fulfill their postgraduate work service obligation by conducting a survey of 84 individual federal, state, local, and tribal government agencies, as well as federally funded research and development centers (FFRDCs). NSF generated recommendations for the SFS Program Office, based on the results of its survey: 1. Provide all university PIs with a list of agencies participating in the SFS Program, identifying those that require U.S. citizenship for employment and those that hire lawful permanent residents; 2. If a lawful permanent resident recipient is unable to secure a program internship, consider requiring the recipient's university to place the recipient on a mutually beneficial cyber research project; 3. For the required postgraduate program work service obligations, research the feasibility and legality of implementing a program policy that requires recipients who are lawful permanent resident to become U.S. citizens within 18 months of graduation; 4. Examine state, local, or tribal government-affiliated non-profit organizations that are considered to be critical infrastructure, and thus less able to accept lawful permanent resident program recipients. In addition to recommendations resulting from the survey, NSF officials stated that lawful permanent residents are able to meet their postgraduate work service obligation by obtaining employment as a faculty member at a university participating in the program. In addition to NSF's efforts to remediate this particular challenge, OPM officials outlined remediation efforts by universities participating in the program. Specifically, they stated that prior to recipients signing the SFS Program Agreement, the university discusses with the recipient the difficulty of securing postgraduate employment as a non-U.S. citizen. The university then establishes a plan to support the recipient's future success, such as recipients becoming U.S. citizens near their graduation date or focusing on state or local government employment opportunities.

	Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
Postgraduate Work Service Obligation Risks and Challenges[g]	NSF	Most educational institutions participating in the SFS Program are not able to expand capacity of their SFS Programs due to a severe shortage of cybersecurity faculty.	In response to this shortage, NSF officials referenced the National Defense Authorization Act for Fiscal Year 2021[h] as amended by 15 U.S.C. § 7442.[i] Specifically, the expansion of recipient employment opportunities to include placement as an educator in the field of cybersecurity at a participating universities in the program. As a result, in April 2021, NSF updated the SFS Program Solicitation, NSF 21-580,[j] to reflect the change in statute, thus allowing for 10 percent of recipients to fulfill their postgraduate work service obligation as educators in the field of cybersecurity at universities already participating in the program. As these faculty positions become available, the SFS Program Office routinely shares opportunities with university PIs and their recipients. NSF expects this change in the program legal requirements to have a positive impact in addressing the severe shortage of cybersecurity faculty.
	OPM	Some federal government agencies do not fully leverage the flexibility of appointing recipients directly into the excepted service, and non-competitively convert them once they have completed their required postgraduate program work service obligation.[k] According to OPM officials, when the SFS Program was established, there was no specific federal government hiring authority that allowed federal agencies to directly hire recipients. Agencies were instructed to hire recipients using whatever hiring authority available to them at that time. In many cases, this required the recipients to compete with other employment applicants that did not have a SFS postgraduate work service obligation. The Cybersecurity Enhancement Act of 2014,[l] allowed federal agencies to appoint recipients into the excepted service citing the law as the hiring authority. This law successfully addressed the challenge of how federal agencies can hire recipients. However, some agencies still do not fully leverage their flexibility in hiring recipients into the excepted service.	To address this challenge, OPM continually markets to federal agencies the opportunity to non-competitively convert recipients through the provisions in the Cybersecurity Enhancement Act of 2014. Additionally, OPM officials stated they provide guidance to federal agencies who request their assistance in hiring recipients. OPM officials have also conducted virtual meetings with federal agencies to educate them regarding the SFS Program, including recruiting and hiring of recipients. OPM officials stated they plan to continue their efforts to remediate this challenge by continuing to offer virtual as well as in-person meetings regarding the recruiting and hiring of scholarship recipients.

Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
PIs	Recent statutory changes related to definitions and categories of federal government branch agencies have resulted in challenges for PIs attempting to approve recipient postgraduate work service employment. Specifically, a PI stated that it can be difficult to determine how to identify a federal agency's program designation, at least 70 percent of recipients can be placed in a federal executive agency Similarly, no more than 20 percent of recipients can be placed in other positions such as federal legislative branch agencies; interstate agencies; state, local, or tribal government agencies; and state, local, or tribal government-affiliated non-profits considered critical to the infrastructure. Lastly, no more than 10 percent of recipients can be placed as educators in the field of cybersecurity at qualifying universities that participate in the program. Additionally, the rule has caused complications for some universities with relationships with FFRDCs. For example, PIs explained that, at previous SFS Program job fairs, organizations such as the MITRE Corporation as well as other FFRDCs, have been allowed to attend. These organizations often tell recipients that their organizations are approved for SFS internships and employment. However, PIs have had to deny job offers made to their recipients in order to stay within the program placement threshold percentages.	In response to this challenge, NSF officials, in coordination with OPM SFS Program officials, made enhancements to the SFS System to include more specific job categories, and are working to provide resources to PIs to ensure they can easily determine the agency's category. For example, NSF added a list of federal executive branch agencies to their public-facing website. NSF and OPM officials also explained that the process for university PIs to review and make recommendations on recipient employment opportunities has been streamlined. For example, PIs are only required to review and recommend approval or disapproval for commitments reported by recipients that fall in the non-executive branch agency and educator categories. In these instances, the PI receives email communication containing guidance on how to properly classify the commitment.
	The amount of time for recipients to obtain a security clearance for eligible federal government executive branch positions is a challenge. According to PIs, the length of time it takes for a recipient to apply for and obtain a security clearance affects their ability to accept employment within the 18-month window required by the program to begin their postgraduate work service obligation. PIs stated that it can take up to a year or more for a recipient to receive their security clearance, and recipients are not allowed to be employed during this waiting period.	Both NSF and OPM are aware of the challenge and, while shortening the security clearance process is beyond their control, they are implementing remediation actions to the extent possible. Specifically, NSF officials stated that guidance is provided to recipients with expectations for the security clearance process, the types of information that will be needed, encouraging recipients to prepare by gathering required information early. Recipients are also urged by NSF and OPM SFS Program officials to begin their postgraduate employment search early. However, recipients who have not secured a position of employment within the 18-month period are able to submit a request for an extension to the SFS Program Office. In addition, NSF and OPM are urging agencies to recruit and make tentative offers of employment early to recipients in order to remediate this challenge.

	Source of Risks and Challenges	Risks and Challenges Descriptions	Steps Taken to Mitigate Risks and Challenges
Scholarship Recipient Tracking Risks and Challenges[m]	NSF, OPM, PIs	Tracking recipients from entry into the SFS Program until 8 years following the completion of their postgraduate work service obligation is a challenge. As previously discussed, NSF and OPM have limitations in tracking recipients beyond their postgraduate work service obligation. This is a particular problem for recipients who work in the intelligence community. According to NSF and OPM officials, scholarship recipients who join federal government intelligence community agencies to complete their postgraduate work service obligation are often advised by these agencies to not provide additional information to the program, including not responding to the annual surveys. Additionally, PIs who are required to track their recipients after graduation, stated it is difficult to continue in their role as an advisor to recipients who are employed in the intelligence community, due to similar issues.	OPM officials stated that they are continuing to explore solutions to determine the best way to track recipients once they have accepted employment with federal intelligence community agencies. Current remediation efforts taken by OPM in response to this challenge include allowing the recipient to submit their postgraduate SFS Program employment verification via fax, mail, or by phone in lieu of reporting it online in the SFS System.
COVID-19 Risks and Challenges[n]	PIs	The ability for recipients to meet program requirements was a challenge as a result of COVID-19. According to one PI, the success of the SFS Program at the university level is based on in-person interactions that provide community support. Without the ability to conduct SFS Program activities in-person, one PI stated that many of their recipients were adversely impacted. Additionally, one PI explained that due to COVID-19, the 2020 and 2021 SFS job fairs were conducted virtually instead of in-person. This change made it more difficult for scholarship recipients to obtain the required program summer internship and secure program-approved postgraduate employment.	To remediate the challenges related to COVID-19, NSF and OPM SFS Program officials provided pandemic guidance to PIs, allowed additional time for the recipients to search for postgraduate positions, and made exceptions to allow recipients to complete internship requirements at organizations that would normally be non-approved. In addition, NSF established the 2020 SFS Summer Experience to substitute cancelled internships with research and professional development summer activities. Specifically. NSF organized 30 summer projects in lieu of mandatory internships, and created provisions for additional COVID-19 related stipends for the recipients. NSF officials plan to hold the January 2023 SFS job fair in person.

Legend: NSF = National Science Foundation; OPM = Office of Personnel Management, PI = Principle Investigator

Source: GAO analysis of CyberCorps® Scholarship for Service program data. | GAO-22-105187

[a] Administrative overhead risks and challenges are those that relate to SFS Program policies and procedures that inherently impose a greater workload on OPM's SFS Program Office, OPM Human Resource Solutions, as well as university PIs.

[b] Legal requirements for the SFS program are addressed by § 302 of the Cybersecurity Enhancement Act of 2014 as amended by the NDAA for Fiscal Years 2018 and 2021 (codified at 15 U.S.C. § 7442).

[c] NSF 06-507.

[d] Student eligibility legislation challenges are related to legislation that inherently imposed difficulty for scholarship recipients that are not U.S. citizens.

[e] Public Law No. 113-274, 128 Stat. 2971 (2014).

[f] Public Law No. 113-274.

[g] Postgraduate work service obligation challenges are those related to federal legislation and other provisions that inherently impose difficulty for scholarship recipients, SFS PIs, and scholarship recipient employers.

[h] NDAA for Fiscal Year 2021, Pub. L. No. 116-283, 134 Stat. 3388 (Jan. 1, 2021).

[i] Legal requirements for the SFS program are addressed by § 302 of the Cybersecurity Enhancement Act of 2014 as amended by the NDAA for Fiscal Years 2018 and 2021 (codified at 15 U.S.C. § 7442).

[j] NSF 21-580, SFS Program solicitation states, "With permission of the OPM SFS Program Office, a limited number of students, but no more than 10 percent of scholarship recipients, may be placed as educators in the field of cybersecurity at qualified institutions of higher education that provide SFS scholarships. Such placement would fulfill the scholarship recipient's postgraduate work service obligation."

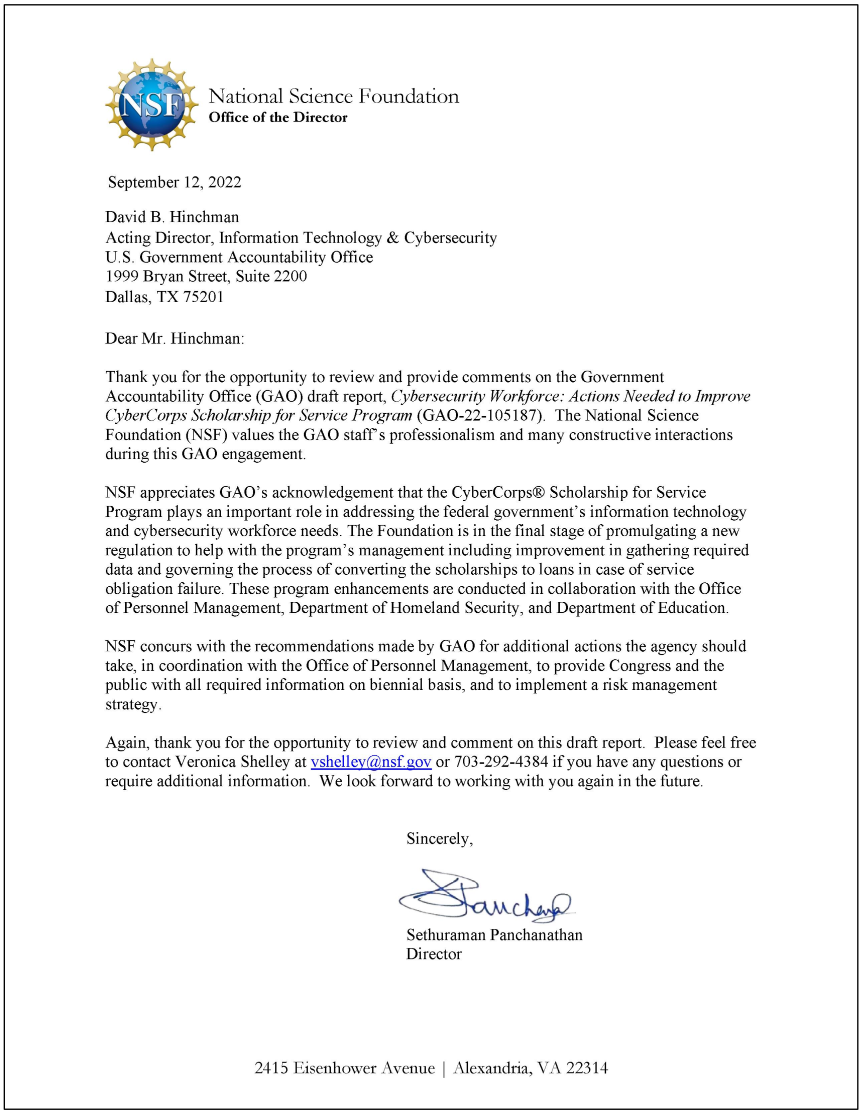
[k] OPM's excepted service flexibilities enable agencies to streamline hiring of recipients when it is not feasible or not practical to use traditional competitive hiring procedures. In the case of the SFS Program, excepted service allows scholarship recipients to obtain a competitive service job without competing with other applicants in open competition.

[l] Public Law No. 113-274.

[m] Scholarship recipient tracking challenges are those that relate to the SFS Program's inability to effectively track recipients from program entry until 8 years following the completion of their postgraduate work service obligation.

[n] COVID-19 challenges are those that relate to an increased inability for recipients to meet SFS Program requirements as a result of the pandemic.

Appendix V: Comments from the National Science Foundation



National Science Foundation
Office of the Director

September 12, 2022

David B. Hinchman
Acting Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
1999 Bryan Street, Suite 2200
Dallas, TX 75201

Dear Mr. Hinchman:

Thank you for the opportunity to review and provide comments on the Government Accountability Office (GAO) draft report, *Cybersecurity Workforce: Actions Needed to Improve CyberCorps Scholarship for Service Program* (GAO-22-105187). The National Science Foundation (NSF) values the GAO staff's professionalism and many constructive interactions during this GAO engagement.

NSF appreciates GAO's acknowledgement that the CyberCorps® Scholarship for Service Program plays an important role in addressing the federal government's information technology and cybersecurity workforce needs. The Foundation is in the final stage of promulgating a new regulation to help with the program's management including improvement in gathering required data and governing the process of converting the scholarships to loans in case of service obligation failure. These program enhancements are conducted in collaboration with the Office of Personnel Management, Department of Homeland Security, and Department of Education.

NSF concurs with the recommendations made by GAO for additional actions the agency should take, in coordination with the Office of Personnel Management, to provide Congress and the public with all required information on biennial basis, and to implement a risk management strategy.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact Veronica Shelley at vshelley@nsf.gov or 703-292-4384 if you have any questions or require additional information. We look forward to working with you again in the future.

Sincerely,

Sethuraman Panchanathan
Director

2415 Eisenhower Avenue | Alexandria, VA 22314

Text of Appendix V: Comments from the National Science Foundation

September 12, 2022

David B. Hinchman

Acting Director, Information Technology & Cybersecurity

U.S. Government Accountability Office 1999 Bryan Street, Suite 2200

Dallas, TX 75201

Dear Mr. Hinchman:

Thank you for the opportunity to review and provide comments on the Government Accountability Office (GAO) draft report, Cybersecurity Workforce: Actions Needed to Improve CyberCorps Scholarship for Service Program (GAO-22-105187). The National Science Foundation (NSF) values the GAO staff's professionalism and many constructive interactions during this GAO engagement.

NSF appreciates GAO's acknowledgement that the CyberCorps® Scholarship for Service Program plays an important role in addressing the federal government's information technology and cybersecurity workforce needs. The Foundation is in the final stage of promulgating a new regulation to help with the program's management including improvement in gathering required data and governing the process of converting the scholarships to loans in case of service obligation failure. These program enhancements are conducted in collaboration with the Office of Personnel Management, Department of Homeland Security, and Department of Education.

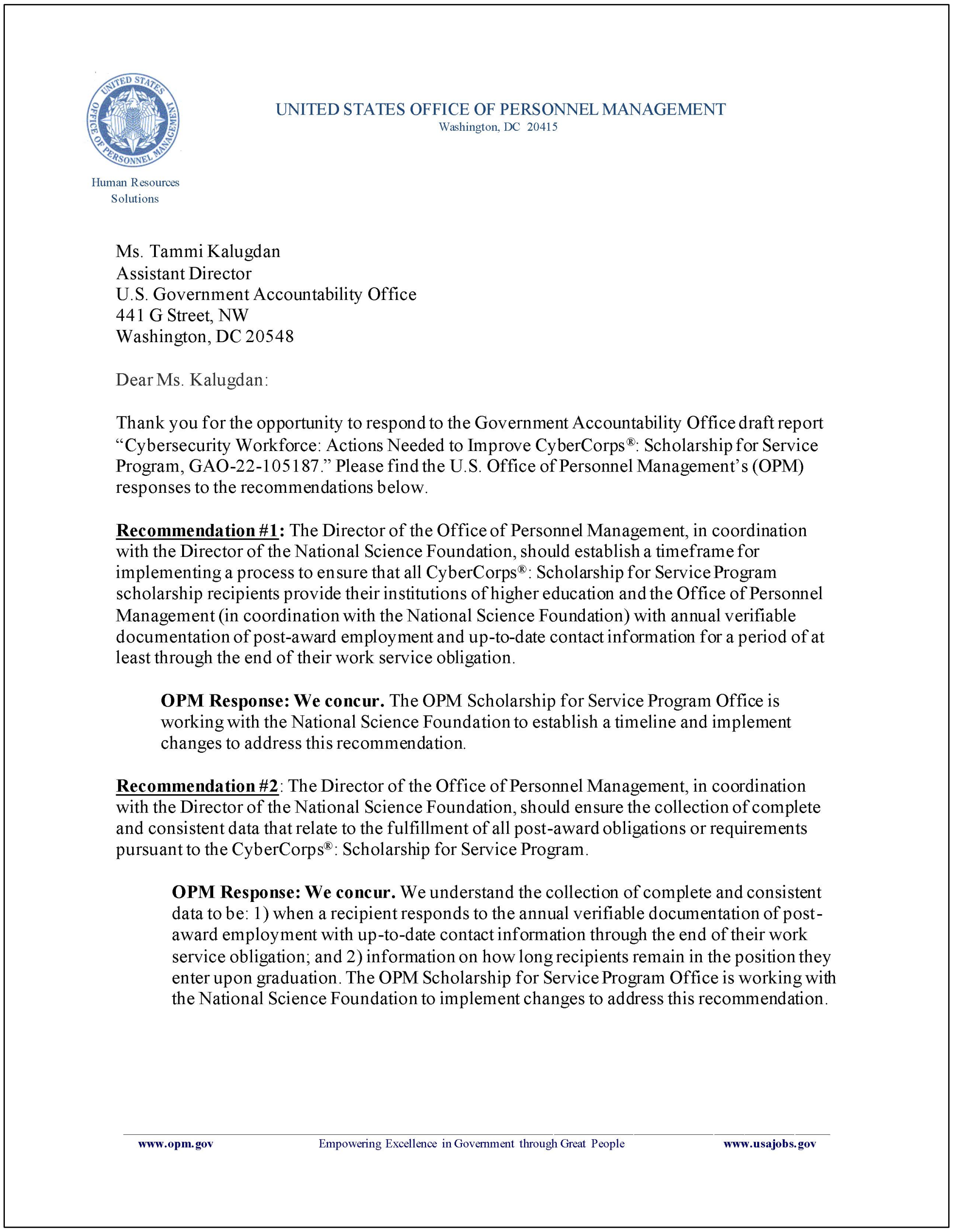
NSF concurs with the recommendations made by GAO for additional actions the agency should take, in coordination with the Office of Personnel Management, to provide Congress and the public with all required information on biennial basis, and to implement a risk management strategy.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact Veronica Shelley at vshelley@nsf.gov or 703-292-4384 if you have any questions or require additional information. We look forward to working with you again in the future.

Sincerely,

Sethuraman Panchanathan Director

Appendix VI: Comments from the U.S. Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Human Resources
Solutions

Ms. Tammi Kalugdan
Assistant Director
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Kalugdan:

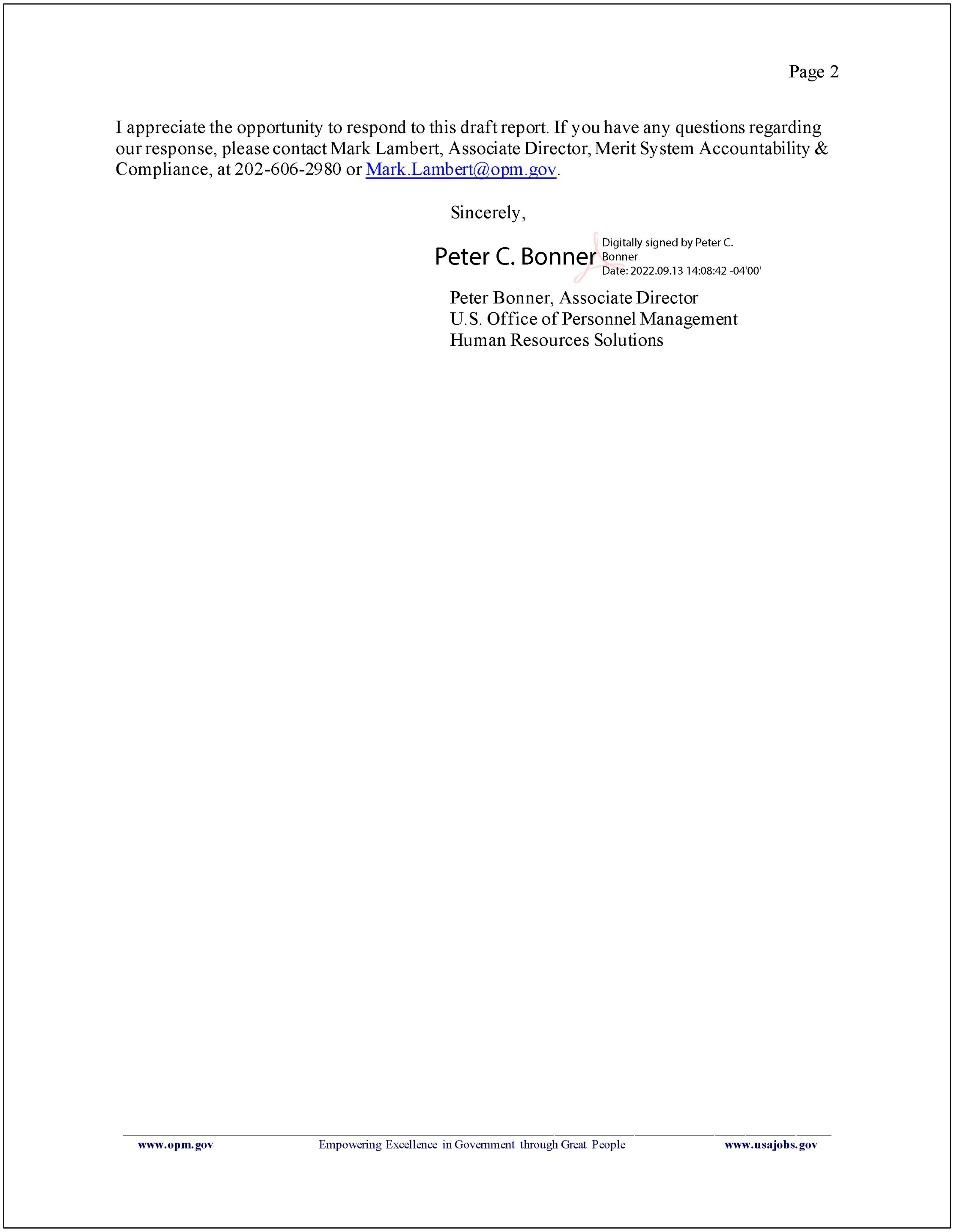
Thank you for the opportunity to respond to the Government Accountability Office draft report "Cybersecurity Workforce: Actions Needed to Improve CyberCorps®: Scholarship for Service Program, GAO-22-105187." Please find the U.S. Office of Personnel Management's (OPM) responses to the recommendations below.

Recommendation #1: The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should establish a timeframe for implementing a process to ensure that all CyberCorps®: Scholarship for Service Program scholarship recipients provide their institutions of higher education and the Office of Personnel Management (in coordination with the National Science Foundation) with annual verifiable documentation of post-award employment and up-to-date contact information for a period of at least through the end of their work service obligation.

> **OPM Response: We concur.** The OPM Scholarship for Service Program Office is working with the National Science Foundation to establish a timeline and implement changes to address this recommendation.

Recommendation #2: The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should ensure the collection of complete and consistent data that relate to the fulfillment of all post-award obligations or requirements pursuant to the CyberCorps®: Scholarship for Service Program.

> **OPM Response: We concur.** We understand the collection of complete and consistent data to be: 1) when a recipient responds to the annual verifiable documentation of post-award employment with up-to-date contact information through the end of their work service obligation; and 2) information on how long recipients remain in the position they enter upon graduation. The OPM Scholarship for Service Program Office is working with the National Science Foundation to implement changes to address this recommendation.



I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mark Lambert, Associate Director, Merit System Accountability & Compliance, at 202-606-2980 or Mark.Lambert@opm.gov.

Sincerely,

Peter C. Bonner Digitally signed by Peter C. Bonner
Date: 2022.09.13 14:08:42 -04'00'

Peter Bonner, Associate Director
U.S. Office of Personnel Management
Human Resources Solutions

Text of Appendix VI: Comments from the U.S. Office of Personnel Management

Ms. Tammi Kalugdan Assistant Director

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

Dear Ms. Kalugdan:

Thank you for the opportunity to respond to the Government Accountability Office draft report "Cybersecurity Workforce: Actions Needed to Improve CyberCorps®: Scholarship for Service Program, GAO-22-105187." Please find the U.S. Office of Personnel Management's (OPM) responses to the recommendations below.

Recommendation #1: The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should establish a timeframe for implementing a process to ensure that all CyberCorps®: Scholarship for Service Program scholarship recipients provide their institutions of higher education and the Office of Personnel Management (in coordination with the National Science Foundation) with annual verifiable documentation of post-award employment and up-to-date contact information for a period of at least through the end of their work service obligation.

OPM Response: We concur. The OPM Scholarship for Service Program Office is working with the National Science Foundation to establish a timeline and implement changes to address this recommendation.

Recommendation #2: The Director of the Office of Personnel Management, in coordination with the Director of the National Science Foundation, should ensure the collection of complete and consistent data that relate to the fulfillment of all post-award

obligations or requirements pursuant to the CyberCorps®: Scholarship for Service Program.

OPM Response: We concur. We understand the collection of complete and consistent data to be: 1) when a recipient responds to the annual verifiable documentation of post- award employment with up-to-date contact information through the end of their work service obligation; and 2) information on how long recipients remain in the position they enter upon graduation. The OPM Scholarship for Service Program Office is working with the National Science Foundation to implement changes to address this recommendation.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Mark Lambert, Associate Director, Merit System Accountability & Compliance, at 202-606-2980 or Mark.Lambert@opm.gov.

Sincerely,

Peter Bonner, Associate Director

U.S. Office of Personnel Management Human Resources Solutions

Appendix VII: GAO Contact and Staff Acknowledgments

GAO Contact

David B. Hinchman at (214) 777-5719, HinchmanD@gao.gov

Staff Acknowledgments

In addition to the contact listed above, the following staff made significant contributions to this report: Tammi Kalugdan (Assistant Director), Andrea Starosciak (Analyst-in-Charge), Joseph Andrews, Chris Businsky, Lilia Chaidez, Joseph Cook, Donna Epler, Hiama Halay, Corwin Hayward, Franklin Jackson, Colleen Phillips, Priscilla Smith, Andrew Stavisky, Walter Vance, Adam Vodraska, and Haley Weller.

(105187)

GAO’s Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO’s commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO’s email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO’s actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO’s website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548