Privacy Impact Assessment for

Scholarship for Service (SFS)

October 29, 2025

Contact Point
Joshua Chapman
System Owner
Scholarship For Services

Reviewing Official
Becky Ronayne
Senior Agency Official for Privacy

Abstract

The Scholarship for Service (SFS) system is a web application managed by the Office of Personnel Management's (OPM) Human Resources Solutions, Federal Staffing Center, Staff Acquisition, Student Program Services Branch. The SFS system serves government agencies, colleges, and universities, and students awarded the CyberCorps® SFS scholarship. SFS is a unique program designed to increase and strengthen the cadre of federal information assurance professionals that protect the government's critical information infrastructure. SFS is one of the three major OPM systems supported by the Macon General Support System (MCN GSS). This PIA is being conducted because the SFS system collects and maintains personally identifiable information provided by participating students, agency hiring officials from participating agencies, and representatives from participating academic institutions.

Overview

The overall purpose of this system is to administer, evaluate, and report on the Cybercops® program, which involves the awarding of scholarships to students enrolled in participating academic institutions and assuring they meet the SFS requirements.

The CyberCorps® program is managed by the National Science Foundation (NSF) in collaboration with OPM and the U.S. Department of Homeland Security. The program provides grants to academic institutions of higher education to give SFSs to students to support education in cybersecurity and related fields. A memorandum of understanding between NSF and OPM Human Resources Solutions authorizes and tasks OPM with providing the operational framework for the placement and tracking of scholars.

The goals of the CyberCorps® program are to: (1) increase the number of qualified cybersecurity candidates for government cybersecurity positions; (2) improve the national capacity for the education of cybersecurity

professionals and research and development workforce; (3) hire, monitor, and retain high-quality CyberCorps® graduates in the cybersecurity mission of Federal Government; and (4) strengthen partnerships between academic institutions of higher education and federal, state, local, and tribal governments.

The students who receive a SFS (scholars) are selected by participating academic institutions and then approved by OPM. While participating in the program, they are expected to keep their profile, resume, contact information, and internship and post-graduate commitment information updated in the system. Approved OPM and NSF staff who oversee the program (CyberCorps® program staff) use the system to monitor scholars' progress toward meeting the SFS requirements. Approved staff who work for the academic institutions where scholars are or were enrolled (academic institution officials) use the system to review some information about the scholars from their academic institution to help ensure they are meeting their SFS requirements. Approved individuals representing organizations where scholars can intern or work to meet their SFS requirements (agency hiring officials) use the system to review scholars' resumes to identify who might be interested and able to intern and work for their agency.

All scholars must meet the selection criteria established by their participating academic institution and the SFS eligibility requirements set forth in 15 U.S.C. 7442(f). They must agree to participate in meaningful summer internship opportunities or other meaningful temporary appointments in the Federal information technology and cybersecurity workforce during the scholarship period, and work for a period equal to the length of the scholarship after receiving their degree in a position related to cybersecurity as defined in 15 U.S.C. 7442(d). Additionally, scholars must agree to provide OPM (in coordination with NSF), and their academic institution, verifiable documentation of post-award employment and up-to-date contact information on an annual basis.

As required by 15 U.S.C. 7442, scholars are financially liable to the United States if they fail to meet the SFS requirements and do not receive a waiver or deferral. The system allows CyberCorps® program staff, and academic institution officials at the scholar's institution, to monitor scholars' progress toward meeting the requirements.

Section 1.0. Authorities and Other Requirements

1.1. What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Federal Cyber Scholarship-for-Service Program is authorized by section 302 of the Cybersecurity Enhancement Act of 2014, Public Law 113-274, 128 Stat. 2982, codified at 15 U.S.C. § 7442, and 45 C.F.R. § 620. The use of the Social Security Number (SSN) is also governed by E.O. 9397 as amended by E.O. 13478.

1.2. What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The applicable SORN is OPM/Internal—18, CyberCorps: Scholarship for Service (SFS) Records.

1.3. Has a system security plan been completed for the information system(s) supporting the project?

Yes. A system security plan has been completed for the system as part of the Authorization to Operate (ATO). The ATO's expiration date is August 30, 2027.

1.4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The SFS system has a records retention schedule approved by the National Archives and Records Administration. The records schedule number is DAA-0478-2014-0008.

1.5. If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

OMB has approved the collection of information by the SFS program and issued OMB Control Number 3206-0246, Scholarship For Service (SFS) Program Internet Site.

Section 2.0. Characterization of the Information

2.1. Identify the information the project collects, uses, disseminates, and maintains.

The SFS system automates the entire SFS registration process; some information is collected via mail or email. Information is collected and managed by program administrators.

The following information is collected from student participants: full name, SSN, date of birth, signature (written or digital), full address, phone number, email address, complete emergency contact information (first and last name, relationship, email address, and phone number), university/college attending, degree, funding information, field of study, expected graduation date, high school background, post-high school education background (high school state, high school type, current or former member of the U.S. Armed Forces, and years of employment), current certifications, cybersecurity employment information and history, resume information (users can either upload a resume or build one with the following fields (contact information from profile is included): objective, work experience, education, other qualifications (job-related training courses, job-related skills, job-related certificates/licenses, job-related honors, awards, memberships, etc., and supplemental information)), demographic information (gender, ethnicity, race), citizenship or permanent resident status, U.S. Armed Forces status, internship and post-graduation placement information (to include agency name, sub agency name, job title, salary range, and pay plan/series/grade), dates of employment, and required training information. In some situations,

program administrators may also collect from student participants deferral request information (including justification documentation) and/or discharge/waiver request information (including justification documentation).

The following information is collected from academic institution officials: full name, role, university/college, department/field, address, fax number, phone number, email address, institution's website, SFS grant award information, and institution demographics. In some situations, program administrators may also collect from academic institution officials funding disbursement details, funding disbursement information, and/or funding amounts (repaid and owed).

The following information is collected from agency hiring officials: agency name, sub-agency name, agency type, full name, agency address, work location, work phone number, work fax number, work email address, and agency website.

2.2. What are the sources of the information and how is the information collected for the project?

All information collected by the SFS system is submitted via the SFS website by individuals (students, agency hiring officials, or academic institution officials) with authenticated user identities and valid authorization credentials. All information received from the SFS web application is stored in the SFS database.

2.3. Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

The SFS program does not use information from commercial sources or publicly available data.

2.4. Discuss how accuracy of the data is ensured.

The individuals enter their information using the SFS website and therefore are responsible for the accuracy of the information. The SFS program asks

that schools confirm the accuracy of student information (excluding their SSN and demographic information) and recommends that the students review personal information annually. There are no other audits done by the SFS program to confirm data.

2.5. Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that the collected information may not be accurate and will affect an individual's ability to participate in the SFS Program or cause an agency to improperly place an individual.

Mitigation: This risk is mitigated by collecting the information directly from the individual who is interested in ensuring that the information is accurate. The SFS Program asks that the schools confirm the accuracy of student information (excluding their SSN and demographic information) and recommend that the students review personal information annually.

Privacy Risk: There is a risk that the SFS program may collect more information than is necessary to implement the SFS Program effectively.

Mitigation: This risk is mitigated by asking only for the information necessary for the SFS Program. If during review it is found that any unnecessary data is collected inadvertently it is manually redacted.

Section 3.0. Uses of the Information

3.1. Describe how and why the project uses the information.

Student information is used by approved OPM personnel to make updates in the system and facilitate the tracking of students to ensure they are meeting program requirements, to contact the student or their identified emergency contact as needed, to provide access to the student portal section of the SFS website, and to help the students acquire their required internships and post-graduation employment.

Student SSNs are encrypted at the time of registration and are only retrieved and used if the student defaults on their scholarship obligations. In those cases, OPM needs to send the student's information to the NSF for collection which may occur via their academic institution or the U.S. Department of the Treasury. SFS and OPM are not responsible for any further processing of the debt collection once the information has been sent to the NSF for initiation of the debt collection process.

Race and national origin data from students are collected and then stored in the aggregate for statistical purposes.

Contact information from academic institution officials and agency hiring officials are used by OPM for communications concerning their role in the SFS program. For example, academic institution officials are asked to review some information about the scholars from their academic institution to help ensure they are meeting their SFS requirements, while agency hiring officials are asked to review scholars' resumes to identify who might be interested and able to intern and work for their agency.

3.2. Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how OPM plans to use such results.

The SFS project does not use any technology to discover or locate a predictive pattern or anomaly.

3.3. Are there other programs or offices with assigned roles and responsibilities within the system?

Within OPM, SFS program staff, authorized SFS administrators, and the Office of the Chief Information Officer (OCIO) have access to the information in the SFS system. OCIO has access to the system to provide technical support (for example, to review audit logs and provide access information to the SFS program as necessary). No other offices within OPM are assigned

roles or responsibilities and the information is not otherwise shared within OPM.

3.4. Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the SFS program information may be used in a manner that is inconsistent with a user's specific mission area and authorities.

Mitigation: This risk is mitigated through the use of access controls that restrict user access to the information, based on authorization and access permissions in the system. The system maintains access roles for students, agency hiring officials, and investigators that restrict and grant access to information and functionality to support the appropriate need-to-know.

Section 4.0. Notice

4.1. How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

On the SFS website, a Privacy Act Statement is provided to each user when they input information on the website.

Notice is also provided to individuals when they log in regarding program information, the Full Terms and Conditions of Use posted on the site, and Rules of Behavior that they are required to accept before they are granted access. Through these documents, users are made aware of how their information is used to support the business process of the program.

4.2. What opportunities are available for individuals to consent to use, decline to provide information, or opt out of the project?

The program is strictly voluntary. If a student chooses to apply to the program, certain data elements are required in order to process the application for the program.

Once students choose to apply to the program and provide the required information, they cannot decline to consent to particular uses of their

information. Students are notified of the uses of their information through the Privacy Act Statement and the "Full Terms and Conditions of Use" available on the website and can decide not to participate in the program.

4.3. Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that individuals may not be afforded adequate notice about how their information is going to be used.

Mitigation: This risk is mitigated by providing the Privacy Act Statement at the point where the information is collected. It is also mitigated by providing users access when they login to the Full Terms and Conditions of Use, Rules of Behavior, and other OPM information on the SFS website that inform the users why their information is being collected and for what purpose.

Section 5.0. Data Retention by the Project

5.1. Explain how long and for what reason the information is retained.

In accordance with NARA Records Schedule Number DAA-0478-2014-0008, contact information for students is retained for 10 years and 3 months (DAA04 78-2014-0008-0001) after the student's completion of post-graduation commitment. Additional student information, and information about agency and academic institution officials is retained for 6 years (DAA-04 78-20140008-0002) after creation or upon fulfillment of service to the government, whichever is later.

5.2. Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that the SFS program will retain information for longer than is necessary.

Mitigation: This risk is mitigated by adhering to the applicable records schedule.

Section 6.0. Information Sharing

6.1. Is information shared outside of OPM as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

The SFS program is designed to share information with the students, academic institution officials, and agency hiring officials who are participating in the program, as well as with members of the public, as appropriate.

Students' contact information and resumes are available to approved agency hiring officials for use in recruitment and hiring in read-only access through a password-protected site. Student information is also made available in read only access to academic institution officials at the institution where the student attends.

In situations where a student requests to leave the program due to medical or hardship reasons, or in situations where waivers or deferrals of service obligation have been requested, student information, including name, academic institution, funding amounts, and justification documentation provided by the student, is shared with the NSF.

In situations where a student defaults on their scholarship obligation and goes into repayment status, student information, including name, academic institution, funding disbursement information, and student SSN are retrieved and provided to the NSF for collection, which may occur via their academic institution or the U.S. Department of the Treasury.

The names, university phone numbers, and university email addresses of academic institution officials are made available to the public with their approval as part of marketing the program.

The agency hiring officials' names, agency phone numbers, and agency email addresses are provided to approved students only when they state in

their registration that their contact information may be made available to participating students.

6.2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

The external sharing of SFS information described in Section 6.1 is consistent with the purposes stated in the OPM/Internal-18 SORN. The SORN contains Routine Uses that, permit the release of SFS information to academic institution officials to review resumes, employment information, education information, and contact information and to agency hiring officials to obtain information about scholars seeking employment.

j. To academic institution officials to ensure the information about the scholars from their institution is accurate. However, demographic information will not be released to academic institution officials.

k. To agency hiring officials so they can identify scholars who may be interested in interning or working at their organization. However, demographic information will not be released to agency hiring officials.

l. To the National Science Foundation (NSF) if the scholar requests a waiver or deferral of a service obligation so the NSF can determine whether to approve that wavier or deferral.

m. To academic institutions, the NSF, and the U.S. Department of the Treasury to recoup SFS payments made to scholars who do not complete their SFS requirements or receive permission to waive those requirements.

6.3. Does the project place limitations on re-dissemination?

The Rules of Behavior that the agency hiring officials are presented with at each sign in state that they will obtain, use, or disclose the information only in connection with the performance of their official duties and only for authorized purposes, and they will not disclose any information to other agencies or persons not expressly authorized to receive or have access to it.

6.4. Describe how the project maintains a record of any disclosures outside of OPM.

The SFS web application captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes. Audit record content includes, for all audit records: (i) the date and time of the event; (ii) the component of the information system where the event occurred; (iii) the type of event; (iv) subject identity; and (v) the outcome (success or failure) of the event.

6.5. Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the information in the SFS system will be shared for purposes other than the stated purposes of the SFS program.

Mitigation: This risk is mitigated by ensuring that the SFS information is available only to authorized users who have registered with and have been granted an account by the SFS program team. In addition, OPM technical personnel review and analyze application audit records weekly to ensure that information is accessed appropriately. This audit record review is documented. Agency hiring officials are also presented with SFS Rules of Behavior at each sign in.

Section 7.0. Redress

7.1. What are the procedures that allow individuals to access their information?

For students, agency hiring officials, and academic institution officials, the account registration process is initiated via an online form. Registration information is sent to the SFS Program Office. The Program Office representative is then able to approve and activate the account. After site registration has been approved, the requesting account user needs to create a Login.gov account, set their authentication methods, and link to their SFS email address used to register with the SFS site to sign into the SFS system and access any information they have submitted to the SFS system.

Government employees can also use their Personal Identity Verification (PIV) card or Common Access Card (CAC).

In addition, as noted in the OPM/Internal-18 SORN, individuals can obtain access to information about themselves in the SFS system by sending an email request to SFS@opm.gov or mail their request to the Office of Personnel Management, Office of the Executive Secretariat, Privacy, and Information Management - FOIA, 1900 E Street NW, OESPIM/FOIA Room 5H35, Washington, DC 20415-0001 and complying with OPM's Privacy Act regulations regarding verification of identity and access to records, available at 5 C.F.R. part 297.

7.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Agency and academic institution officials can access, correct, and update their information online.

Students can directly access and correct or update many data fields online. A limited number of fields in student records can only be changed by approved OPM personnel to ensure records remain accurate. For fields that cannot be changed directly by the user, the change can be made by sending a request to the SFS Program Office at SFS@opm.gov.

In addition, as noted in the OPM/Internal-18 SORN, individuals can request an amendment to their records by sending an email request to SFS@opm.gov or mail their request to the Office of Personnel Management, Office of the Executive Secretariat, Privacy, and Information Management - FOIA, 1900 E Street NW, OESPIM/FOIA Room 5H35, Washington, DC 20415-0001 and complying with OPM's Privacy Act regulations regarding verification of identity and access to records, available at 5 C.F.R. part 297.

7.3. How does the project notify individuals about the procedures for correcting their information?

Individuals are informed when they register with the SFS program that they may use their valid account information to access their information in the system and correct numerous data fields. For those data fields that the user is not permitted to update, users are informed that they may request a correction by contacting the SFS Program Office at SFS@opm.gov In addition, the OPM/Internal-18 SORN notifies individuals that they may request that information be corrected by contacting the SFS Program Manager.

7.4. Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not be afforded adequate opportunity to access their information and/or correct or amend erroneous or incomplete information.

Mitigation: This risk is mitigated because the SFS program allows users to update their information online via the SFS system. In addition, because a limited number of fields in the SFS records can only be changed by approved OPM personnel to ensure records remain accurate, the SFS Program Management Office may be contacted to request changes to the information. The SFS website provides points of contact for additional assistance. In addition, the applicable SORN sets out the procedure for individuals to access and amend information about them that is contained in the SFS system.

Section 8.0. Auditing and Accountability

8.1. How does the project ensure that the information is used in accordance with stated practices in the PIA?

The SFS system maintains access roles for students, agency hiring officials, and academic institution officials that restrict and grant access to information and functionality to support the business process need. The SFS

web application captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes.

OPM personnel review and analyze application audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

8.2. Describe what privacy training is provided to users either generally or specifically relevant to the project.

All OPM employees receive annual Security and Privacy Awareness training. There is no role-based training necessary to use the system.

8.3. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Students are only eligible to access the SFS system if a participating academic institution has awarded them a scholarship. Once the SFS program office is notified about the scholarship recipients, the students can register and are approved by the SFS program office to access their own information to view and make changes.

Only those academic institutions awarded an NSF grant may register with the SFS system. The registering academic institution officials must provide information to demonstrate to the SFS program office that they are actively working on the SFS program at that institution and be approved for access. Once approved, they have access to their data and read-only access to the data (excluding the SSN and demographic information) of students in the SFS program at their institution to track their progress through the program.

Agency hiring officials must provide email documentation that they are agency hiring officials with duties associated with recruiting and hiring cyber talent when they register. Once approved, they have read-only access to

student information (excluding SSN and demographic information) of students actively searching for employment.

OPM personnel who have access to the system must demonstrate a need-to know and be approved by the SFS Program Manager.

8.4. How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within OPM and outside?

Any new information-sharing agreements or MOUs and any new uses of the SFS information or new access to the SFS system must be approved by the SFS Program Manager in coordination with NSF and appropriate OPM offices.

Responsible Officials

Joshua Chapman
System Owner

Approval Signature

Becky Ronayne
Senior Agency Official for Privacy