Privacy Impact Assessment
for the

Scholarship for Service (SFS)

May 3, 2017

Program Owner
Erika Vega
Human Resources Solutions
Federal Staffing Center
Staff Acquisition Management Section

Reviewing Official
Kellie Cosgrove Riley
Chief Privacy Officer
Office of Personnel Management

OPM Form 5003

Abstract

The Scholarship for Service (SFS) system is a web application managed by the Office of Personnel Management's Human Resources Solutions, Federal Staffing Center, Staff Acquisition Management Section. 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. It is one of the three major U.S Office of Personnel Management (OPM) systems that the Macon General Support System (MCN GSS) supports. This PIA is being conducted because the SFS system collects and maintains personally identifiable information provided by participating students, agency officials from participating agencies, and representatives from participating academic institutions.

Overview

The Scholarship for Service (SFS) Program was established by the National Science Foundation (NSF), in coordination with the U.S. Office of Personnel Management (OPM) and the Department of Homeland Security (DHS), in accordance with the Cybersecurity Enhancement Act of 2014 (Public Law No: 113-274). This initiative reflects the critical need for Information Technology (IT) professionals, industrial control system security professionals, and security managers in Federal, State, local and tribal governments. Students identified by their institutions for SFS Scholarships must meet selection criteria based on prior academic performance, likelihood of success in obtaining the degree, and suitability for government employment. Upon graduation, scholarship recipients are required to work a period equal to the length of their scholarship in Federal, state, local or tribal government or in other approved organizations as cybersecurity professionals.

The purpose of the SFS system is to register scholarship recipient's contact information, education, and experience to allow OPM the ability to fulfill its responsibility of monitoring the students' progress and to provide this information to potential government employers. Students are elected by participating universities and colleges to receive the scholarship. Once selected and approved by OPM, the student is provided instructions on how to register their profile and resume on-line. Approved agency officials and approved academic institution officials are then able to retrieve resumes, including contact information, of the scholarship recipients through a password protected website. OPM restricts access to all of these records to only those OPM employees who are SFS program staff and authorized SFS Administrators. SFS administrators are responsible for establishing, activating, modifying, reviewing, disabling, and removing accounts. They also run reports to gain insight into the various aspects of the accounts.

A Memorandum of Understanding (MOU) between NSF and OPM authorizes and tasks OPM with providing the operational framework for the placement and tracking of students throughout the academic phase, post-graduation government employment obligation phase, and the retention phase.

The SFS website is an automated online application, located at http://www.sfs.opm.gov that collects and maintains information provided by participating students, agency officials from participating agencies, and representatives from participating academic institutions.

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 at15 U.S.C. § 7442.

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

The SFS system is covered by OPM INTERNAL-18 - Federal Cyber Service: Scholarship for Service (SFS) SORN, available at (http://www.ofr.gov/Privacy/2011/opm.aspx#int18).

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

Along with the system security plan, the SFS system was issued an Authorization to Operate (ATO) on April 12, 2017.

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

The SFS system does have 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.

Section 2.0 Characterization of the Information

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

The following information is collected for Student Participants: Full name, Social Security Number (SSN), signature, date of birth, Mother's maiden name, full address, phone number, email address, complete emergency contact information, university/college attending, degree funded, field of study, expected completion date, date available for internship, date available for post-graduation commitment, high school background, post high school education background, current certifications, cybersecurity employment information and history, resume information, demographic information (gender, ethnicity, race), US 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.

The following information is collected for agency officials: Agency name, sub agency name, full name, agency address, work location, work phone number, work fax number, work email address, and agency website.

The following information is collected for academic institution officials: Full name, university/college, department/field, address, fax number, phone number, email address, website, SFS award information, institution demographics.

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 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. 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 information that is collected 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 has an interest in ensuring that the information is accurate.

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. Student's social security numbers are encrypted at the time of registration and are only retrieved if the student defaults on his scholarship obligations and OPM needs to send the student's information to the Department of Treasury for collection. Race and national origin data is collected and then stored aggregately for statistical purposes.

Contact information from academic institution officials and agency officials is used by OPM for communications concerning the SFS program.

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 a tool to analyze the data within the application or to generate analytical reports.

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

Only SFS program staff and authorized SFS administrators have access to the information in the SFS system. No other offices 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 officials, and investigators that restrict and grant access to information and functionality to support the business process need.

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, there is a Privacy Act statement provided to each user when they input information on the website.

Notice is also provided to individuals via program information and Full Terms and Conditions of Use posted on the site, as well as Rules of Behavior. 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 uses, 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.

Students must consent to all uses of the information and cannot choose only certain uses. The student participation into the program is voluntary and the student is notified of the use of their information through "Full Terms and Conditions of Use" for the system. The student can decide not to participate in the program.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk:

There is a risk is 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 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 (DAA-04 78-2014-0008-0001) after the student's completion of post-graduation commitment. Additional student data, agency and academic institution officials is retained for 6 years (DAA-04 78-2014-0008-0002) 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 and periodic manual reviews performed by the Program Office.

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 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 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.

The names, University phone numbers, and University email addresses of academic institution officials are made available to the public with their approval.

The names, agency phone numbers, and agency email addresses of agency officials are provided to approved students only when the agency officials 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 - Federal Cyber Service: Scholarship for Service SORN. The SORN contains Routine Uses that specifically permit the release of SFS information to academic institution officials to review resumes and to agency officials to obtain information about students who are seeking employment.

6.3 Does the project place limitations on re-dissemination?

The Rules of Behavior that the agency officials are required to accept on a yearly basis states that they will obtain, use or disclose the data only in connection with the performance of their official duties solely for authorized purposes and they will not disclose any data 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 of the events. Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the

information system, where the event occurred; (iii) 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 been granted an account by the SFS program team. In addition, OPM technical personnel review and analyze application audit records to ensure that information is accessed appropriately and Agency Officials are also required to review and accept the SFS Rules of Behavior on an annual basis.

Section 7.0 Redress

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

For students, agency officials, and academic institution officials the account registration process is initiated via an online form. Registration information is sent to the SFS Program Manager. The Program Manager is then able to activate/approve the account. After the approval process, the requesting account user is able to gain access to the system using a valid login id and password and can access any information they have submitted to the system.

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

Agency officials and academic institution officials can directly access and 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.

In addition, as noted in the OPM INTERNAL-18 Federal Cyber Service: Scholarship for Service SORN, individuals can obtain access to information about themselves in the SFS system by sending a request to the OPM FOIA Officer at 1900 E Street, NW, Washington, DC 20415–7900 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 correction by contacting the SFS Program Office at SFS@opm.gov. In addition, the OPM INTERNAL-18 Federal Cyber Service: Scholarship for Service 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 provides users with the capability to update their information online via the SFS website. 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 this PIA?

The SFS system maintains access roles for students, agency 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 of the events.

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 which covers the process of handling PII related information. There are no role-based trainings 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 they have been awarded a scholarship by a participating academic institution. Once the SFS program office is notified about the scholarship recipients, the students can register and are approved by the SFS program office to have access only to their own information to view and make changes.

Only those academic institutions that have been 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) of students in the SFS program at their institution to track their progress through the program.

Agency officials must provide email documentation that they are an agency official with duties associated to recruiting and hiring at the time they register. Once approved, they have read-only access to student information (excluding SSN) 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.

Section 9.0 Responsible Officials

Erika Vega
Staff Acquisition Program Manager
HRS/CCS/FSG/SAB
U.S. Office of Personnel Management

Section 10.0 Approval Signature

Signed copy on file with the OPM Chief Privacy Officer.

Kellie Cosgrove Riley
Chief Privacy Officer
Office of Personnel Management