



## OFFICE OF PERSONNEL MANAGEMENT

[Docket ID: OPM-2025-0075]

### Privacy Act of 1974; System of Records

**AGENCY:** Human Resources Solutions (HRS), U.S. Office of Personnel Management.

**ACTION:** Notice of a modified system of records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Office of Personnel Management (OPM) proposes to modify and republish its existing system of records, titled “OPM/Internal—18, CyberCorps: Scholarship for Service (SFS) Records.” The overall purpose of this system is to administer, evaluate, and report on the CyberCorps® program, which involves the awarding of SFSs to students enrolled in participating academic institutions and assuring the students meet the SFS requirements. The students who receive an 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 National Science Foundation (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.

**DATES:** Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The modifications to this system are effective upon publication in the Federal Register, except for the new or modified routine uses, which are effective **[INSERT DATE 31 DAYS AFTER DATE OF PUBLICATION IN THE**

**FEDERAL REGISTER].**

**ADDRESSES:** You may submit written comments using the Federal eRulemaking Portal at <https://www.regulations.gov>. All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the internet at <https://www.regulations.gov> without change, including any personal identifiers.

**FOR FURTHER INFORMATION CONTACT:** Stephanie Travis, HR Consultant, Scholarship for Service Program, Office of Personnel Management, at [SFS@opm.gov](mailto:SFS@opm.gov).

**SUPPLEMENTARY INFORMATION:** In accordance with the Privacy Act of 1974, OPM proposes to modify the current system of records to more comprehensively monitor whether scholars are meeting their SFS requirements, to meet public reporting requirements set forth by law, and to limit collection to the information needed to operate the program. While minor and editorial changes and updates are being made throughout the notice, the most substantial changes are to the purpose(s) of the system, categories of individuals covered by the system, categories of records in the system, and routine uses.

The CyberCorps® program is managed by 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.

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.

Demographic data (e.g., sex, ethnicity, race) will not be released to agency hiring officials or academic institution officials and will only be released publicly in de-identified form.

In accordance with 5 U.S.C. 552a(r), OPM has provided a report of this modified system of records to the Office of Management and Budget and to Congress. This modified system of records will be included in OPM's inventory of record systems.

U.S. Office of Personnel Management.

**Jerson Matias,**

*Federal Register Liaison.*

**SYSTEM NAME AND NUMBER:** OPM/Internal—18, CyberCorps: Scholarship for Service (SFS) Records.

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Human Resources Solutions, Office of Personnel Management, Room 2469L, 1900 E Street NW, Washington, DC 20415-0001.

**SYSTEM MANAGER(S):** Associate Director, Human Resources Solutions, Office of Personnel Management, Room 2469L, 1900 E Street NW, Washington, DC 20415-0001.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 15 U.S.C. 7442, Federal Cyber Scholarship-for-Service Program, 45 CFR Part 620, CyberCorps® Scholarship for Service (SFS) Program, and E.O. 9397 as amended by E.O. 13478.

**PURPOSE(S) OF THE SYSTEM:** The purpose of this system is to administer, evaluate, and report on the CyberCorps® program. This includes: (a) enrolling students who receive a SFS (scholars) in the program; (b) connecting scholars to internships and post-graduate work opportunities; (c) tracking, managing, and monitoring scholars' progress and compliance with the SFS requirements; (d) recouping payments from scholars who do not fulfill the SFS requirements or receive a waiver; (e) analyzing and reporting CyberCorps® program results, to ensure the program aligns with cybersecurity workforce development goals and Federal Government needs; and (f) managing access to the system.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** The categories of individuals whose information may be included in the system are: (a) scholars; (b) approved staff who work for the academic institutions where the scholars are located and are responsible for helping to ensure the scholars from their institution are meeting the SFS requirements (academic institution officials); (c) approved individuals representing organizations where scholars can intern or work to meet their SFS requirements (agency hiring officials); and (d) approved U.S. Office of Personnel Management (OPM) and National Science Foundation staff who oversee the CyberCorps® program (CyberCorps® program staff):

## **CATEGORIES OF RECORDS IN THE SYSTEM:**

- **Scholars:** The records in the system may include their full name(s), Social Security Number, signature, date of birth, contact information, emergency contact information, academic institution where enrolled, degree funded, funding start and end dates, field of study, expected completion date, date available for internship, date available for post-graduation commitment, education history, current certifications, employment history (including a resume), demographic information (e.g., sex, ethnicity, race), citizenship or permanent resident status, US armed forces status, internship and post-graduation placement information (including the agency name, sub agency name, job title, salary range and pay plan/series/grade, dates of employment and required training information), and supporting documentation. The records may include requests to defer or waive their SFS requirements, justification for that request, and the outcome. The records may also include how a scholar has not met their SFS requirements and how they are repaying their SFS.
- **Academic Institution Officials:** The records in the system may include their full name(s), role, title, academic institution, department/field, contact information, and website. The records may also include information about their institution's CyberCorps® grant and other publicly available information about their institution.
- **Agency Hiring Officials:** The records in the system may include their full name(s), agency name, sub agency name, agency type, agency address(s), work contact information, and agency website.
- **CyberCorps® Program Staff:** The records in the system may include their name, email, username for the electronic system used to facilitate their access to the information in this system, and information about their access to the records in that electronic system.

**RECORD SOURCE CATEGORIES:** Information in this system of records is obtained from scholars, academic institution officials, agency hiring officials, and CyberCorps® Program Staff.

## **ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING**

**CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, the records in this system may be disclosed outside OPM as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

- a. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body, when OPM or another agency representing OPM determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
- b. To the Department of Justice when (a) OPM, or any component thereof; (b) any OPM employee in their official capacity; (c) any OPM employee in their individual capacity where the Department of Justice has agreed to represent the employee; or (d) the United States, where OPM determines that litigation is likely to affect OPM or any of its components, is a party to litigation or has an interest in such litigation, and the use of such records by the Department of Justice is deemed by OPM to be relevant and necessary to the litigation.
- c. Where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law – criminal, civil, or regulatory in nature – the relevant records may be referred to the appropriate federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law.
- d. To a member of Congress or staff acting upon the member's behalf, when the member or staff requests the information on behalf of, and at the request of, the individual to whom the record pertains.
- e. To the National Archives and Records Administration (NARA) for records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

- f. To appropriate agencies, entities, and persons when (1) OPM suspects or has confirmed that there has been a breach of the system of records, (2) OPM has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, OPM (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with OPM's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
- g. To another Federal agency or Federal entity, when OPM determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.
- h. To contractors, grantees, experts, consultants, or volunteers performing or working on a contract, service, grant, cooperative agreement, or other assignment for OPM to the extent necessary to accomplish an agency function related to this system of records.
- i. 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.
- j. 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.
- k. 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 waiver or deferral.
- l. 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.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** The records may be retrieved by name and email address.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** The SFS Program has a Records Retention Schedule, DAA-0478-2014-0008, approved by NARA. Certain records about a scholar must be retained for at least 10 years and 3 months after that scholar completes their post-graduation commitment. All other information must be retained for at least 6 years after creation or upon fulfillment of service to the government, whichever is later.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** Records in this system are protected from unauthorized access and misuse through various administrative, technical, and physical security measures in accordance with its Automated Information Systems Security Program. All these security measures comply with the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014, OMB policies, and standards and guidance from the National Institute of Standards and Technology. For example, access to records is limited to individuals who need the information to perform their official duties and have appropriate clearances or permissions.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to their records in this system may email their request to [foia@opm.gov](mailto:foia@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. The email or letter should:

1. Include the words “Privacy Act Records Access Request”,
2. State that the request relates to “OPM/Internal—18, CyberCorps: Scholarship for Service (SFS) Records,” and
3. Clearly describe the information requested.

The letter or email must also include the individual's:

1. Full name, and any former names,
2. Date of birth,
3. Preference for how they want to be contacted (home address, telephone number, and/or personal email), and
4. Signature.

Additional requirements regarding record access requests, including the rights of guardians and how records may be provided, may be found in 5 CFR Part 297, Privacy Procedures for Personnel Records.

**CONTESTING RECORD PROCEDURES:** Individuals wishing to request an amendment of records about them may email their request to [foia@opm.gov](mailto:foia@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. The email or letter should:

1. Include the words "Privacy Act Amendment Request",
2. State that the request relates to "OPM/Internal—18, CyberCorps: Scholarship for Service (SFS) Records,"
3. Clearly describe the records the individual wants to amend and why, and
4. Include any documents which could help substantiate the request.

The letter or email must also include the individual's:

1. Full name, and any former names,
2. Date of birth,
3. Preference for how they want to be contacted (home address, telephone number, and/or personal email), and
4. Signature.

Additional requirements regarding record access requests, including the rights of guardians and how records may be provided, may be found in 5 CFR Part 297, Privacy Procedures for Personnel Records.

**NOTIFICATION PROCEDURES:** See “Record Access Procedures.”

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** 79 FR 42064 (July 18, 2014) and 87 FR 5874 (February 2, 2022).

[FR Doc. 2025-13362 Filed: 7/16/2025 8:45 am; Publication Date: 7/17/2025]