UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

System of Records Notice (SORN) Guide

This document implements the OPM Information Security and Privacy Policy

Chief Information Officer (CIO)

April 2010

A New Day for the Civil Service

Table of Contents

REVISION HISTORY

Version Number	Version Date	Revision Summary
1.0	April 2010	Initial Release

EXECUTIVE SUMMARY

The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of records maintained on individuals. The Act (5 U.S.C. 552a) regulates the collection, maintenance, use, and dissemination of records about individuals that are retrieved by personal identifier and collected, used or disseminated by agencies and departments of the executive branch, including OPM. To ensure compliance with the Federal requirements, agencies must foster an environment conducive to the protection of personal privacy within their organization.

The Privacy Act also mandates the publishing of system of records notices (SORNs) for newly created and revised systems of records. Since its enactment, Office of Management and Budget (OMB) memoranda have provided additional guidance on the interpretation of the Privacy Act.

This guide assists OPM program offices in determining if their systems of records are subject to the Privacy Act of 1974, as amended. It contains instructions on how to draft the appropriate SORN to publish in the Federal Register, how to complete letters and narrative statements for Congress and the Office of Management and Budget (OMB) if needed, and how to obtain OPM approval for draft SORNs before publication.

The version of this document that is posted to the Web is the official, authoritative version.

1. POLICY STATEMENT

It is Office of Personnel Management (OPM) policy to publish a system of records notice (SORN) in the Federal Register for any agency-maintained information technology (IT) system or paper file system that contains information on individuals and retrieves the information by a personal identifier. It is OPM policy to publish a system of records notice in the Federal Register before periodically reviewing existing systems of records and the published notices that describe them to ensure that they are accurate and to complete and publish notices in the federal register for all new or revised systems of records.

2. INTRODUCTION

2.1 Purpose

This guide is designed to assist OPM program offices in determining if their systems of records are subject to the Privacy Act of 1974, as amended. The guide also contains instructions on how to draft the appropriate SORN to publish in the Federal Register, and how to complete letters and narrative statements for Congress and the Office of Management and Budget (OMB) concerning the creation of a new system of records or the significant alteration to or termination of an existing system of records.

SORNs have the following purposes:

- To identify the purpose of a system of records.
- To identify which individuals are covered by information in a system of records.
- To identify the categories of records that are maintained about the individuals.
- To identify how the information is shared by the agency (routine uses).[1]
- To inform the public of the existence of records.
- To provide notice to the public of their rights and procedures under the Privacy Act for accessing and correcting information maintained by the agency on an individual.[2]

Whenever a Federal agency maintains information about an individual in a system of records and retrieves the information by a personal identifier, it must publish a SORN in the Federal Register.[3]

2.2 Scope and Applicability

This guide covers how to identify a system of records, what are the components of a system of records, and how to draft and publish a SORN and supporting documentation (which consists of a narrative statement and letters to Congress and OMB), if needed.

Anyone who is involved in the SORN process at OPM must know and adhere to the policies and procedures in the SORN Guide. If you are seeking information on OPM's privacy policies in

[1] 5 U.S.C. 552a(a)(5).
[2] 5 U.S.C. 552a(a)(5).
[3] 5 U.S.C. 552a(e)(4); 5 U.S.C. 552a(5); see OMB Circular A-130, Appendix I, 4(c).

general, please see the most recent version of the Information Security and Privacy Policy, available on the OPM intranet.

2.3 Legal Authority

OPM developed the SORN Guide to comply with the laws and guidance listed below:

- Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub. L. 93-579.
- OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, Appendix I.
- OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records"
- Privacy Act Implementation, Guidelines and Responsibilities, July 9, 1975.

2.4 Maintenance of the Official Version

The SORN Guide will be modified as appropriate to ensure it remains current with the following:

- Release of new executive, legislative, or technical policy or guidance.
- Changes in vulnerabilities, risks, or threats.
- OPM Inspector General (IG) findings stemming from audits.
- Changes to OPM's Information Security and Privacy Policy.

The OPM CIO reviews and approves all revisions to the SORN Guide. Once approved, a new version of the SORN Guide will be published on the OPM intranet.

3. SYSTEM OF RECORDS NOTICES (SORNs)

3.1 Requirements of the Privacy Act

A SORN **is required** when all of the following apply:

- Records are maintained[4] by a Federal agency.
- The records contain information about an individual[5].
- The records are retrieved by a personal identifier.

[4] Maintain as defined by the Privacy Act of 1974 includes maintain, collect, use or disseminate.

[5] Individual as defined by the Privacy Act of 1974 means a citizen of the United States or an alien lawfully admitted for permanent residence.

A SORN **is not required** when one or more of the following applies:

- The information collected is not considered a record as defined by the Privacy Act.
- The records are not retrieved using a personal identifier.

3.2 Retrieved by Personal Identifier

To be considered a system of records within the meaning of the Privacy Act, records that OPM maintains must be retrieved by a person's name or other personal identifying information (referred to as a "personal identifier"). A personal identifier might include an individual's name, address, email address, telephone number, social security number, photograph, biometric information, or any other unique identifier that can be linked to an individual. This means the requirements mandated by the Privacy Act are not applicable to OPM records unless the records are retrieved by a personal identifier.

Mere maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to trigger the conduct of a privacy impact assessment (PIA). For information on how to conduct a PIA, see the Privacy Impact Assessment Guide on the intranet at http://theo.opm.gov/policies/ispp/index.asp.

To trigger the SORN requirements of the Privacy Act, information must actually be retrieved by a personal identifier.

As an example, let's assume OPM operates a visitor management system. The system stores information about individuals by name and date of arrival at OPM, but the system retrieves information only by date of arrival at OPM. Under these circumstances, the visitor management system is not a system of records under the Privacy Act. However, if the system retrieved information by an individual's identifying information; it would qualify as a system of records under the Privacy Act.

Most IT systems are designed to make records management and retrieval more efficient and less time consuming than a paper file system. In today's IT environment, most systems are designed to retrieve records by multiple identifiers, including by personal identifier.

It is important to note that any time an agency retrieves material from a system of records by personal identifier; the requirements of the Privacy Act apply, regardless of whether the records are electronic or paper.

3.3 Systems of Records Classifications

OPM classifies systems of records into three classifications: internal, Governmentwide, and central. Each classification is explained below.

a. Internal: Internal systems of records are records created within OPM for its employees or

administrative duties or mission (e.g., security files). The following characteristics also apply:

- The systems of records are owned by the agency to cover its internal records.
- The corresponding SORNs are often referred to as "umbrella" system notices.

b. Governmentwide: Governmentwide systems of records are records for which OPM writes the policy but does not have physical custody as a matter of necessity (e.g., general personnel records). Federal agencies may use Governmentwide SORNs to cover Governmentwide records systems. The following characteristics also apply:

- The physical records contained within the system of records belong to the respective agency.
- OPM still retains some authority over the records.
- The corresponding SORNs begin with the identifier GOVT-1, 2, etc.

c. Central: Central systems of records are records for which OPM writes the policy and actually has physical custody (e.g., retirement records). Federal agencies are permitted to maintain copies. The following characteristics also apply:

- The corresponding SORNs are owned by OPM, which maintains full responsibility for the central systems of records.
- Notices begin with the identifier CENTRAL-1, 2, etc.

3.4 Do I Need to Create a New SORN or Amend an Existing SORN?

Appendix I to OMB Circular No. A-130, Federal Agency Responsibilities for Maintaining Records About Individuals serves as the baseline for distinguishing between the criteria for drafting a new SORN versus amending an existing SORN.

3.4.1 Criteria for Creating a New SORN

A "new" system of records is one for which no public notice is currently published in the Federal Register. A new SORN must be published when any one of the following criteria is met:

- A program, authorized by a new or existing statute or Executive order (EO), maintains information on an individual and retrieves that information by personal identifier.
- There is a new organization of records resulting in the consolidation of two or more existing systems into one new umbrella system, whenever the consolidation cannot be classified under a current SORN.
- It is discovered that records about individuals are being created and used, and that this activity is not covered by a currently published SORN. In this case, OMB requires the temporary suspension of data collection and disclosure.

- A new organization (configuration) of existing records about individuals that was not previously subject to the Privacy Act (i.e., was not a system of records) results in the creation of a system of records.

The SORN must appear in the Federal Register for a 30-day comment period before the agency begins to operate the system to collect and use the information. The agency must also send letters and a narrative statement to OMB and Congress explaining the need for the new system of records. OMB and Congress require an additional 10 days to review the request, resulting in a total waiting period of 40 days before the agency begins to operate the system to collect and use the information . Although it is not a requirement of the Privacy Act, it is OPM policy to publish a 40 day SORN to encompass all requirements. See appendix F for a sample new SORN.

3.4.2 Criteria for Amending an Existing SORN[6]

There are two types of amendments to SORNs: a significant alteration and a nonsignificant alteration.

If a significant alteration needs to be made to a system of records, the agency must immediately amend the existing SORN for that system of records and republish it in the Federal Register for a 30-day public comment period. Significant alterations also require the agency to send letters and a narrative statement to OMB and Congress explaining the alterations before the agency can begin to operate the system to collect and use the information. OMB and Congress require an additional 10 days to review the request, resulting in a total waiting period of 40 days before the agency begins to operate the system to collect and use the information. Although it is not a requirement of the Privacy Act, it is OPM policy to publish a 40 day SORN to encompass all requirements.
Note: The proposed alterations to the existing system of records should be provided in the SUPPLEMENTARY INFORMATION in the introductory section of the notice and the complete modified SORN should follow in its entirety.

Significant alterations include:

- **Change in the number or type of individuals on whom records are maintained**. (Changes that involve the number, rather than the type, of individuals about whom records are kept need to be reported only when the change alters the **character and purpose** of the system of records.)
- **Expansion of the types or categories of information maintained**. For example, if an employee file is expanded to include data on education and training, this is considered an expansion of the types or categories of information maintained.
- **Change in the manner in which the records are organized, indexed, or retrieved that results in a change in the nature or scope of these records**. Examples are splitting an existing system of records into two or more different system of records, which may occur in centralization or a decentralization of organizational responsibilities.

[6] OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals, Appendix I.

- **Change in the purpose for which information in the system of records is used**.
- **Change in equipment configuration**. This means changing the hardware or software on which the system of records operates to create the potential for either more or easier access.
- **Change in procedures associated with the system in a manner that affects an individual's exercise of his or her rights**.

For systems with nonsignificant alterations, such as a change in system owner, the only requirement is that a revised SORN be published in the Federal Register. The 30-day public comment period and 10 additional day OMB and Congress review period is not required for nonsignificant alterations.

Please consult the OPM Privacy Act Officer for a final determination of the nature of any changes to a system of records.

3.5 How to Terminate an Existing System of Records

A system of records is considered to be terminated whenever the information is no longer accessed by individuals' names or other identifiers, or whenever it is consolidated with another system of records. Terminating a system may involve the physical destruction of records; it may involve purging the system of individual identifiers and maintaining the data in another form, such as statistical data; and it may involve altering the manner in which the records are accessed so that records are no longer accessed by the name of the subject individuals or other personal identifiers. Because records retired to a Federal Records Center (FRC) are still under the control of OPM, the act of retiring an inactive system to the FRC does not in itself constitute termination of the system. Though it is not a requirement of the Privacy Act, it is OPM policy that a terminated system of records requires a notice to be published in the Federal Register announcing the termination.

See appendix H for a sample terminated SORN.

3.6 How to Draft and Publish a SORN[7]

SORNs must be clear, unambiguous, and understandable to the general public while fulfilling the necessary legal requirements of the Privacy Act. The publication requirements of the SORN are intended to:

1. Prevent the creation of a system of records without first giving individuals an opportunity to review and comment on the purpose and routine uses for which their information is collected.
2. Help individuals locate systems of records that are likely to contain information pertaining to them.

[7] Federal Register Document Drafting Handbook

3.6.1 Drafting Guidelines

The following guidelines should be followed when drafting a SORN:

- *Remember the audience.* The SORN must be written in a manner that allows the public to understand the system of records being described.
- *Ensure the SORN contains no spelling or grammatical errors.* SORNs are published in the Federal Register and on OPM's Web site. SORNs submitted to the Privacy Program Manager must be free of spelling and grammatical errors.
- *Expand acronyms.* Spell out each acronym the first time it is used in the document. For example: Office of Management and Budget (OMB). Do not use acronyms in the summary of the notice.
- *Use plain English.* Use words, phrases, and names that are readily known to the average person.
- *Define technical terms and references.* Keep in mind that readers may not understand technical terms when they are introduced without definition.
- *Cite legal references and other previously published documents.* References to other programs and systems require explanations so the general public can gain a complete understanding of the context of the program or system. If a document pertaining to the SORN has previously been published in the Federal Register, provide the citation and, if possible, a very brief description of the document type (e.g., system of records notice, statute, or final or proposed rule). Use the complete name of reference documents. For example: National Institute of Standards and Technology (NIST) Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
- *Use active voice.* Ensure the SORN employs active voice rather than passive voice whenever possible. Also, use short and simple sentences whenever possible to improve clarity.

3.7 OPM SORN Approval Process

Before drafting a SORN, all program offices must contact the OPM Privacy Act Officer to discuss appropriate routine uses for the system, and generally to coordinate OPM Privacy Act efforts.

Step 1. The system owner drafts the SORN, narrative statement, and letters to OMB and Congress, if needed, and creates a SORN submission package in the OPM Document Management System (DMS). The system owner routes the package to the following offices for approval:

- Associate Director of his or her division
- Office of the Chief Information Officer
- Office of Congressional Relations (for new or amended SORNs)
- Office of General Counsel
- Office of the Director

- Facilities, Security, & Contracting, Publications Management Group

Step 2. The OPM Privacy Program Manager, located in the Office of the Chief Information Office, reviews all SORNs, narrative statements, and letters to OMB and Congress, and recommends approval to the CIO.

Step 3. Once the CIO approves the package, it is routed to the Office of General Counsel (OGC) for approval. (Note: If the package represents a new or significantly altered SORN, the Office of Congressional Relations (OCR) needs to approve the letters and narrative statements to Congress and OMB before they are routed to OGC.)

Step 4. Once OGC approves the package, it is routed to the Director for signature. (Note: If OGC proposes changes, the package passes back to the system owner for revision and changes recommended by OGC.)

Step 5. Once the Director signs the SORN package, it is routed to the Publications Group for publishing in the Federal Register[8]and to OCR for submission to Congress and OMB.

Step 6. The public has 30 days to comment and OMB and Congress have 10 days to review and comment on the SORN and the system owner must record and respond to the comments.

Step 7. Once the SORN is published it will be posted to the OPM.GOV Web site by the Privacy Act Officer.

4. COMPLIANCE, ENFORCEMENT, AND EXCEPTIONS[9]

Compliance with the OPM SORN Guide is mandatory. Enforcement and monitoring of this policy is the responsibility of the Chief Information Officer (CIO). The CIO continually reviews and monitors the status of OPM's SORNS by monitoring:

- Compliance with the Information Security and Privacy Policy, procedures, standards, and guidelines.
- User awareness of the SORN Guide policies.
- Active adoption of the OPM SORN Guide requirements.

The OPM Office of the Inspector General (OIG) conducts independent audits to examine and evaluate OPM’s compliance with the SORN Guide. The OIG provides the results to the CIO. The CIO submits the results of these audits in an annual report to OMB outlining OPM’s SORN status and ongoing activities.

Violations of the policy contained in the SORN Guide may result in the loss or limitation of access to OPM information systems and information. Anyone who violates the policy also may face administrative action ranging from counseling to removal from the agency, as well as

[8] OMB Circular A-130, Appendix I, 4 (c) through (e) and 5.

[9] OPM Information Security and Privacy Policy.

criminal penalties or financial liability, depending on the severity of the misuse. In addition, all OPM employees and contractors are subject to penalties established by the Privacy Act of 1974. Certain penalties apply to the misuse or unauthorized disclosure of personally identifiable information. The Act (5 U.S.C. 552a(g)) provides for civil remedies for injured parties, including actual damages, attorney fees, and litigation costs. The Act (5 U.S.C. 552a(i)(1)(2)(3)) also provides for criminal penalties of up to $5,000 for Government employees and contractors, as follows:

(1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

A policy violation is an **infringement or nonobservance of OPM policy**. OPM employees who suspect policy violations must report them to their OPM supervisors, managers, associate directors, or office directors, as appropriate. Contractors must report suspected violations to their contracting officer's technical representative.

There are no exceptions to the SORN process. However, certain exemptions to the Privacy Act can be claimed, as listed in appendix D.

5. ROLES AND RESPONSIBILITIES

Persons in the positions identified in this section have a role in or are directly responsible for the development and completion of system of records notices (SORNs) at OPM. Coordination among these roles is essential for the successful completion of a SORN.

5.1 OPM Director

The OPM Director is responsible for reporting each new or significantly altered system of records to appropriate Federal agencies (which will normally include the Office of Management and Budget (OMB), U.S. Senate, and House of Representatives) and for signing the final SORN before publication in the Federal Register.

5.2 Chief Information Officer (CIO)

Responsibilities of the Chief Information Officer (CIO) include:

- Overseeing the privacy program.
- Ensuring that all SORNs, narrative statements, and congressional and OMB letters are ready for review by the Office of General Counsel and the Office of the Director.

5.3 Privacy Program Manager

Responsibilities of the Privacy Program Manager include:

- Reviewing SORNs, narrative statements, and congressional and OMB letters before they are published in the Federal Register and ensuring that SORNs meet the requirements of the Privacy Act.
- Detailing the process for developing, approving, publishing, and maintaining a master inventory of SORNs.
- Determining if a SORN is adequately represented in a privacy impact assessment (PIA).
- Assigning identifiers and numbers to new systems of records.

5.4 Privacy Act Officer

Responsibilities of the Privacy Act Officer include:

- Assisting system owners with drafting a SORN for all new, significantly altered, and terminated systems of records.
- Assisting system owners with drafting the appropriate narrative statement and congressional and OMB letters, in consultation with the Privacy Program Manager.
- Publishing SORNs on the OPM.gov Web site.
- Ensuring that the OPM inventory of SORNs is kept up to date.

5.5 Information Technology Security Officer (ITSO)

The Information Technology Security Officer (ITSO) is responsible for ensuring that automated systems of records have appropriate system safeguards as part of the certification and accreditation (C&A) package.

5.6 Office of Congressional Relations (OCR)

The Office of Congressional Relations (OCR) is responsible for reviewing congressional and OMB letters and sending them electronically to the appropriate officials.

5.7 Office of General Counsel (OGC)

The Office of General Counsel (OGC) is responsible for advising agency officials on compliance with applicable laws, regulations, and other controlling authorities and clearing all SORNs for publication in the Federal Register.

5.8 OPM Records Officer

The OPM Records Officer, who reports to the CIO, is responsible for collaborating with the system owner to develop an approved records schedule for each system of records with the National Archives and Records Administration (NARA).

5.9 Publications Management Group

Responsibilities of the Publications Management Group include:

- Publishing the final signed SORN in the Federal Register.
- Notifying the Privacy Program Manager of the SORN publication date and page number.

5.10 System Owners

Responsibilities of system owners include:

- Collaborating with the Privacy Act Officer to draft a SORN for each new, significantly altered, and terminated system of records throughout the life cycle of the system.
- Collaborating with the OPM Records Officer to develop an approved records schedule with NARA.
- Drafting the appropriate congressional and OMB letters and narrative statements in consultation with the Privacy Act Officer for all new and significantly altered systems of records.
- Disposing of and retaining each system of records in accordance with the appropriate records schedule.
- Addressing comments from the public during the mandatory 30-day comment period in the Federal Register and 40 day OMB and Congress review period and amending the SORN if necessary.
- Notifying the Privacy Program Manager of any alterations in the system that may affect the SORN, as applicable and foreseeable.

APPENDIX A: ACRONYM LIST

Acronym	Expansion
C&A	certification and accreditation
CFR	Code of Federal Regulations
FISMA	Federal Information Security Management Act
FRC	Federal Records Center
IT	information technology
ITSO	Information Technology Security Officer
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NPRM	Notice of Proposed Rulemaking
OCR	Office of Congressional Relations
OGC	Office of General Counsel
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	privacy impact assessment
SORN	system of records notice

APPENDIX B: GLOSSARY

control: Records are considered to be under the control of an agency if they are maintained by or on behalf of the agency. (Source: 5 U.S.C. 552a(e).) The control requirement establishes accountability for the Privacy Act provisions and OMB Privacy Act Implementation Guidelines and Responsibilities. (Source: 40 FR 28952.)

Federal Register: Official daily publication for rules, proposed rules, notices of Federal agencies and organizations, and Executive orders and other presidential documents.

individual: A citizen of the United States or an alien lawfully admitted for permanent residence. (Source: 5 U.S.C. 552a(a)(2).)

maintain: includes maintain, collect, use, or disseminate a record. (Source: 5 U.S.C. 552a(a)(3).)

nonsignificant alteration: Change or revision to an existing system of records that is not classified as a significant alteration. (Source: OMB Circular A-130

personal identifier: Individual's name, address, email address, telephone number, social security number, photograph, biometric information, or other unique identifier that can be linked to an individual. (Best practice expansion from 5 U.S.C. 552a(a)(5).)

privacy impact assessment (PIA): Analysis of how information is handled to:

1. Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
2. Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.
3. Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

(Source: OMB Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.)

record: Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history that contains his name, or other identifying particular assigned to the individual" (address, fingerprint, voice print, or photograph). (Source: 5 U.S.C. 552a(a)(4).)

routine use: With respect to the disclosure of a record, the use of the record for a purpose that is compatible with the purpose for which it was collected. (Source: 5 U.S.C. 552a(a)(7).)

significant alteration: Any change that is made to the system of records requiring an amendment to an existing system of records. Occurs when the manner in which the records are organized changes, the manner in which records are retrieved changes, or the scope of the records changes. (Source: OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals.)

system of records: Group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual (a personal identifier). (Source: 5 U.S.C. 552a(a)(5).)

system of records notice (SORN): Statement providing to the public notice of the existence and character of a group of records under the control of any agency, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (Source: OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals.)

system owner: Typically a senior program manager or executive responsible for a set of mission-critical functions of the agency. In this role, he or she serves as the person responsible for one or more information system supporting his or her assigned functions. (Source: OPM Information Security and Privacy Policy)

APPENDIX C: LIBRARY OF ROUTINE USES

Best Practices

Accepted best practices in the Federal community have helped to shape methods of compliance with the Privacy Act. One best practice is the use of "routine use libraries" (5 U.S.C. 552a(a)(7) and (b)(3)). Per 5 U.S.C. 552a(a)(7), the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

Additional best practices regarding routine use are mentioned below:

- Routine uses generally aim to promote simplicity and economy and avoid redundancy.
- Routine uses must be compatible with the purpose of the original collection, so not all routine uses in the library listed below will be appropriate for a given system of records notice (SORN).
- Agencies must review each routine use carefully and determine which are appropriate and compatible for a particular system of records.
- Very few SORNs will need to use all the routine uses in the library, and some SORNs will have specific sharing needs that are not covered by these routine uses. Such systems and programs will need to develop additional routine uses to meet their needs. Further, the routine uses provided in the library may be modified to meet specific mission needs.
- Routine uses are not necessary to share information within an agency as long as the sharing is required for the performance of the recipient's official duties (5 U.S.C. 552a(b)(1)).

Each agency must periodically review its routine uses to identify any that are no longer justified or that are no longer compatible with the purpose for which the information was collected (OMB Memorandum 99-05).

Below is the approved library of routine uses for internal and central systems of records. For routine uses of Governmentwide systems of records, please consult with the Privacy Act Officer and the Office of General Counsel.

Library of Approved OPM Internal and Central Routine Uses

As published in 53 FR 1997, Jan. 26, 1988, as amended at 57 FR 20956, May 18, 1992:

"*Prefatory Statement of Routine Uses for OPM's Internal and Central Systems of Records*

Certain established routine uses have been found to be applicable to the majority of OPM's Internal and Central systems of records. These repetitive routine uses will be published in their entirety once, in this Prefatory Statement. Each Internal and Central system notice will note which of these routine uses are applicable to that notice, and will also include the full text of any routine uses unique to that system of records."

1. For Law Enforcement Purposes--To disclose pertinent information to the appropriate Federal, State, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where OPM becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

2. For Certain Disclosures to Other Federal Agencies--To disclose information to a Federal agency, in response to its request in connection with the hiring or retention of an employee, the issuance of a security clearance, the conducting of a suitability or security investigation of an individual, the classifying of jobs, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency's decision on the matter.

3. For Congressional Inquiry--To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

4. For Judicial/Administrative Proceedings--To disclose information to another Federal agency, to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding. In those cases where the Government is not a party to the proceeding, records may be disclosed if a subpoena has been signed by a judge.

5. For National Archives and Records Administration--To disclose information to the National Archives and Records Administration for use in records management inspections.

6. Within OPM for Statistical/Analytical Studies--By OPM in the production of summary descriptive statistics and analytical studies in support of the function for which the records are collected and maintained, or for related workforce studies. While published studies do not contain individual identifiers, in some instances the selection of elements of data included in the study may be structured in such a way as to make the data individually identifiable by inference.

7. For Litigation--To disclose information to the Department of Justice, or in a proceeding before a court, adjudicative body, or other administrative body before which OPM is authorized to appear, when:

(1) OPM, or any component thereof; or
(2) Any employee of OPM in his or her official capacity; or
(3) Any employee of OPM in his or her individual capacity where the Department of Justice or OPM has agreed to represent the employee; or
(4) The United States, when 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 or OPM is deemed by OPM to be relevant and necessary to the litigation provided, however, that the disclosure is compatible with the purpose for which records were collected.

8. For the Merit Systems Protection Board--To disclose information to officials of the Merit Systems Protection Board or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of OPM rules and regulations, investigations of alleged or possible prohibited personnel practices, and such other functions, e.g., as promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

9. For the Equal Employment Opportunity Commission--To disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations into alleged or possible discrimination practices in the Federal sector, compliance by Federal agencies with the Uniform Guidelines on Employee Selection Procedures or other functions vested in the Commission and to otherwise ensure compliance with the provisions of 5 U.S.C. 7201.

10. For the Federal Labor Relations Authority--To disclose information to the Federal Labor Relations Authority or its General Counsel when requested in connection with investigations of allegations of unfair labor practices or matters before the Federal Service Impasses Panel.

11. For Non-Federal Personnel--To disclose information to contractors, grantees, or volunteers performing or working on a contract, service, grant, cooperative agreement, or job for the Federal Government.

APPENDIX D: HOW TO COMPLETE A SYSTEM OF RECORDS NOTICE (SORN)

This appendix outlines the elements that must be addressed in a system of records notice (SORN). A SORN is comprised of an introductory section in which OPM announces the creation of a new, significantly altered, or terminated system of records. This is followed by a section that describes the components of the system of record. Below is a sample introductory section for a new SORN, followed by a tutorial with examples on how to complete the component descriptions of the SORN for publication in the Federal Register. SORN templates are available from the Privacy Program Manager at piamail@opm.gov.

Sample Introductory Section for a New SORN

Publication Date _____
6325-38

OFFICE OF PERSONNEL MANAGEMENT

PRIVACY ACT OF 1974: NEW SYSTEM OF RECORDS

AGENCY: U.S. Office of Personnel Management (OPM)

ACTION: Notice of a new system of records.

SUMMARY: OPM proposes to add a new system of records to its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the agency (5 U.S.C. 552a(e)(4)). The system has been operational since March 24, 2003 without incident. In 2006, OPM implemented the Certification and Accreditation process and the Federal Cyber Service: Scholarship for Service Program was identified as system of record and requiring a notice at that time.

DATES: This action will be effective without further notice on **[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless comments are received that would result in a contrary determination.

ADDRESSES: Send written comments to the Office of Personnel Management, ATTN: Kathryn Roberson, Manager, Federal Cyber Service: Scholarship for Service Program, 8610 Broadway, Rm. 305, San Antonio, TX 78217.

FOR FURTHER INFORMATION CONTACT: Kathryn Roberson, 202-369-1011.

SUPPLEMENTARY INFORMATION: The Federal Cyber Service: Scholarship For Service website (SFS) allows OPM the ability to fulfill its responsibility for the SFS program which was established by the National Science Foundation in accordance with the Federal Cyber Service Training and Education Initiative as described in the President's *National Plan for Information Systems Protection* to facilitate the timely registration, selection and placement of program-enrolled students in Federal agencies. Specified OPM personnel use SFS to update student information. The system also affords registered agency officials read-only access to student resumes to consider them for placement with their agency. Furthermore, it allows registered university officials limited read-only access to students in their program so they can ensure students are meeting program requirements.

U.S. OFFICE OF PERSONNEL MANAGEMENT

_____

John Berry
Director

6325-38

Tutorial on Completing the SORN Components Section

System identifier:
This identifier and number are assigned by the Privacy Program Manager based on the classification of the system.

> **Example**
> OPM/GOVT-1

System name:
The system name must identify the general purpose and, if possible, the general categories of individuals covered. Use a name the public will readily understand, not internal "buzz words" or project or IT system names.

> **Example**
> System name:
> Presidential Management Fellows (PMF) Program Records (August 21, 2009, 74 FR 42334).
>
> **Note: The information following the system name represents the Federal Register citation, the date published, and the volume and page number.**

Security classification:
This is a statement of whether the system is classified or unclassified. This is an optional element.

System location:
For electronic or paper records, this is the main server or central file location. List the complete mailing addresses of **all** the OPM offices or contractor-maintained sites where the records are located (post office boxes are not considered locations). If multiple locations are used, identify each of them. For security reasons, do **not** list the location of backup files.

> **Example**
> System location:
> U.S. Office of Personnel Management, Employee Services, Recruitment and Diversity, Recruitment & USAJOBS, Student Programs, Presidential Management Fellows Program, 1900 E Street NW, Washington, DC 20415.

Categories of individuals covered by the system:
This includes the types of individuals with respect to whom records will be maintained on the system (employees, contractors, etc.). Identify **all** the categories of individuals covered by the system of records to which records in the system pertain. Use clear, easily understood terms. Avoid the use of broad, overly general descriptions. Once the notice is published, you may collect data only on the individuals described **and no others**. If you wish to add a new category of individuals covered, you must first alter the existing notice and republish it in the Federal Register **before** adding the new category of individuals covered.

Example
Categories of individuals covered by the system:
OPM civilian employees; nonappropriated funded employees; interns or students employed and paid directly by OPM (interns or students hired through contractual agreements are not eligible); eligible interns or students hired for the summer months.

Categories of records in the system:
Describe all the types of records the system contains. Identify each data element or record being maintained on an individual. Each personal data element must be **relevant and necessary** to accomplish an agency purpose grounded in law (Federal statute, regulation, or Executive order). If a form is used to collect the data, copy fields from the form. If the data is maintained electronically, list each field in the record layout. A Privacy Act statement must appear on any form, paper or electronic, that collects information directly from the subject individual to be maintained in the system of records. Once the notice is published, you may collect only the records described **and no others**. If you wish to add new records being maintained, you must first alter the existing notice and republish it in the Federal Register **before** adding the new records being maintained.

Example
Categories of records in the system: These records contain information about the covered individuals relating to name, social security number, academic background, home address, telephone numbers, e-mail addresses, employment history, Indian and veterans' preference, and other personal information needed during the application, nomination, assessment, and selection processes, and as needed for training and development opportunities impacting PMFs and participating agencies. This system also will contain confidential evaluation information and assessment scores not available to the public.

Hint #1: Collect the least amount of data required to accomplish the agency mission or function.

Hint #2: List the data elements you collect now or plan to collect at a future date. Including a data element doesn't mandate that you actually collect it; it merely authorizes you to collect it if it's needed. **If you eliminate something you later find you need, you must revise and republish the notice in the Federal Register before you begin collecting that data element.**

Hint #3: If you collect many data elements, you can group like-items together. If, for example, you collect details about a person's education, you need only list "education data." **Exception:** Collections covering medical, rehabilitation, and personal financial data must include each data element.

Authority for maintenance of the system:
This is the agency's authority to maintain the system. Cite the specific Federal statutes or Executive orders that authorize **your agency** to collect and maintain the data or system of records. If you collect social security numbers, list "Executive Order 9397 as amended by

Executive Order 13478" in your authority entry. OPM issuances may also be listed at the end of this element to allow the public to learn more about your authorities and data uses; however, they do not stand alone as authorities.

Example:
Authority for maintenance of the system:
Executive Order 9397 as Amended by Executive Order 13478 signed by President George W. Bush on November 18, 2008, Relating to Federal Agency Use of Social Security Numbers.

Purpose(s):
This is an explanation of why the program collects these particular records. Cite the internal (OPM-specific) uses made of the information. Start with the primary purposes and follow up with secondary purposes. Keep in mind that **all** internal uses must be compatible with the primary purpose of collecting the data. Describe who uses the data and what they use it for.

Once the notice is published, you may only use the data for the purposes you have described **and no others**. If a new purpose is required, you **may not** use the information for that new purpose until the notice is revised and republished in the Federal Register.

Example
Purpose:
These records are used by program personnel for the following reasons:

a. To determine basic program eligibility and to evaluate the nominees in a structured assessment process conducted by OPM.

b. To group the applicants into various categories (e.g., applicants, nominees, finalists, and nonselectees) and make a final determination as to those candidates who will be referred (as finalists to become Fellows) to participating agencies for employment consideration.

c. For program evaluation functions to determine the effectiveness of the program and to improve program operations.

d. To facilitate interaction and communication between PMF Program participants and alumni.

e. To track PMF appointments, certifications, conversions, reappointments, withdrawals, resignations, extensions, waivers, and deferrals.

f. To track agency reimbursements for PMF appointments.

g. To schedule and track PMF participation in program-sponsored training and development events (e.g., orientation, forums, graduation).

h. To track contact information of applicants, nominees, finalists, Fellows, agency PMF coordinators, PMF supervisors, graduate school nomination officials, and other relevant stakeholders.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:
Routine uses apply to information sharing external to OPM. The term "routine use" is defined, with respect to the disclosure of a record, as "the use of such record for a purpose which is compatible with the purpose for which the record was collected." This section describes each situation in which OPM may share records on individuals covered by to the SORN under the Privacy Act Section (a)(b)(3).

The routine uses must be compatible and consistent with the purpose for which the record was collected. This ensures the public receives adequate notice of the agency's planned uses of the information in the system of records.

The following language must be included prior to the list of routine uses:

"*In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside OPM as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:"*

Example
Common routine uses for most systems of records include sharing:

- For audits and oversight.
- For congressional inquiries.
- With contractors, grantees, and experts to perform OPM-authorized activities.
- For investigations of potential violations of law.
- For intelligence purposes.
- With the National Archives and Records Administration (NARA) for records management purposes.
- For litigation purposes.
- For data breach and mitigation response.

Appendix C provides the OPM Library of Routine Uses, which may be included in the SORN exactly as they are written. Routine uses must be compatible with the purpose of the original collection, so not all routine uses in the library will be appropriate for a given SORN. OPM program offices must review each routine use carefully and determine which are appropriate and compatible for each particular system of records. Very few SORNs will need to use all the routine uses in the library and some SORNs will have specific sharing needs that are not covered

by these routine uses. Such systems and programs will need to develop additional routine uses to meet their needs. Further, the routine uses provided in the library may be modified to meet specific mission needs, if there is sufficient justification. An office that contemplates taking such a step should confer with the Office of the Chief Information Officer.

Routine uses apply to information sharing external to OPM. Information sharing within OPM does not need a specific routine use. OPM is considered one agency; routine uses are not necessary to share information within OPM as long as the sharing is required for the performance of the recipient's official duties.[10] Information sharing within OPM should be addressed in the purpose and supplementary information to the SORN, and in a privacy impact assessment (PIA) when applicable.

Disclosure to consumer reporting agencies:
State what information is disclosed to consumer reporting agencies. If no information is disclosed, state "None."

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
Describe the policies and practices in which records are handled for each respective practice.

Storage:
Describe the manner in which the records are stored. For example, are the records paper or electronic? Are the records stored in a locked or unlocked metal file cabinet, or magnetic, optical, or electronic media? Many SORNs state that the records are stored in a central computer database. Also, if information is stored on backups in a different format, note that here.

Retrievability:
This element informs the public how OPM retrieves the records. To be subject to the Privacy Act, the records must be retrieved by a personal identifier. (OMB guidelines state that the "is retrieved by" criterion "implies that the grouping of records under the control of an agency **is accessed by** the agency by use of a personal identifier; not merely that a capability or potential for retrieval exists.")

> **Example**
> Retrievability:
> Information is retrieved by the individual's name and last four digits of his or her social security number.
>
> **Caution:** If a single electronic record contains the name of any individual other than the subject, make sure you never retrieve on the name or identifier of the person who is **not** the subject. Retrieving on multiple names clouds the issue of who the true subject of the record is.

[10] 5 U.S.C. 552(a)(b)(1).

Safeguards:
For this element, describe the **physical, technical,** and **administrative** safeguards taken to protect the records, identifying the safeguards for both paper and electronic records (e.g., locked rooms, password assignments). The safeguards must be sufficient to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards. Do not describe safeguards in such detail as to compromise system security.

Appendix III to OMB Circular A-130 defines "adequate security" as security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes ensuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls.

> **Hint #5:** Start with the physical safeguards, then the technical, and lastly administrative safeguards. Information for this entry will come from the C&A process.
>
> **Hint #6:** All individuals granted accesses to the system of records must have taken Privacy Act training. OPM requires annual Privacy Act training. Training modules are available on the Internet at http://hr.golearnportal.org.

Retention and disposal:
Indicate how long the record is retained before it is destroyed or transferred to a Federal Records Center (FRC). For records transferred to an FRC, show the length of retention at the FRC. The retention period you claim must agree with the OPM Records Schedule in the OPM Records Management Handbook on the intranet, found at http://theo.opm.gov/references/it/policies.asp, or the NARA publication, General Records Schedule, available at http://www.archives.gov/records-mgmt/grs/. If the system contains more than one type of record, show the retention period for each type. For example, unapproved applications may be kept for a shorter time than approved applications.

If your records are not covered by a current disposal authority, contact the OPM Records Officer to have the records scheduled.

System manager and address:
Identify the position title and address of the system manager. This is generally the system owner or the program manager who oversees the program.

Notification procedure:
This is the basic information needed for an individual to make a proper information request to the system manager and for the manager to provide a proper response to the request.[11] This element describes how an individual may determine if there are records pertaining to him or her in the system of records. The default wording is listed below.

[11] OMB, Privacy Act Implementation, Guidelines and Responsibilities, 40 F.R. 28961 (July 9, 1975).

Default Wording
Individuals wishing to determine whether this system of records contains information about them may do so by writing to FOI/P, OPM, ATTN: FOIA Officer, 1900 E Street, NW, Room 5415, Washington, DC 20415-7900.
Individuals must furnish the following information for their records to be located:

1. *Full name.*

2. *Date and place of birth.*

3. *Social security number.*

4. *Signature.*

5. *Available information regarding the type of information requested.*

6. *The reason the individual believes this system contains information about him or her.*

7. *The address to which the information should be sent.*

Individuals requesting access must also comply with OPM's Privacy Act regulations regarding verification of identity and access to records (5 CFR 297).

Record access procedures:
This section describes how the individual may gain access to his or her record. The default wording is listed below.

Example
Individuals wishing to request an amendment of records about them should write to [name of program, name of system manager, mailing address], and furnish the following information for their records to be located:

(1) Full name.
(2) Date and place of birth.
(3) Social security number.
(4) Signature.
(5) Precise identification of the information to be amended.

Individuals requesting an amendment must also follow OPM's Privacy Act regulations regarding verification of identity and amendment to records (5 CFR 297).

Some records are more sensitive than others. If you require the individual to provide proof of identity, use the following wording in this element:

Default Wording
"In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on [date]. [Signature].'

If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on [date]. [Signature].'"

Contesting record procedures:
Describe how an individual may contest information pertaining to him or her in the system of records. Similar to "Record Access Procedures," this section may be the same as "Notification Procedure." As such, the program office may state, "See Notification Procedure above."

Record source categories:
This section includes where the agency received the records (e.g., from the individual, other system of records, etc.). List all sources of the information you are maintaining. Sources can be within OPM or outside of OPM. Do you get data from other Federal entities? What about private entities? What about State or local agencies? Keep in mind that the Privacy Act requires that data be collected from the record subject whenever the possibility of adverse action is present. As a general practice, rely on the individual to supply the data whenever possible.

Exemptions claimed for the system:
Often the response here is "None," because many systems do not meet the requirements to claim exemptions to the Privacy Act. If you believe an exemption applies to the system of records, please review the text of general exemptions (j) and specific exemptions (k) printed below. After reviewing the Privacy Act text, determine which exemption is appropriate and consult with the OPM Privacy Act Officer and OPM Office of General Counsel to draft a notice of proposed rulemaking (NPRM).

Text of General Exemption (j) of the Privacy Act:
The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is:

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and

consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.[12]

Text of Specific Exemptions (k) of the Privacy Act:
The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is:

(1) subject to the provisions of section 552(b)(1) of this title;

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;

(4) required by statute to be maintained and used solely as statistical records;

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source

[12] 5 U.S.C. 552a(j)

would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.[13]

Any exemptions taken in an NPRM must be published as a Final Rule before they are effective; simply publishing an NPRM will not exempt the system.[14]

[13] 5 U.S.C. 552a(k).

[14] OMB Circular A-130, Appendix I, 4(c)(5).

APPENDIX E: SAMPLE OPM NARRATIVE STATEMENTS

New System Report - Narrative Statement

OPM/Internal-18, Federal Cyber Service: Scholarship For Service website

1. **What is the purpose for establishing OPM/Internal-18, Federal Cyber Service: Scholarship For Service website?**
The Federal Cyber Service: Scholarship For Service (SFS) website will allow OPM to maintain a more accurate list of participating students in order to successfully facilitate the timely placement of participating students.

2. **What is the authority for maintaining OPM/Internal-18, Federal Cyber Service: Scholarship For Service website?**
The SFS Program was established by the National Science Foundation in accordance with the Federal Cyber Service Training and Education Initiative as described in the President's *National Plan for Information Systems Protection.*

3. **What is the probable or potential effect of OPM/Interna1-18, Federal Cyber Service: Scholarship For Service website?**
The probable or potential effect on the privacy of individuals is limited; access to records are restricted to individuals who have the appropriate clearance and need-to-know for disclosures to other Federal agencies.

4. **What steps will we take to minimize the risk of unauthorized access to OPM/Internal-18, Web-Enabled Voting Rights System records?**
To minimize the risk of unauthorized access to these records, OPM has adopted appropriate administrative, technical, and physical controls in accordance with its Automated Information Systems Security Program to protect information in the SFS database.

5. **Are the routine uses for OPM/Internal-18, Federal Cyber Service: Scholarship For Service website, compatible with the purpose for which they are collected?**
The routine uses for this system of records are compatible with the purpose for which these records are collected. SFS will allow OPM's Center for Talent Services to register scholarship recipient's education and experience and to provide this information to potential Federal employers.

6. **Are there any OMB Control Numbers, expiration dates, and titles of any information collection requests (e.g., forms, surveys, etc.) contained in OPM/Internal-18, Federal Cyber Service: Scholarship for Service website, and approved by OMB under the Paperwork Reduction Act?**
OMB Approved # 3206-0246
Expires: 05/31/2010

Alteration of Existing System of Records – Narrative Statement

OPM/Internal-16, Adjudications Officer Control Files

1. What is the purpose of altering the systems of records notice for OPM/Internal-16, Adjudications Officer Control Files?

OPM is proposing to add information to the categories of individuals covered by this System, revise the routine uses, and update the retention of the Standard Form 312.

2. What is the authority for maintaining the OPM/Internal-16, Adjudications Officer Control Files

The authorities for maintenance of the System include the following, with any revisions or amendments: Executive Orders 10450, 12958, and 12968.

3. What is the probable or potential individual privacy effect on amending and updating the OPM/Internal-16, Adjudications Officer Control Files

The probable or potential effect on individual privacy is limited; Records in OPM/Internal-16 are restricted to individuals who have the appropriate background investigation and a need to know in order to perform their official duties.

4. What steps will we take to minimize the risk of unauthorized access to the OPM/Internal-16, Adjudications Officer Control Files

OPM stores the files in locked, metal file cabinets in a secured room. OPM restricts access to the records on the database to employees who have the appropriate background investigation and need to know in order to perform their official duties.

5. Are the routine uses for the OPM/Internal-16, Adjudications Officer Control Files, compatible with the purpose for which they are collected?

The routine uses for this system of records are compatible with the purpose for which these records are collected.

6. Provide OMB Control Numbers, expiration dates, and titles of any information collection requests (e.g., forms, surveys, etc.) contained in the system of records and approved by OMB under the Paperwork Reduction Act.

None.

APPENDIX F: SAMPLE NEW SYSTEM OF RECORDS NOTICE (SORN)

Publication Date _____
6325-38

OFFICE OF PERSONNEL MANAGEMENT

PRIVACY ACT OF 1974: NEW SYSTEM OF RECORDS

AGENCY: U.S. Office of Personnel Management (OPM)

ACTION: Notice of a new system of records.

SUMMARY: OPM proposes to add a new system of records to its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of records maintained by the agency (5 U.S.C. 552a(e)(4)). The system has been operational since March 24, 2003 without incident. Publication of this system of records was inadvertently delayed. In the meantime, appropriate measures were taken to maintain the integrity and confidentiality of the information.

DATES: This action will be effective without further notice on **[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless comments are received that would result in a contrary determination.

ADDRESSES: Send written comments to the Office of Personnel Management, ATTN: Kathryn Roberson, Manager, Federal Cyber Service: Scholarship for Service Program, 8610 Broadway, Rm. 305, San Antonio, TX 78217.

FOR FURTHER INFORMATION CONTACT: Kathryn Roberson, 202-369-1011.

SUPPLEMENTARY INFORMATION: The Federal Cyber Service: Scholarship For Service website (SFS) allows OPM the ability to fulfill its responsibility for the SFS program which was

established by the National Science Foundation in accordance with the Federal Cyber Service Training and Education Initiative, as described in the President's *National Plan for Information Systems Protection*, to facilitate the timely registration, selection and placement of program-enrolled students in Federal agencies. Specified OPM personnel use SFS to update student information. The system also affords registered agency officials read-only access to student resumes to consider them for placement with their agency. Furthermore, it allows registered university officials limited read-only access to students in their program so they can ensure students are meeting program requirements.

U.S. OFFICE OF PERSONNEL MANAGEMENT

_____

John Berry
Director

6325-38

APPENDIX G: SAMPLE AMENDED SYSTEM OF RECORDS NOTICE (SORN)

Publication Date_____
6325-38

OFFICE OF PERSONNEL MANAGEMENT

AGENCY: U.S. Office of Personnel Management (OPM)

ACTION: Notice of amendment to system of records.

SUMMARY: OPM has amended an existing system of records subject to the Privacy Act of 1974 (5 U.S.C. 552a). This action is necessary to meet the requirements of the Privacy Act to publish in the Federal Register notice of the existence and character of system of records maintained by the agency (5 U.S.C. 552a(e)(4)).

DATES: The changes became effective in November 2003. The system has been operational for 6 years without incident. Comments will be accepted until **[INSERT DATE 40 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**

ADDRESSES: Written comments must be sent to the U.S. Office of Personnel Management, Presidential Management Fellows Program, ATTN: Rob Timmins (OPM\Central-11), 1900 E Street, NW, Room 1425, Washington, DC 20415.

FOR FURTHER INFORMATION CONTACT: Rob Timmins, (202) 606-2674, fax (202) 606-3040, or email to Rob.Timmins@opm.gov. Please include your complete mailing address with your request.

SUPPLEMENTARY INFORMATION: This notice serves to update and amend collection, analysis, and maintenance of OPM\Central-11 (Presidential Management Fellows Program) as a result of new program regulations and an increased use of automated information technology. Revisions include the following: (1) Authority of Program now results from Executive Order

13318, Presidential Management Fellows Program, signed by President George W. Bush on November 21, 2003; (2) The Executive order changed the name from Presidential Management Intern (PMI) Program to the Presidential Management Fellows (PMF) Program; (3) There is no longer a category of records collection for semi-finalists; (4) As a result of the OPM re-organization in March 2003, the system location has been updated to reflect current name; and (5) The system manager contact has been updated to reflect the new PMF Program organization and location.

U.S. Office of Personnel Management

_____

John Berry
Director

Billing Code: 6325-38

APPENDIX H: SAMPLE TERMINATED SYSTEM OF RECORDS NOTICE (SORN)

Publication Date_____
6325-11

OFFICE OF PERSONNEL MANAGEMENT

AGENCY: U.S. Office of Personnel Management (OPM)

ACTION: Notification of Termination of a System of Records

SUMMARY: The Office of Personnel Management is terminating a system of records, OPM\Central-21 Retirement Records, that is no longer in use.

DATE: Effective July 29, 2010

FOR FURTHER INFORMATION CONTACT: John Doe, (202) 606-2222, fax (202) 606-3333, or email to john.doe@opm.gov. Please include your complete mailing address with your request.

SUPPLEMENTARY INFORMATION: On August 21, 1999, and pursuant to the provisions of the Privacy Act of 1974, there was published in the *Federal Register* (57 FR 32221) a system of records notice establishing the OPM\Central-21 Retirement Records system of records. Accordingly, this notice formally terminates this system of records.

U.S. Office of Personnel Management

_____
John Berry
Director

Billing Code: 6325-11

APPENDIX I: SAMPLE CONGRESSIONAL AND OMB LETTERS

Letter to the Chairman of Government Affairs

The Honorable Joseph Lieberman
Chairman

Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Lieberman:

As required by the Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503), I am providing you with a copy of the Federal Register notice that we prepared regarding a new system of records known as the OPM Central 15, Combined Federal Campaign.

Copies of the notice are also being sent to the Chairman, Committee on Government Reform and Oversight, U. S. House of Representatives and the Office of Information and Regulatory Affairs, Office of Management and Budget.

A narrative statement, as required in the Office of Management and Budget Circular No. A-130, accompanies this letter.

For further information, your staff may contact Tania Shand at (202) 606-1300.

Sincerely,

John Berry
Director

Enclosures

Cc: Chairman of the Committee on Government Reform and Oversight,
U.S. House of Representatives
Administrator, Office of Information and Regulatory Affairs,
Office of Management and Budget

Letter to the Office of Reform

The Honorable Edolphus Towns
Chairman

Committee on Government Reform and Oversight
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Towns:

As required by the Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503), I am providing you with a copy of the Federal Register notice that we prepared regarding a new system of records known as the OPM Internal 18 Scholarship For Services.

Copies of the notice are also being sent to the Chairman, Senate Committee on Governmental Affairs and the Office of Information and Regulatory Affairs, Office of Management and Budget.

A narrative statement, as required in the Office of Management and Budget Circular No. A-130, accompanies this letter.

For further information, your staff may contact Tania Shand at (202) 606-1300.

Sincerely,

John Berry
Director

Enclosures

Cc: Chairman of the Committee on Homeland Security and Governmental Affairs,
United States Senate
Administrator, Office of Information and Regulatory Affairs,
Office of Management and Budget

Letter to Office of Information and Regulatory Affairs (OIRA), OMB

Mr. Cass Sunstein
Administrator

Office of Information and Regulatory Affairs
Office of Management and Budget
725 7th Street, N.W.
Washington, DC 20503

Dear Mr. Sunstein:

As required by the Computer Matching and Privacy Protection Act of 1988 (Public Law 100-503), I am providing you with a copy of the Federal Register notice that we prepared regarding a new system of records known as the OPM Internal 18 Federal Cyber Service: Scholarship For Service website.

Copies of the notice are also being sent to the Chairman, Senate Committee on Governmental Affairs, and Chairman, Committee on Government Reform, U. S. House of Representatives.

A narrative statement, as required in the Office of Management and Budget Circular No. A-130, accompanies this letter.

For further information, your staff may contact Tania Shand at (202) 606-2150.

Sincerely,

John Berry
Director

Enclosures

Cc: Chairman of the Committee on Homeland Security and Governmental Affairs,
United States Senate
Chairman of the Committee on Government Reform and Oversight,
U. S. House of Representatives

APPENDIX J: DRAFTING A PRIVACY ACT STATEMENT

What Is a Privacy Act Statement?

The Privacy Act of 1974 (5 U.S.C. 552a) provides protection to individuals by ensuring that personal information collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner that precludes unwarranted intrusions on individual privacy.

Under 5 U.S.C. 552a (e)(3), agencies are required to provide what is commonly referred to as a Privacy Act statement to all persons who are asked to provide personal information about themselves that will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier, such as social security number).

Drafting a Privacy Act Statement

When drafting a Privacy Act statement, include the following elements:

- Authority: The legal authority for collecting the information – statute, Executive order, or regulation.
- Purpose: The purpose for collecting the information and how OPM will use it.
- Routine Uses: To whom OPM may disclose the information outside of the agency and for what purposes.
- Disclosure: Mandatory or Voluntary. Whether providing the information is mandatory or voluntary. OPM can only make collection mandatory when a Federal statute, Executive order, regulation, or other lawful order specifically imposes a duty on the person to provide the information; and the person is subject to a specific penalty for failing to provide the requested information. This also describes the effects, if any, of not providing the information – for example, the loss or denial of a privilege, benefit, or entitlement sought as a consequence of not furnishing the requested information.

Before requesting a social security number (SSN), *even if it will not go into a system of records*, the agency must provide notice to the individual that includes:

- The law or authority for collecting the SSN.
- How OPM will use the SSN.
- Whether disclosure is mandatory or voluntary.

Notice regarding the collection, use, and authorization of SSNs must be incorporated into the Privacy Act statement. This is addressed by adding a sentence to the Privacy Act statement regarding the collection of the SSN. OPM cannot deny a legal right, benefit, or privilege if an individual refuses to provide his or her SSN unless the law requires disclosure or, for systems operated before January 1, 1975, a law or regulation adopted before that date required disclosure in order to verify the identity of the individual.

APPENDIX K: REFERENCES

- OMB Circular A-130, Federal Agency Responsibilities for Maintaining Records About Individuals.
- OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records.
- Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub. L. 93-579.
- Privacy Act Implementation, Guidelines and Responsibilities, July 9, 1975.

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
Chief Information Officer (CIO)
1900 E Street, NW
Washington, DC 20415

CIO/IM/ITSP-0002