

1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

- (a) **Date PIA was completed:** January 14, 2009
- (b) **Name of system:** Retirement Records System
- (c) **System acronym:** RRS
- (d) **IT Asset Baseline (ITAB) number:** 524
- (e) **System description (Briefly describe scope, purpose, and major functions):**
RRS is a records keeping system that maintains service history and financial information used to pay Department of State (DoS) and other government annuitant. RRS maintains information on approximately 62,000 Federal employees (GS and FSO) and Foreign Nationals who are currently employed, terminated, retired, or deceased. In addition to DoS employees, RRS maintains information on employees at the Broadcast Board of Governors (BBG).
- (f) **Reason for performing PIA:**
- New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security re-certification
- (g) **Explanation of modification (if applicable):**
- (h) **Date of previous PIA (if applicable):**

3. Characterization of the Information

The system:

- does NOT contain PII. If this is the case, you must only complete Section 13.
- does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Names, financial addresses, birth dates and social security numbers. The source of information is Federal employees (GS and FSO) and Foreign Nationals who are currently employed, terminated, retired or deceased. In addition to DoS employees, RRS maintains information on employees at the BBG.

b. How is the information collected?

The information is collected from DoS and BBG personnel and payroll systems such as Foreign Affairs Retirement and Disability System, the Civil Service Retirement System, and the Federal Employees Retirement System.

c. Why is the information collected and maintained?

The information is used to create the employee's Individual Retirement Record.

d. How will the information be checked for accuracy?

The Bureau of Resource Management checks to make sure the information provided is complete and accurate. At retirement, the Retirement Accounts Division verifies the amounts against the records in CAPPs and, in old payroll books to determine the year to date amounts are correct.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 U.S.C. 2651a (Organization of the Department of State);
- 22 U.S.C. 3921 (Management of service);
- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 4042 (Maintenance of the Foreign Service Retirement and Disability Fund);
- 42 U.S.C. 653 (the Personal Responsibility and Work Opportunity Reconciliation Act of 1996);
- Executive Order 11491, as amended (Labor-management relations in the Federal service);
- 5 U.S.C. 5501-5584 (Pay Administration); and
- 31 U.S.C. 901-903 (Agency Chief Financial Officers).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

This system collects the absolute minimum amount of personally identifiable information required to satisfy the statutory purposes of this system and the mission of the bureau. The employees and contractors working for the DoS have undergone a thorough background security investigation. Access to the Department and its annexes is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals with proper escort. Access to computerized files is under the direct supervision and files are password protected.

4. Uses of the Information

a. Describe all uses of the information.

RRS contains the historical employee data collected for the purpose of creating an official record of retirement and, for calculating the annuity payment at retirement.

b. What types of methods are used to analyze the data? What new information may be produced?

This system does not create new data but updates and correct data entries in RRS to replicate data in CAPPS.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Not applicable

d. Is the system a contractor used and owned system?

This is a government owned system but contractors are involved in the design and development of the system. All contractors undergo an annual computer security briefing and Privacy Act briefing. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Access Control Facility (ACF2) software tool provides the controls to protect the data from unauthorized access or use. Only employees with a need to know are granted access to the records. Users have undergone background checks and received training in handling personally identifiable information. Users receive security awareness training annually. Users are restricted to browsing only data that they are authorized to view for official purpose of their duties only.

5. Retention

a. How long is information retained?

The information is retained in accordance with the records disposition schedule for 56 years.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

To prevent unauthorized use and exposure of information, access to these records are limited to authorized personnel and password protected. Regular backups are performed and, recovery procedures are in place for computerized files. When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

The data is shared with the Human Resource's Office of Retirement, as well as the Resource Management's Retirement Accounts Division. Authorized users from both bureaus require access to historical employee data, in order to accurately process an employee's retirement from active service.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Employees with a need to know are granted access. All file access is governed by ACF2 software tool, which provides the controls to protect the data from unauthorized access or use. Only employees with a need to know are granted access to the records and, all users are trained annually as to the use and misuse of Sensitive but Unclassified data.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The use of the information is in accordance with the stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized person.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

For Civil Service personnel only, an employee's data is shared with the Retirement Office in the Office of Personnel Management (OPM) in order for the employee to receive retirement benefits.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

The Resource Management Retirement Accounts Division forwards the data (paper forms) via Federal Express to OPM.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Risks to privacy are mitigated by limited access to and release of personal information. Information may only be released on a need-to-know basis to other government agencies having statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose. The delivery of paper files are tracked and monitored.

8. Notice

The system:

- constitutes a system of records covered by the Privacy Act.

Personnel Payroll System, State-30

does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Individuals are made aware of the uses of the information prior to the collection. Notice is published in the system of record State-30, Personnel Payroll Records.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, the individuals have the right not to provide the information. No penalties or denial of a right, benefit, or privilege might result from this action but without this information services may be delayed or not accomplished.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No, the system would not be able to provide services or utilized the system for its intended use.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The System of Records Notice Personnel Payroll Records State-30 was published in the Federal Register for comment 40 days prior to collection. The Notice is available on the Department of State public-facing website and the Federal Register for review. The notice provides individuals with details such as the information that will be collected, routine use of the information and notification procedures. There are no known associated risks.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The record subjects have notification and redress rights under the Privacy Act, and that the relevant procedures are or will be described in State-30. Individuals who want to gain access or amend records pertaining to them should write to the Director, Office of Information Programs and Services, A/ISS/IPS, U.S. Department of State, SA-2 Washington D.C. 20522-8001.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress procedures offered to individuals are reasonable and adequate in relation to the system's purposes and uses.

10. Controls on Access

- a. **What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?**

All users maintain a least a public trust and SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access records, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). A username and password is created and user's access is restricted depending upon their role and need to know. Audit logs are maintained to record system and user activity including invalid logon attempts and access to data. Information System Security Officer monitors audits logs monthly for unusual activity.

- b. **What privacy orientation or training for the system is provided authorized users?**

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access.

- c. **Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.**

There are no risks expected.

11. Technologies

- a. **What technologies are used in the system that involve privacy risk?**

No technologies are used in this system that would involve privacy risk.

- b. **Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

Not applicable

12. Security

What is the security certification and accreditation (C&A) status of the system?

C&A is current and valid until December 31, 2009.