

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: 8/18/2008
- (b) Name of system: Document Imaging System
- (c) System acronym: DIS
- (d) IT Asset Baseline (ITAB) number: 871
- (e) System description (Briefly describe scope, purpose, and major functions):

This system converts paper records to electronic files by scanning new submissions as well as existing paper files for current and retired Department of State (DOS), employees, their beneficiaries and contractors. The image files will enable accounts managers and technicians to accomplish their tasks faster and without the requirement to move paper files back and forth from storage.

- (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): Addition of interface between Claims DIS and the Global Financial Management System (GFMS)

- (h) Date of previous PIA (if applicable): 4/25/2008

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?

The source of information is forms that are filled out by DOS employees, retirees, their beneficiaries and contractors that are then scanned into DIS and maintained in shared drive. Documents maintained in DIS include forms that collect information on employment, retirement pay and other documents processed by the Office of Claims. Personally identifiable information that is maintained includes names, address, social

security numbers, tax identification numbers, date of birth, age, marital status, vendor information, financial banking information, beneficiary and insurance information.

b. How is the information collected?

The information maintained in DIS is forms collected by Foreign Service National (FSN), Retirement Annuity Division (RAD) and CLAIMS that are scanned and converted to electronic records.

c. Why is the information collected and maintained?

The electronic files allow accounts managers and technicians of FSN, RAD, and CLAIMS to accomplish their tasks faster and eliminate the requirement to move paper files to and from storage.

d. How will the information be checked for accuracy?

The data is reviewed by administrative personnel when the information is collected by forms. The accuracy of the information is dependent on the quality controls established when forms are processed.

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

Federal Financial Management Improvement Act (FFMIA) of 1996.

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

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 folders are password protected.

4. Uses of the Information

a. Describe all uses of the information.

The electronic files allow accounts managers and technicians to accomplish their tasks faster and eliminate the requirement to move paper files to and from storage. The PII will be only be used in accordance with the form's purpose. Data can be retrieved by an individual name, social security number, date of birth or employee number.

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

No new data or previously unavailable data will be created.

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 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.**

Users are accustomed to working with electronic records, 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 retention periods for records maintained in DIS varies from 3 to 99 years, depending upon the specific kind of record.

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

Regular backups are performed and recovery procedures are in place for electronic records. Access to electronic records are restricted to authorized personnel, is password-protected and under the direct supervision of the system manager. 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?**

Information is shared only with users that have been cleared by department management and require access to the electronic records to perform their official duties.

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

Access to folders that maintain electronic record must be authorized by supervisor. The folders are password protected and assigned level of permission that restricts the data use.

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

Risks to privacy are mitigated by granting access to authorized person and permissions that are established by their supervisor.

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?**

No data is shared outside the department.

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

No data is shared outside the department.

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

Not applicable.

8. Notice

The system:

contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit www.state.gov/m/a/ips/c25533.htm for list of all published systems):

STATE-30, Personnel Payroll Records

does NOT contain information covered by the Privacy Act.

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

DIS does not collect personal information directly from individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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

DIS does not collect personal information directly from individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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?

DIS does not collect personal information directly from individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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.

DIS does not collect personal information directly from individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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?

Procedures for notification and redress are published in the system of record State-30, Personnel Payroll Records and rules published at 22 CFR 171.31

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose 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?**

Internal access to DIS is limited to authorized staff having a need for the system in the performance of their official duties. All users maintain a least a SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access the electronic records maintained on the share drive, 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). Completed applications are also reviewed and approved by the Information System Security Officer prior to assigning the individual a logon. A system use notification ("warning banner") is displayed before logon is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged and audited. Access to folders that maintain electronic record must be authorized by supervisor. The supervisor will assign the level of permission for each user and restrict the data that may be seen and the degree to which data may be modified.

- 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 expected residual risks.

11. Technologies

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

No technologies commonly considered to elevate privacy risk are employed.

- 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?

ATO dated May 22, 2008 will expire May 31, 2011