Privacy Impact Assessment (PIA)

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: 6/30/2010

(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): The following changes are planned:

1. The DIS databases are currently hosted on three physical servers running Windows 2003. GFSC will consolidate these three physical servers into one physical server running Windows 2008 64 Bit.

2. DIS is currently hosted on the Oracle 9i database platform. Oracle will cease to support any additional patches of database version of 9i after July 2010; DoS has mandated that systems running Oracle version 9i move to 10g or 11g.

3. Currently there are three database servers and three database instances supporting the DIS. GFSC will consolidate three database servers to one database server with three database instances. The DIS application code will continue to reside on three discrete servers.

4. The DIS uses the Kofax Ascent Capture Version 7.5 Software for scanning and optical character recognition in the DIS; vendor support for release 7.5 is near its end. GFSC will upgrade Kofax from version 7.5 to 8.0.

5. GFSC will add American Payroll instance to our list of databases; the result is four instances on one database server.

6. GFSC will apply upgrades to the DocWise components of the DIS, upgrading DocWise in Retirement from 5.3 to 5.4, Claims 5.0 to 5.4 and FSN 5.0 to 5.4.

7. GFSC will apply upgrades to the Northrop ePower software on all servers from 6.4.1 to 6.5.2.

(h) Date of previous PIA (if applicable): 8/18/2008

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 a 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, addresses, 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), the Retirement Annuity Division (RAD), Claims, and American Payroll that are scanned and converted to electronic records. Hundreds of various forms are collected from a variety of agencies, including the Department of State, the Department of Homeland Security, the Department of Defense, the Department of Justice, and the Department of Transportation. Some of these forms contain a Privacy Act notice, while others do not; however, all information collected is covered by the System of Records Notice, State-30, which notifies the record subject of his or her privacy rights.

c. Why is the information collected and maintained?

The electronic files allow accounts managers and technicians of FSNs, RAD, Claims, and American Payroll 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 from information on the forms is reviewed by administrative personnel. The accuracy of the information is dependent on the quality controls performed when forms are processed. A search of the Global Employment Management System (GEMS) and preexisting records in DIS is performed to verify that the record subject's information does, indeed, belong to him or her.

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 amount and type of data collected in DIS is necessary to perform its functions. 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 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 (i.e. processing payroll requests, paying claims, etc.) faster and eliminate the requirement to move paper files to and from storage. The PII will 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.

No commercial information, publicly available information, or information from other Federal agency databases is used.

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.

Information obtained from record subjects has a specific use, described in 4(a) above. 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 vary 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 is restricted to authorized personnel, is password-protected, and is 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 (NARA).

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 not shared with other internal organizations.

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

Information in DIS is not shared internally.

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

Risks to privacy from internal sharing are not applicable to DIS.

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.

Since information from DIS is not shared externally, this section does not apply.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

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?

Notice is provided to the record subjects upon collection of their information through Privacy Act notices contained on some of the collection forms. In this way, they are made aware of the potential uses of their personal information. Some forms do not contain the Privacy Act notice, but the information collected is covered by State-30, Personnel Payroll Records.

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

An individual can decline to provide information on the forms that are used in DIS, but this could result in a negative outcome on the desired action (i.e. payroll not being processed properly, claims not being paid on time, etc.)

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?

As stated in the previous section, record subjects can refuse to provide information, but this lack of complete information could delay or hinder DIS's processes.

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.

Through State-30, Personnel Payroll Records, record subjects are notified of a collection of their personal information. In addition, they are free to refuse to provide all requested data, though this could result in a delay or hindrance in DIS's processes.

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 Records Notice 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 Public Trust security clearance level in order to gain access to the Department's unclassified computer network. To access the electronic records maintained, 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 refrain from prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning the individual a logon. A system use notification ("warning banner") is displayed before logon, 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 records must be authorized by a 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.

Due to the access controls and safeguards in place for DIS, the privacy risk resulting from unauthorized access to the system in question is mitigated.

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.