PRIVACY IMPACT ASSESSMENT

Document Imaging System PIA

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Date of completion of this PIA: July 2022
(b) Name of system: Document Imaging System
(c) System acronym: DIS
(d) Bureau: Comptroller and Global Financial Services (CGFS)
(e) iMatrix Asset ID Number: 871
(f) Child systems (if applicable) and iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

DIS converts paper records to electronic files by scanning new submissions as well as existing paper files for current and retired Department of State (Department) employees, their beneficiaries, and contractors. The system also accepts electronic files (email, forms, documents, etc.) that in the past would be printed out for filing. This system provides electronic filing and storage for data collected for CGFS compensation or financial transaction service activities. This electronic filing enables account managers and technicians to accomplish their tasks faster and without the requirement to move paper files back and forth from physical storage.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

Documents maintained in DIS include information on employment, retirement pay, general accounting, vendor transactions, accounts receivable, cashiering, and other compensation and financial management services. These documents collect name, work address, personal phone number, personal email address, place of birth, photo, social security number, tax identification number, date of birth, age, marital status, employee identification number, vendor information, financial banking information, beneficiary, and insurance information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

The legal authorities for collecting the information varies by client office within CGFS collecting the data:

General:

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);
31 U.S.C. 901-903 (Agency Chief Financial Officer's Act).

Compensation Data:

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).

Financial Management (Accounting, Disbursing, Claims) Data:

The Federal Financial Management Act (FFMIA) of 1996.

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Personnel Payroll Records, STATE-30
  Global Financial Management System, STATE-73

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):

February 11, 1998
July 15, 2008

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  A-05-xxx-xx (from the Department of State Records Disposition Schedules. The entire 05 series is dedicated to the CGFS bureau records. The DIS system may contain imaged documents from any record type described in this series.)

- Disposition Authority Number:
  NN-170-072, item 1a, item 3-16, item 18-27, item 29-32b
  N1-059-01-08, item 1a-18d
  N1-059-10-12, item 1-5
  N1-059-86-03, item 1
  N1-059-99-01, item 4a
  N1-059-99-11, item 1a-3b
  N1-059-99-18, item 1a(1)-6
  NC1-059-77-26, item 9
  NC1-059-78-14, item 1a-1b
  NC1-059-79-1, item 1
  NC1-059-80-14, item 1a-1b, item 2, item 4-6
  NC1-059-81-04, item 1, item 2b, item 4
  NN-164-098, item 1-2
  NN-166-004, item 8a-8b
  NN-170-072, item 33-34, item 36-37, item 49-52, item 54a-81, item 86, item 90-92h, item 100-101, item 106c-109, 123, item 128, item 133-142, item 144-150, item 152-157
  NN-173-075, item 2-3, item 6, item 8-13e, item 15-16, item 21-24
  NN-173-139, item 1
  NN-173-226, item 1
  NN-173-127, item 1, item 6
  DAA-GRS-2013-0003-0001 (GRS 1.1, item 010)
  DAA-GRS-2013-0003-0002 (GRS 1.1, item 011)
  DAA-GRS-2013-0005-0003 (GRS 3.1, item 051)

DAA-GRS-2013-0006-0008 (GRS 3.2, item 051)
DAA-GRS-2014-0004-0001 (GRS 2.5, Item 010)
DAA-GRS-2016-0013-0001 (GRS 1.1, Item 001)
DAA-GRS-2016-0015-0001 (GRS 2.4, item 010)
DAA-GRS-2016-0015-0003 (GRS 2.4, item 030)
DAA-GRS-2016-0015-0004 (GRS 2.4, item 040)
DAA-GRS-2016-0015-0007 (GRS 2.4, item 061)
DAA-GRS-2017-0003-0002 (GRS 5.2, item 020)
DAA-GRS-2017-0005-0001 (GRS 1.1, item 080)

- Length of time the information is retained in the system:
  The retention periods for records maintained in DIS vary from 3 to 99 years, depending upon the specific type of record.

- Type of information retained in the system:
  Compensation and Financial Management information.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☐ Members of the Public
☒ U.S. Government employees/Contractor employees
☒ Other - Annuitants

(b) On what other entities above is PII maintained in the system?

☒ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?

The collection of SSNs varies by client office and their collection requirements. Authorization comes from the following:

- 5 U.S.C. 301 (Management of the Department of State)
- 31 U.S.C. 902 (Agency Chief Financial Officer's Act).22 USC 4071h (FSPS General and Administrative Provisions), The Federal Financial Management Act (FFMIA) of 1996.
- 22 USC 4071h (FSPS General and Administrative Provisions)
- The Federal Financial Management Act (FFMIA) of 1996.

(d) How is the PII collected?

Each client office collects completed electronic or paper forms, correspondence, and other documents that are generated by Department employees, retirees, their beneficiaries, and contractors via email, cables, and other official channels. Forms, correspondence, and other documents are then scanned or imported into DIS. Electronic submissions are stored and preserved in the format in which they are received to ensure data integrity. Typically, submissions are in the form of PDFs and e-mails but DIS will also accept other file formats and maintains these files in their original form.

(e) Where is the information housed?

☒ Department-owned equipment
☐ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

(f) What process is used to determine if the PII is accurate?

The data are reviewed by client office personnel when the information is originally submitted on electric or paper forms. The accuracy of the information is dependent on the quality controls established by each client office when forms are processed. Since DIS does not collect data directly from an individual, it is the responsibility of the client office to ensure the accuracy of the data when they receive it from the individual.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Yes, the system is an electronic document storage system. Information is as current as the documents scanned into the system. Information in the forms cannot be updated once in the system; however, new forms associated with the employee, vendor, or customer can be added to the logical folder containing like forms.

(h) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources nor is the information publicly available.

(i) How was the minimization of PII in the system considered?

The types of documents (containing PII) stored in DIS have been reviewed by the Managing Director of Global Compensation and determined to be required data to meet the needs of the business.

5. Use of information

(a) What is/are the intended use(s) for the PII?

Specific information and use vary by client office. Overall, the intended use for the PII within DIS is for CGFS compensation or financial transaction service activities. DIS simply provides the electronic storage and retrieval functions of the PII in order to replace physical paper filing in client offices.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes. Document Imaging System is designed to provide client offices with the ability to index, store, search for, and retrieve documents electronically. Some of these documents contain PII.

(c) Does the system analyze the PII stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the PII?

Manual analysis is done on scanned forms/documents by indexing key fields for retrieval purposes. Each client office defines their key fields and populates/verifies the indexing when documents are scanned.

(2) Does the analysis result in new information?

No, key fields contain data derived from the forms/documents submitted.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☒No

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal: No data are shared with other offices outside of the owning office. Client offices must have a DIS account to access the system and each office has their own DIS application for their specific business process.

External: No information will be shared outside of the Department.

(b) What information will be shared?

Internal: N/A

External: N/A

(c) What is the purpose for sharing the information?

Internal: N/A

External: N/A

(d) The information to be shared is transmitted or disclosed by what methods?

Internal: N/A

External: N/A

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal: N/A

External: N/A

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

DIS does not directly collect information from record subjects. Each client office is responsible for providing notice to individuals to whom they are providing service concerning the collection of data associated with the various forms eventually scanned into DIS.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?

☐Yes ☒No

If yes, how do record subjects grant consent?

If no, why are record subjects not allowed to provide consent?

As noted in 7(a), DIS does not collect information directly from individuals, it only stores completed forms and documents. Each client office is responsible for ensuring that their customers have been provided the opportunity to grant consent.

(c) What procedures allow record subjects to gain access to their information?

DIS does not collect data directly from individuals. Retrieval of the documents stored in DIS would be through the respective client office. Each client office that collects data for storage in DIS has procedures in place for allowing individuals to request and obtain the information that client office collects.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

This system does not collect information directly from the record subject. If an individual wishes to correct inaccurate or erroneous information, they would request that update through the client office. This would then be reflected in DIS when the client office scans additional forms or correspondences into the system providing artifacts of the processing of that correction in the system of record.

(e) By what means are record subjects notified of the procedures to correct their information?

DIS does not directly collect information. Each client office is responsible for providing amendment procedures to individuals to whom they are providing service.

8. Security Controls

(a) How is all of the information in the system secured?

All system security configurations are done per Bureau of Diplomatic Security's (DS) Security Guidelines where they exist (e.g., Windows Server, Internet Information Services (IIS), Oracle) and the other custom components are configured per vendor best practices for security. Access to the backend (i.e., server, database) is restricted to the Office of Global Systems Operations (CGFS/GSO) staff. Windows/Active Directory

(AD) accounts and groups are used to limit access to the operating system, system files and application/database files. Access to user management controls is restricted to the CGFS Information Systems Security Office (ISSO).

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Each client office has its own roles for configuration. The director of each client office determines what roles will be utilized for that client office. Supervisors submit requests for staff access to the system and the CGFS ISSO grants staff access to DIS. The CGFS ISSO then provisions access to the client instance with the requested role(s). The staff only has access to the data imported into DIS for that particular client office.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Internal access to DIS is limited to authorized staff with a need to access the system in the performance of their official duties. All users maintain at 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 prohibited activities (e.g., curiosity browsing). To access DIS specifically, a user must have access approved by a supervisor and provisioned by the CGFS ISSO. The system uses Single Sign-On, so the user's AD account is provisioned with access to DIS. Users are required to have a need to see the information before being granted access. Each client office has its own DIS instance with separate database and secure electronic storage location. Within each client instance, role-based security is implemented to further distinguish least privilege and to ensure need to know requirements are maintained.

(d) How is access to data in the system determined for each role identified above?

The Director of each client office determines what roles will be utilized for that client office. Staff within each client office can submit access requests to the CGFS ISSO to gain access. Such requests must be accompanied by the review and approval of their supervisor. The CGFS ISSO then provisions access to the client instance with the requested role(s) using the requestor's AD user account.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

Completed applications are reviewed and approved by the Information System Security Officer (ISSO) prior to assigning the individual an account. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity (expected and unexpected) is monitored, logged, and audited at the operating system/file, database, and application levels by the ISSO. Detection of any unexplained activity would trigger an Incident Response action. Annual audits are done to review user accounts and access levels.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All users are required to complete computer security and privacy awareness training prior to being given access to the system. The mandatory computer security (PS800 Cyber Security Awareness) training must be completed yearly in order to retain access and the privacy awareness (PA318 Protecting Personally Identifiable Information) training is required to be completed every two years. Both ensure that users understand the proper protocols for protecting the vast amounts of PII they have access to.