US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2025

OPDIV:

ACF

Name:

Strategic Work Information and Folder Transfer

PIA Unique Identifier:

P-6739401-154848

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Significant System Management Change

Describe in further detail any changes to the system that have occurred since the last PIA.

The system has changed ownership from the Office of the Secretary (OS) to the Administration for Children and Families (ACF)/Office of the Chief Information Officer (OCIO). ACF will be conducting a Re-Authorization to Operate (Re-ATO) on the system.

In 2024, Sole Solutions Inc. (SSI)is funded to provide the Strategic Work Information and Folder Transfer (SWIFT) Digital Mail Solution. The SWIFT Digital Mail solution automates the incoming mail within ACF's correspondence process. Mail items received at ACF will be scanned and converted into a digital image that is securely delivered to the component's appropriate resource mailbox. Leveraging automation of classification and distribution of received mail, eliminates the need to manually consolidate, organize and disperse the incoming mail. SWIFT Digital Mail is an existing application at Centers for Medicare and Medicaid Services (CMS) that has successfully passed a security assessment for a Federal Information Security Modernization Act (FISMA) Moderate

system. No new code development was done for the ACF version of Digital Mail and the security boundary did not change.

Describe the purpose of the system.

The purpose of the Strategic Work Information and Folder Transfer (SWIFT) system is to collect, route, track, and manage correspondence, regulations, memos, invitations, requests for meeting, briefings, and reports to Congress. These documents come from the general public, Congress, state and local government officials, and internal Health and Human Services (HHS) offices.

ACF owns one of the three SWIFT instances, which supports users from the Department, ACF, Substance Abuse and Mental Health Services Administration (SAMHSA), Office of the Assistant Secretary for Health (OASH), the Assistant Secretary for Preparedness and Response (ASPR), and the Assistant Secretary for Planning and Evaluation (ASPE). The Department can transfer correspondence they receive to the specific operating division (OpDiv) that has the subject matter expertise to respond.

Mail items received at ACF will be scanned and converted into a digital image that is securely delivered to the component's appropriate resource mailbox; the resource mailbox is internal to ACF and restricted to authorized personnel for access and response management.

Sole Solutions Inc. (SSI) developed a connector from SWIFT to ASPR SharePoint. Office of the Secretary (OS)/Office of Documents and Regulations Management (ODRM) staff scan the correspondence/documents into the Secretary's Policy System (SPS) and transfer it to ACF SWIFT. And then Final responses originated from OS/ODRM are routed back to the SPS system in OS/ODRM, while those that originated from ACF SWIFT are routed into ACF SWIFT. There are Interconnection Security Agreement (ISA) for Assistant Secretary for Preparedness and Response (ASPR) and SPS.

Describe the type of information the system will collect, maintain (store), or share.

The SWIFT system maintains and stores the following types of information:

Public Relations information to include correspondence submitted directly by public citizens (names, addresses, email addresses, phone numbers, dates of letters, to whom the letter is addressed, names of signatories, topic of letter); the information is used to create responses for United States (U.S.) Congress requests.

Congressional Liaisons Operations information to include any correspondence data (including a release form from a constituent and the constituent's information, to possibly include social security number (SSN), dates of birth, etc.) associated with formal requests from Congress. This information isn't entered into a field in the system but is kept on the document stored within the system.

Payment information in the form of applications and payment details.

Social Services information related to social welfare services extended to children and adults with special needs, including family life education and counseling, adoption, guardianship, foster care, and rehabilitation services.

Personally identifiable information (PII) to include such data as SSNs, government-issued identifiers (IDs), medical history, employment history, photographic identifiers, driver's license numbers, vehicle identifiers, biometric identifiers, and legal documents (Memoranda of Understanding, Memoranda of Agreements, and Litigation Hold documents).

As for medical history and HIPAA compliance, the Security Rule requires regulated entities to implement reasonable and appropriate administrative, physical, and technical safeguards for protecting Electronic Protected Health Information (ePHI). SWIFT meets this requirement by virtue of being a FISMA-Moderate system. SWIFT is not a public-facing system and is behind the HHS firewall.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

SWIFT is used to collect, route, track, and manage correspondence, regulations, memos, invitations, requests for meetings, briefings, and reports to Congress. The documents scanned into SWIFT are received from individuals and organizations in the general public, Congress, state and local government officials, and internal HHS offices containing any concerns and/or inquiries. SWIFT also

permits indexing, retrieval, and storage of these documents as well as workflow management (for tracking the process of responding to inquiries). Currently all information within SWIFT is kept permanently. Documents scanned into SWIFT are received from various sources, stored as scanned attachments, and kept permanently in the system. The Personally Identifiable Information (PII) in SWIFT originates from documents scanned into the system, which are received from individuals and organizations within the general public. SWIFT does not utilize any of the PII stored in the system.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Notes
Legal Documents
Education Records
Employment Status
HHS ID of SWIFT users only.
There is an element of unknown data that may be stored in the unstructured data consisting of scanned, attached files related to the correspondence.

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Correspondents may include anyone that chooses to write to ACF, SAMHSA, OASH, ASPE, and ASPR.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII collected from the inquiring party is used for the agency to provide a direct response to the individual or inquiring organization. The primary purpose of the PII collected from system users is to handle system authentication.

Describe the secondary uses for which the PII will be used.

There are no secondary uses of PII.

Identify legal authorities governing information use and disclosure specific to the system and program.

5 U.S.C. § 301, Departmental Regulations.

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

Correspondence Tracking Management System (CTMS),'' HHS/CMS/OSORA No. 09–70–3005

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Other Text Entry

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Office of Management and Budget (OMB) information collection approval requirements are not applicable.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Per the Interconnection Security Agreement between the Administration for Children and Families (ACF) and the Immediate Office of the Secretary (IOS), the operation pertains to the specified technical and security requirements regarding the interconnection between the Strategic Work Information Folder Transfer (SWIFT) system and the Secretary's Policy System (SPS).

The standard benefits that can be obtained between the interconnected systems can range but are not limited to:
The exchange of data and information between specific users.
Customized levels of access to proprietary databases.
Potential 24×7 communications.

ACF SWIFT receives correspondence in the form of unstructured data (example: letters) and structured data (example: sender's name) from SPS. After processing, ACF SWIFT sends response letters and structured data about the correspondence back to SPS for the purposes of tracking and managing executive correspondence.

Describe the procedures for accounting for disclosures.

The SWIFT system maintains an accounting of disclosures which can be provided upon official request. The account contains the date, nature, and purpose of inquiry and the name (s) and address(es) of each correspondence recipient.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

For public inquiries, there is no process in place because the SWIFT system does not request or elicit information from individuals. The purpose of the system is to manage responses to public inquiries, which are made voluntarily.

For SWIFT users, there is no process in place because users provide their PII voluntarily.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

There is no method for individuals to opt-out of the collection or use of their PII as there is no direct interaction with the SWIFT system. The collection of PII is unsolicited; individuals that are submitting inquiries, correspondence, or other messages to HHS or the OpDivs are doing so voluntarily, and those messages are logged into SWIFT for tracking.

If an individual or organization writes to HHS or the other OpDivs and does not provide any identifying information, then the correspondence is labeled as "anonymous" in SWIFT and no response is provided.

For SWIFT users, there is no method to opt-out because users submit their PII voluntarily.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

For public inquiries, there is no process in place because constituents provide their PII voluntarily.

For SWIFT users, the SWIFT system will follow the ACF solution delivery life cycle process for any changes to the system. This will include any major or minor changes requested by other SWIFT stakeholders, as well as the SWIFT annual “Tech Refresh”. The ACF Software Development Lifecycle (SDLC) process includes a standard change request form that requires the project team to identify who and how communication will be provided to the system users prior to the change implementation.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

When an individual receives a response to their inquiry or other message, they can use this avenue to share any concerns with their PII being inappropriately obtained, used, or disclosed. The OpDiv point of contact that responded to their inquiry can assist in resolution in the event that an individual would like to make a change or ask how their information is being used or disclosed.

If a SWIFT system user has a concern with their PII or needs to correct an inaccuracy, they can contact the SWIFT help desk via phone. The phone number is provided to the users upon account creation and periodically during on-site visits conducted by the direct contractor.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

The PII collected from individuals and organizations making an inquiry is used for transactional purposes only, meaning the Department or OpDiv responds to the inquiry as needed and that is the end of the interaction with that particular record. Given this functional use, there is no process in place for periodic reviews of this information.

For SWIFT users:

Accuracy

A user list is distributed to each SWIFT stakeholder point of contact to confirm whether the accounts are still required or can be disabled. The user credentials themselves are not maintained in SWIFT so the accuracy (with exception of the SWIFT role), integrity, and availability is handled outside of SWIFT by Windows Active Directory which provides authentication services for the users.

Availability

For SWIFT system users, PII availability is verified quarterly when a user list is generated from the SWIFT system by the SWIFT O&M Contractor. The user list is distributed to each SWIFT stakeholder point of contact to confirm whether the user accounts are still required or can be disabled. If there are any issues with generating the user list (thus the availability of PII), the SWIFT O&M Contractor fixes the issue.

Integrity

A user list is distributed quarterly to each SWIFT stakeholder point of contact to confirm whether the accounts are still required or can be disabled. The list is sent by only the Sole Solutions, Inc (SSI) Service Desk Manager to only bona fide stakeholders and any requested changes are accepted from only those stakeholders. Only designated SSI employees with SSI-privileged accounts can modify or delete accounts within the SWIFT system.

Relevancy

For SWIFT system users, data relevancy is handled through a quarterly review process.

Overall, SWIFT is encrypted with Transport Layer Security (TLS) 1.2 for Data in transit and Advanced Encryption Standard AES-256 for data at rest. The SWIFT system uses Security Information and Event Management (SIEM) tool to collect logs on the system. SWIFT servers have been configured to send alerts to operations team and security personnel in the event of an audit processing failure.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

SWIFT users are limited to OpDiv employees that contribute to the review and response of correspondence. SWIFT administrators (direct contractors) are broken into Tier II and Tier III level personnel to handle daily operations and maintenance, which includes user account creation and trouble shooting. Only Tier III personnel have create, read, update, and delete (CRUD) access to the SWIFT data.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

System users are granted only the access necessary to perform their job. This level of access is granted based on each user's position description as identified on the employee's Official Form-8. In addition, the system is designed based on set permissions therefore, employee access and use are based on their need to know. A user will only have access to their SWIFT folders and documents that has been sent to them.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Annual HHS Mandatory Cybersecurity Information Systems Security Awareness and Privacy Awareness training are required and documented as completed yearly by all IOS and Contractor users of SWIFT. In addition prior to accessing the system each employee must accept the rules of behavior prior to accessing their computer system that gives them access to SWIFT.

Describe training system users receive (above and beyond general security and privacy awareness training).

All SWIFT administrators are required to complete role-based training. Evidence of this is maintained by the direct contractor.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Below is the General Records Schedule (GRS) for the Strategic Work Information and Folder Transfer (SWIFT) Privacy Impact Assessment (PIA).

(NARA) disposition authority DAA-0468-2011-0006-0003 is superseded.

DAA-0468-2023-0002
Disposition Instruction: Permanent: Cutoff: Cut off four (4) years after the files were created.
Transfer to the National Archives twenty-five (25) year(s) after cutoff.
Disposition Authority: DAA-0468-2023-0002-0001.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

The SWIFT system is being accredited in alignment with ACF's moderate system baseline and has the following controls in place to secure PII:
Administrative - only federal staff and direct contractors are approved for system user accounts; role-based access control (RBAC) is in place to limit access to PII, access is restricted to occur on government furnished equipment (GFE), suspicious activity is reported to government officials.
Technical - the system sits behind the HHS firewall (meaning only accessible within the HHS network), multi-factor authentication used in conjunction with an Active Directory, all traffic is encrypted, audit logs in place, anomalous activity is monitored (e.g. system activity outside specific hours).
Physical - the system is housed in a Program Support Center (PSC) data center that employs the following: maintain a personnel listing that is reviewed and approved by the data center officials, all personnel require badges in order to access the data center and dual authentication through badge readers followed by biometric scans is in place, security guards are present at all building entry and exit points, camera systems in place to continuously record and monitor building activity.