US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

OS

Name:

Strategic Work Information and Folder Transfer

PIA Unique Identifier:

P-6739401-154848

The subject of this PIA is which of the following?

Minor Application (child)

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.

Agency

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

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

None

Describe the purpose of the system.

The purpose of Strategic Work Information and Folder Transfer (SWIFT) 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 HHS offices. The Office of the Secretary (OS) Immediate Office of the Secretary (IOS) SWIFT application is located on servers maintained by the Management Application Hosting Center (MAHC) and is being used by the Assistant Secretary for Planning and Evaluation (ASPE), the Assistant Secretary for Preparedness and Response (ASPR), the Administration for Children and Families (ACF), Office of the Assistant Secretary for Health (OASH), and Substance Abuse and Mental Health Services Administration (SAMHSA) to house their SWIFT modules.

In March 2016, the Office of the Secretary (OS) Immediate Office of the Secretary (IOS) stopped using SWIFT as its correspondence control system, but the mentioned HHS offices continue to use SWIFT.

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

The type of information the system collects are from scanned documents received by the office and correspondence generated in response to those documents. The information includes structured data about the individual, organization or contact that mailed or emailed the documents. Contact information can be name, organization, address, city, state, zip code, telephone and e-mail.

Correspondence could conceivably contain any kind of information, including health, financial, commercial, congressional, emergency disasters, invitations, or HHS related information.

Personally identifiable information (PII) includes contact information (if the author of the original correspondence is an individual) and may include any other type of information provided by the correspondent.

Information provided is entirely voluntary, and consists of unsolicited correspondence.

The SWIFT contractors are direct contractors and they maintain SWIFT remotely through the HHS assigned laptop via HHS virtual private network (VPN) using their HHS Elevated Alt Card provided by the HHS Office of Security and Strategic Information (OSSI).

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

SWIFT is a correspondence control system in use by the Assistant Secretary for Planning and Evaluation (ASPE), the Assistant Secretary for Preparedness and Response (ASPR), the Administration for Children and Families (ACF), Office of the Assistant Secretary for Health (OASH) and Substance Abuse and Mental Health Services Administration (SAMHSA). The documents scanned into SWIFT are from individuals and organizations in the general public, Congress, and state and local government officials, and contain their concerns and inquiries. SWIFT also permits indexing and storage of these documents, retrieval, workflow management (for tracking the process of responding to inquiries). The information is permanent.

The system generates tracking numbers used for retrieving stored correspondence.

The contractors are direct contractors who maintain SWIFT remotely through the HHS assigned laptop via HHS VPN using their Elevated Alt Card provided by the HHS Office of Security and Strategic Information (OSSI).

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

Yes

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

Name

E-Mail Address

Mailing Address

Phone Numbers

System may contain any information relevant to inquiries made by correspondents e.g., financial

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Correspondents could include anyone that chooses to write to the Secretary's Office. IOS SWIFT Contractors are considered to be direct contractors.

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

SWIFT is used to track responses and correspondence, which can include providing information, policy interpretations, responses to journalistic inquiries, and many other kinds of correspondence.

PII may be shared with appropriate points of contact in order to respond to the correspondence. Correspondence may include inquiries, requests for resolution of concerns, or any other matter. The information is shared with offices within the Department of Health and Human Services (DHHS) who may be able to assist in appropriately responding to correspondence sent to the Secretary.

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

There are no secondary usage 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.

Secretariat’s CORR Control System 09-90-0037

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

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

This is not applicable. Information in the system does not require answers to any questions, and is not collected in a specific format that will require the Office of Management and Budget information collection approval.

Is the PII shared with other organizations?

Yes

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

Within HHS

Information is shared with Staff Divisions (StaffDivs) and Operating Divisions (OpDivs) system users. Access is only given where HHS OpDivs and StaffDivs author, clear or provide direct replies to regulations, correspondence and memos. PII is also disclosed to all Executive Secretary employees, HHS Regulations offices, HHS Office of the Secretary (OS) Immediate Office of the Secretary (IOS) Scheduling and Advanced users who daily use SWIFT, but they only see information pertaining to cases that they author or have given permission to see by the agency for information only purposes.

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

There are Interagency Agreements in place for the use of the IOS SWIFT servers by ACF, ASPE, ASPR, OASH and SAMHSA. These HHS offices jointly pay to use the servers for their SWIFT systems. As of March 2015, IOS stopped using SWIFT as its correspondence system.

Describe the procedures for accounting for disclosures.

The SWIFT system maintains an accounting of disclosures in that the dates, nature, purpose, names and addresses of each correspondence is captured by the system

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

Individuals who make inquiries to the Secretary or the offices that have modules in SWIFT servers are automatically documented in SWIFT. Currently there is no prior notice given to inform the inquirer that their name, phone number and address sent to HHS will be logged into SWIFT due to their inquiry. However, prior to the end of the 1st quarter, IOS plans to modify the system to include an automatic response to be emailed to the inquirer email address.

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.

SWIFT does not request PII from individuals. However, individuals are given the opportunity to opt-in to the collection of their information when they send PII themselves in the correspondence provided through the system. As a result no need to provide an opt-out methods.

Information is used for the purposes for which individuals request that it be used, which is to address concerns or request responses to inquiries. If a person opts out of providing his/her name and/or organization, the name does not appear on these documents, and is labeled as "anonymous" for action. Thus the OPDIV or StaffDiv will not be able to respond to the requester.

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

Major changes would need to be reflected in the System of Records Notice (SORN), which would be available to the public. Use of the system other than this is transactional and individuals are unlikely to need any notification of major changes.

Individuals provide information for the purposes of requesting that the Secretary provide responses to inquiries or take certain actions. The only use of the PII is to attempt to respond to requests, which was the senders' intent in providing it.

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.

Individuals receive responses from appropriate points of contact (such as OpDivs) in response to their correspondence. If their concerns include concerns about the use of PII, the point of contact (POC) would assist in resolving complaints regarding PII use as well.

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

Information is used transactionally and there would be no value to periodic reviews and updates.

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

Users:

HHS correspondence and responses

Administrators:

user account maintenance and correspondence assignments and processing

Developers:

System enhancements

Contractors:

System administration

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

The SWIFT Administrators and developers are contractor employees who do not enter information into SWIFT. Only Government employees (users) review the correspondence received to enter PII into the system. System administrators and developers who are contractors will be able to see PII (Name, organization and phone numbers) of users for account creation and trouble shooting problems only.

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 jobs. 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 as information only by the authoring agency.

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. Administrators of SWIFT are also required and documented as have taken the Role -Based Training.

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

None

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.

Records are maintained indefinitely using the records management schedule. Hardcopies of correspondence are sent to a Retention Center. The authority is DAA-0468-2011-0006-0003 and the Master Files are permanent. Cut off of at the end of the fiscal year in which correspondence was created or received. Transfer to the National Archives in 4 year blocks immediately after cut off. National Archives and Records Administration (NARA) is determining the appropriate Records Control Schedule (RCS) Job Number for all of the PII maintained in the system and the PII should be maintained until a determination is provided.

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

Controls are selected and implemented consistent with all federal requirements. A certification and accreditation package has been assembled and is updated as required. Administratively, only internal users with network and user accounts can access the system. Technical controls include intrusion detection and the use of firewalls. Physical controls include hosting the server at a secure facility.