US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2024

OPDIV:

ACF

Name:

Solution Delivery System (SDS)

PIA Unique Identifier:

P-4092056-930231

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.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The purpose of Solution Delivery System (SDS) is to support the current Administration for Children and Families (ACF) operations, increase efficiency, reduce cost, and enhance the overall customer experience. By providing a structured approach to solution delivery, an SDS can help ACF achieve their goals more effectively and efficiently. The SDS will collect the Name, Phone Number, and Email address of ACF’s customers (ACF team members, both Feds and contractors) when requesting service.

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

Solution Delivery Service (SDS) will collect and store the following general information for all tickets: unique ticket number, requester name, requester program office, official email, phone numbers, dates, request category, and description with a priority and/or risk level assigned to each by the OCIO Service. The information collected will be stored for 3 years.

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

Solution Delivery Service (SDS) will provide the ACF OCIO Service Desk with a tool for incident management, change management, and service requests (the Catalog). The key goal for this tool is to provide business solutions more effectively and efficiently.

Incident Management – Is the process of identifying, analyzing, and resolving incidents that occur within ACF, it can be described as an event that disrupt the normal operation, for (example email server is down, or mid server is down)

Change management – Is the process planning implementing, and monitoring changes to ACF processes system, or service after being reviewed by the Change Advisory Board (CAB). It minimizes the negative impact of changes and it also allow to keep track of all changes and when they are implemented.

Service Request – Is a process of requesting technical and business needs through service catalogs; access, software or equipment can be requested through this process. They are typically initiated through ACF service desks.

Information (unique ticket number, requester name, requester program office, requester's official email, requester phone numbers, dates, request category, and description) collected by Solution Delivery Service (SDS) is used to track the request from initiation through completion, communicate with the customer/users, and provide metrics for analysist on system issues, recurrence of incidents, and to determine problems (root causes) of issues in systems so that they can be addressed.

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
Phone Numbers
Unique Ticket #; Employee ID
Request Category
Service Description
Request Date
Requester Program Office Information

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

PII is used to identify specific user who are making request for either an incident or request.

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

The PII has no secondary use

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

5 USC 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.

OPM/GOVT-1 General Personnel Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Non-Applicable

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable, an information collection number is not needed.

Is the PII shared with other organizations?

No

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

There is no formal process in place to notify individuals that their information will be collected. Once a user calls, the informal notification process requires the information to be requested and collected in order to provide them with service.

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 are fields on the intake forms for an email address and phone number to be input by the customer – or they provide it to use directly via an email or phone call to us. The information is needed to deliver the requested service to the customer. There is no ability to opt-out, as the collected information is needed to communicate to the user.

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

ACF Tech / ACF OCIO would put out a broadcast communication possibly via email and a banner on the customer facing SDS page. We could do either an ACF-wide communication or we could send out notification to only those uses within the SDS system.

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.

Users would need to contact the Administration for Children and Families (ACF) Incident Response Team (IRT), at acf_irt@acf.hhs.gov.

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

Integrity: Access to PII is provided only to approved users with a need-to-know. Audit logs capture user activity. Multi-factor authentication is required for access to the system. ACF Tech/OCIO uses a variety of manual and automatic tools and processes to limit risk of unauthorized access. User accounts are disabled via HHS Lightweight Directory Access Protocol (LDAP).

Availability: Ensuring timely and reliable access to information. ACF ServiceNow instance resides on the ServiceNow Data Center / Cloud as part of the HHS ServiceNow Software as a Service (SaaS).

Accuracy: Data is provided directly by individuals about themselves and via HHS LDAP. If the user calls the Service Desk, user repeats back information to validate.

Relevancy: Users can correct any information via the Service Desk; it is also updated via HHS LDAP connection to ensure relevancy for providing superior customer service to users.

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.

Access is based on Role Based Access Control (RBAC) which is determined by the system owner or the service desk lead.

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.

There is access control list (ACL) in place that restricts or allow users to view tables and data based on their roles and Job assignment

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.

There is mandatory annual compliance training which includes privacy and security training. Also, during the onboarding process, all team members take the Health and Human Services (HHS)/ACF Privacy Training and Rules of Behavior.

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

No additional training provided.

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 covered by General Record Schedule (GRS 3.2): Information Systems Security Records Item 031

Item 031 System access records: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

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

PII is secured using Personal Identity Verification (PIV) cards for authentication as well Virtual Private Network (VPN) access and RedHat Single Sign-On (SSO). Username and password are

also used to access the platform. Cyber Security Training from HHS is also offered to ensure users are familiar with privacy policies.
Administrative: ServiceNow utilizes user roles to control access to features, data, and PII. Only government-authorized users who have passed adjudication, have received their Badge, and have the need to access the information are added by the ServiceNow administrator to the user roles that have access to PII data. These users are removed by the ServiceNow administrator during the offboarding process, as per the Standard Operating Procedure (SOP). These users are on the Operations & Maintenace (O&M) team and need access to support the ACF community.

Technical: The Service Solutions Division (SSD) team utilizes the features within the ServiceNow application, such as user roles, to ensure only authorized people can access areas containing the PII. The team also utilizes RedHat SSO for multi-factor authentication, which requires an active PIV as well as connects to the HHS/ACF Active Directory (AD). This connection to the AD automatically syncs active/inactive HHS/ACF users.

Physical: N/A. ServiceNow is a SaaS product.