US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/23/2026

OPDIV:

ACF

Name:

ACF Workspace for Analysis, Research, and Execution

PIA Unique Identifier:

P-5831788-658352

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

Significant System Management Change

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

The following updates have been made:

#13-Provided further clarification on user and data governance procedures
#20- Added details regarding the legal authority to use SSN
#24- Data is shared with the Department of Homeland Security (DHS) for the purposes of combatting human trafficking.

Describe the purpose of the system.

ACF Workspace for Analysis, Research and Execution (AWARE) will serve as a secure workspace that allows for internal and external data ingestion, reuse, and analytics, enabling ACF to share and analyze data, build enterprise-level insights, enable the creation and use of cross-ACF dashboards, enable the creation and distribution of data sets to partners and stakeholders, and enable additional access for searchers, data scientists, and analysts.

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

Program Offices using AWARE for data analytics will bring their own data to be ingested into AWARE for their program's data exploration and analyses. Any data entering AWARE will already have an authorized Privacy Impact Assessment (PIA) for the systems of record. AWARE will never be a system of record, and hence this PIA is for the technological system that can be used to analyze data already covered by authorized and published PIAs on a temporary basis. For example, the Office of Refugee Resettlement (ORR) Unaccompanied Children (UC) program may use AWARE to analyze data from their operational systems of record, The Office of Family Assistance (OFA) may use AWARE to analyze a dataset extracted from their Temporary Assistance for Needy Families (TANF) data. The only datasets that may be in AWARE that are not under an existing PIA are public datasets like weather or census data.

AWARE may use on a temporary basis the following data types social security numbers, names, drivers licenses numbers, mother's maiden name, email addresses, phone numbers, medical notes, certificates, education records, military status, foreign activities, taxpayer identification (ID), date of birth, photographic identifiers, biometric identifiers, vehicle identifiers, mailing address, medical records number, financial account info, legal documents, device identifiers, employment status, medical records, medical information, foreign activities and passport number.

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

AWARE is a secure analytics and controlled-access environment that allows for approved users with varying levels of role-based privileges to allow teams of analysts from ACF Program Offices to analyze the data from their systems of record, these records can include names, email addresses, social security numbers, date of birth, medical information, medical records, foreign activities, phone numbers, driver's license number, vehicle identifiers, photos, taxpayer ID numbers, certificates, education records, military status, device identifiers, legal documents, passport number, financial records, and military status. AWARE offers the capability to conduct machine learning analyses and large-scale data manipulation with Jupyter notebooks for team collaboration and low-code interfaces to visualize data.

The secure environment is governed by strict oversight of who has access to an ACF Program Office's data, managed by the program office team itself. In some cases, ACF Program Offices may do joint projects where each brings their own datasets and analyst teams, and the collaboration would define how data may be shared within or external to those specific Program Offices. Only office-designated AWARE Administrators have the permissions to add users to AWARE, and the system owner is automatically alerted when new users are added. AWARE Administrators and the System Owner also conduct at-least monthly user reviews to ensure access is still needed. AWARE Administrators are designated through a formal process that documents the designees' responsibilities and office leadership acknowledgement. The responsibilities include:

- Coordinating with the System Owner (SO), System Security or Privacy Officer(SSPO), ACF Chief Information Officer (CIO) and Chief Information Security Officer (CISO), system developers, and system operations team regarding any setting configuration changes, onboarding of non-ACF users, potential changes to the scope of data, or any other modification that affects the Authorization to Operate (ATO) to determine appropriate security controls and identifying resources to implement those controls.
- Supporting the definition and execution of interconnection security agreements (ISAs) or memorandums of understanding (MOUs) before connecting with other ORR systems or sharing sensitive data.
- Verifying that any of ORR's data that includes personally identifiable information (PII) and is used in AWARE is the minimal amount necessary to accomplish mission objectives.

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
Mother's Maiden Name
Vehicle Identifiers
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Certificates
Legal Documents
Education Records
Device Identifiers
Military Status
Employment Status
Foreign Activities
Passport Number
Taxpayer ID
Medical Information

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors
Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

All PII, which would be extracted from existing systems in Program Offices that have a completed PIA. The data from these systems would be used in the large-scale data analysis and exploration projects that the Program Office chooses to execute in AWARE.

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

Used for research, provided the PII maintained in the source system(s) is authorized for secondary use for research purposes.

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.

OFA Temporary Assistance for Needy Families (TANF) 09-80-0375

ORR Unaccompanied Refugee Minors Records 09-80-0329

ORR Division of Children's Services Records 09-80-0321

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Other HHS OpDiv

State/Local/Tribal

Other Federal Entities

Non-Government Sources

Other Non-Government Entities

Identify the OMB information collection approval number and expiration date

Not Applicable, AWARE does not require an information collection

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.

1. ISA with Unaccompanied Alien Children Portal (UAC Portal), valid through August 10, 2028
2. ISA with DHS Homeland Security Investigations Databricks E2, valid through February 26, 2026
3. (In progress) ISA with DHS Customs and Border Control Unified Immigration Portal (UIP)

Describe the procedures for accounting for disclosures.

The AWARE System Owner and ACF Tech Cybersecurity and Privacy Team conduct due diligence to ensure AWARE usage aligns with documents governing data exchanges (e.g. SORNs, memoranda of understanding, relevant statutes).

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

AWARE does not collect any new data, information in AWARE comes from ACF Program Office systems that already have processes in place for notifying individuals when data is collected.

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.

The PII collected in AWARE is collected from other systems. If an individual chooses to opt-out from the collection of their PII, this would happen when a program office was collecting data, which is prior to that data coming to AWARE.

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

AWARE is used for analytics and research purposes. The data in AWARE comes from approved collection systems that have existing notification and consent processes in place for the systems.

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.

Any issues about whether PII was appropriately obtained, used, or disclosed are processes managed by individual Program Offices for their systems of record.

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

Periodic reviews of PII for integrity, availability, accuracy, and relevance are appropriately managed by Program Offices as relates to their source systems. AWARE does have some existing processes in place for use by Program Offices within the AWARE environment.

Data Availability is made possible by making a copy of the production database on a daily basis and storing the copy for backup and potential restore situations.

Data Integrity is maintained by limiting the number of users who have write capability. This is achieved by using role-based access. Roles are separated by Program and by User Type within the system.

Data Relevancy: The relevancy of the data is maintained by each individual ACF Program Office by following the specific retention and destruction schedules for their data.

Data Accuracy: The accuracy of data is measured and audited periodically by individual Program Offices, and AWARE includes some tools that can allow Program Offices to audit data in the environment.

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.

AWARE has a hierarchy of access controls at the ACF level and by program office. Restrictions are available at the dataset and column/row level and PII is only in view for users that have been approved by program office administrators. The environment where AWARE is housed includes keystroke level monitoring and storage of monitoring 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.

The system implements Account Management which is the foundation of principle of Least Privilege and Separation of Duties which ensures that PII is only accessible to users with need to know.

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.

All personnel including both direct contractors and government personnel are required to participate in the ACF annual security compliance training and privacy training.

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

AWARE users may receive additional role-based training as needed.

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.

Data entering the AWARE system will all contain National Archives and Records Administration (NARA) retention and destruction schedules that will be applied to each dataset. These retention and destruction schedules vary by dataset. AWARE users are responsible for working with their records officers to determine specific retention schedules as needed. AWARE administrators check at least annually on whether datasets continue to have a business case to be kept in AWARE.

For example, Case Files on Unaccompanied Children, including Sponsor and Sponsor Household information, maintained temporarily within AWARE are destroyed 5 years from the cutoff date but are authorized for longer retention if business justification is provided. The cutoff date is the end of the Fiscal Year in which the UC is released from ORR program custody. The disposition authority number is DAA-0292-2019-0009.

System User accounts and related profile information are destroyed 6 years after the user account is terminated but are authorized for longer retention if business justification is provided. This retention and destruction requirement is outlined in the General Records Schedule (GRS) 3.2, Item 031 (Systems requiring special accountability for access).

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

AWARE inherits all of the physical controls of the ACF Next Generation Secure Cloud (NGSC) environment. That environment enables role-based security, row, table, and field level access controls, and keystroke level monitoring for privileged users. Further, access controls will be applied to the system via single sign on, ensuring that only users with approval will have access to limited or varying sets of PII. The flexible system allows for these controls to be based on the rules and policies of each Program Office, for each Program Office’s data asset (based on their in-force data use agreement, PIA, SORNs). Further, data will be encrypted at rest and in flight within the AWARE environment.