US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/12/2023

OPDIV:

ACF

Name:

Refugee Arrival Data System (RADS)

PIA Unique Identifier:

P-9629795-369312

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

The PIA is being updated to better describe the Tableau reporting portion of the RADS system.

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

Since the last PIA, RADS has performed normal maintenance on the system making updates to the user interface and the forms consistent with the OMB updates to data collection forms. RADS is adding additional reports in the reporting portion of the system to better communicate with the end users.

Describe the purpose of the system.

The purpose of the Refugee Arrivals Database System (RADS) is to aid the Administration for Children and Families (ACF)/Office of Refugee Resettlement (ORR) in meeting their mission to allow refugees and other populations to become self-sufficient and contributing participants in American society. The system collects and stores information on asylees (asylum applicants and asylum recipients), refugees, entrants, and other populations received from government agencies, case management agencies, and volunteer agencies (VOLAGs). RADS uses this information to provide reports to ORR leadership on geographic, ethnic, and other population characteristics to determine

the needs of these people. In addition, the information is used to provide Congress with statistical analyses to aid in determining future federal funding based on the effectiveness of the program. The RADS Tableau reporting tool is used to create dashboards and Tableau visualizations to enhance ORR's ability to analyze the results of their data collections and program effectiveness and to foster data-driven decision-making process.

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

RADS collects and stores similar data on immigrants, Cuban and Haitian entrants, asylees, refugees, survivors of torture, and victims of trafficking. The information is collected from sources including: Customs and Border Protection (CBP), Church World Services (CWS), United States Council of Catholic Bishops (USCC), United States Citizenship and Immigration Services (USCIS), Department of Justice / Executive Office of Immigration Review (DOJ/EOIR), U.S. Department of State (DOS), Department of Homeland Security (DHS), ACF/Office of Trafficking in Persons (OTIP), State Agencies, VOLAGs, Provider Agencies, and Assister Agencies.

The information collected by RADS includes the following: Alien number (A#), full name, date of birth (DOB), full mailing address (city, state, zip code), phone number, marital status, age, ethnicity, religion/denomination, nationality, refugee class, minor determination, port of entry details, arrival location, destination location, citizenship and birth country, country of origin, Immigration and Naturalization Service (INS) status, education details, English literacy determination, location and name of the organization through which the asylee came, class of administration, sponsor details, petitioner name, beneficiary name, documented type name (e.g. Passport or Green Card), documented identification number, qualifying status, migration status, certificate type and date, demographic information, and as applicable: maiden name, family details, and occupation. Dates are also collected related to: arrival, resettlement, asylum, migration, benefit eligibility, medical screenings, social services enrollment, Refugee Medical Assistance (RMA) and Refugee Cash Assistance (RCA) enrollment, end of eligibility, and application to program.

The Unaccompanied Refugee Minor (URM) case management part of RADS may contain supporting documents uploaded by unaccompanied refugee minor assistors. This data includes PDF files specific to a case that may include information on criminality, medical information or photographic identifiers and would not be included in the results of an aggregate search.

RADS also collects and stores participation and performance data from grantee refugee benefit and assistance programs and detailed instructions for providing this information. This data is used for determining program initiatives, standards, budget requests, and assistance policies. Information solicited in the reports include agency point of contact name, title and contact information, aggregated, statistical, and narrative responses. Examples of narrative responses include program accomplishments and client success stories. Individuals are instructed to exclude Personally Identifiable Information (PII) within the narrative responses.

RADS has ceased collection of Social Security Numbers (SSNs), however SSNs are still stored and encrypted within the system in older records.

RADS Tableau component will be used for sharing information with grantees, including potential PII such as names, alien numbers, location data. RADS Tableau will enforce role and agency access controls to limit the PII to only those agencies that have a business requirement for that information. Requests for user accounts in RADS require the collection of full names, phone number, work or email address, and the agency name for which the user works. Usernames and passwords are also maintained in RADS.

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

RADS collects and stores information on asylees (asylum applicants and asylum recipients), refugees, entrants, and other populations received from government agencies, case management agencies, and VOLAGs. RADS uses this information to provide reports to ORR leadership and to

Congress. ORR has numerous OMB approved forms that instruct users on the data fields for uploading. Each individual is assigned a user role to restrict access to the system on an as needed basis.

RADS includes data for ORR's URM program, which manages placement and eligibility determination information as well as outcomes information on URMs. Authorized RADS users, including care providers, state resettlement agencies, and ACF URM program staff, manually enter data into the URM component. The URM database includes information from grantee refugee benefit and assistance programs regarding their participation and performance data.

RADS collects information on all arrival populations, i.e., refugees and other ORR-served populations entering the country from overseas or at border points, and this information originates from a variety of sources. The data sources provide the information in the following ways: via authorized login to RADS or by providing the RADS technical team an encrypted copy of the data, through email or Department of State (DoS) Worldwide Refugee Admissions Processing System (WRAPS) drop box, for the team to then upload on their behalf.

ORR uses dates to conduct an annual "State Match" to confirm that individuals served by states "match" ORR eligibility requirements. During this process authorized users from state agencies upload their state data into RADS for the RADS technical team to match with federal records through a data quality process.

Performance report information (based on an OMB approved form), that is collected and maintained in RADS, is provided from various states and grantee programs. Authorized RADS users for these programs will enter the information manually.

RADS Tableau is a tool that produces reports and dashboards for the ORR community. RADS Tableau is also used for data analysis. Tableau reports follow strict development standards around the presentation of dashboards and access control to the dashboards. Limitations are set on what data is available in Tableau. Before going live, reports and dashboards are reviewed with end users and the internal data team to ensure that PII is presented to only appropriate populations.

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

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Certificates

Education Records

Passport Number

Alien Number (A#)

Demographic Data:
Marital status, age, ethnicity, religion/denomination, nationality, refugee class, minor determination, port of entry details, arrival location, destination location, arrival date, citizenship and birth country, organization through which the asylee came, class of administration, sponsor details, petitioner name, beneficiary name, Green Card, documented identification number, qualifying status, migration status, and as applicable: maiden name, family details, and occupation.
As noted above, ORR collects “other” case management file information in PDF format that does not match specific data element fields, but provides background information used to serve URMs.
Country of Origin, Immigration and Naturalization Service (INS) status

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

Employees

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

Vendor/Suppliers/Contractors

Asylees, refugees, and entrants to the United States

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The primary purpose for the collection and maintenance of PII within RADS is to authorize and create system users and system accounts for managing URM’s case management module, and for determining federal funding by state. PII is necessary for ORR to operate and maintain its refugee benefits program and for oversight of the State Match program.

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

The secondary purpose for PII use includes administering surveys, conducting the URM study, and research purposes.

Describe the function of the SSN.

SSN is no longer collected as a data element. However, SSNs previously collected under the DOJ I-643 form are still stored in the RADS database.

Cite the legal authority to use the SSN.

Immigration and Nationality Act (INA); I-643 Office of Management and Budget (OMB) approved form #1615-0070

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

INA; Refugee Act of 1980; 45 Code of Federal Regulations (CFR) Part 400 and Part 401

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.

09-80-0325 ORR Internet Refugee Arrivals Data System (iRADS)

Identify the sources of PII in the system.

Email

Other

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

URM ORR-3 & ORR-4 OMB Control No: 0970-0034
Expiration Date: 02/29/2024

URM Application OMB Control No: 0970-0550
Expiration Date: 08/31/2023

ORR-5 OMB Control No: 0970-0043
Expiration Date: 04/30/2024

ORR-6 OMB Control No: 0970-0036
Expiration Date: 12/31/2025

SOT OMB Control No: 0970-0599
Expiration Date: 02/28/2026 (proposed, still in review)

RSS Funding OMB Control No. 0970-0556
Expiration Date: 11/30/2024

DRS Forms OMB NO: 0970-0599
EXPIRATION DATE: 02/28/2026

Is the PII shared with other organizations?

Yes

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

Within HHS

Data from RADS is shared with the Office of Planning, Research and Evaluation (OPRE) on two occasions: (1) the annual survey and (2) the URM study.

Private Sector

Data from RADS that was shared with OPRE is further shared with four research firms to administer the annual survey and to conduct the URM study.
PII data uploaded by grantees may be shared with the appropriate grantees within the RADS system and the Tableau reporting system.

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

Signed memorandums between ORR and OPRE have been executed to inform the ACF Office of the Chief Information Officer (OCIO) of the data transfer and respective data security plans from ORR to the approved research firms in accordance with the applicable data routine use disclosure.

Describe the procedures for accounting for disclosures.

There is currently a Standard Operating Procedure (SOP) in place to account for disclosures. RADS System of Record Notice (SORN) describes every routine use of disclosure and to whom it is made. These include data sharing for normal operations based on user roles, restrictions for access based on these roles, and data sharing for a third-party analysis. RADS has safeguards in place in the event of an inadvertent sharing or intentional hacking of the system.

There are three types of disclosure that apply to RADS:
1. In the normal operation of RADS, data is shared within the application, using the user roles and organizations to limit who has access to which cases and data sets.
2. In some cases, a dataset is prepared for third party analysis.
3. Inadvertent sharing or intentional hacking of RADS that will cause data to be disclosed.

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

ORR populations served through RADS do not directly input their data into the system. A state refugee coordinator or a resettlement agency case worker, or other approved user, inputs the data in the system and confirms that a privacy statement has been communicated to the individual whose data is being collected.

When a new case is created in RADS, a notice showing the Privacy Act Statement (PAS) is presented to the RADS user, whose data is being collected, confirming that the statement is being communicated to the individual. For system users, the individuals are made aware of the collection through the account management process. For all other individuals with PII in the system, data collection occurs at other federal or state agencies and RADS receives a bulk data feed.

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 opt-out option, as the individuals provide their PII to the grantee to receive services offered by ORR. RADS present a statement for the grantee to acknowledge that they have notified the individuals that PII data is being collected.

Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries (e.g. FOIA request) to the System Manager. The request should include the individual's name, Alien Number, telephone number and/or email address, and address of the individual, and must be signed. Verification of identity as described in HHS's Privacy Act regulations may be required. 45 CFR 5b.5

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

Notification of major changes is provided to RADS users when a new deployment is going to be implemented in the production environment. Notification occurs via email sent to users that states when, including the date and time, the system will be unavailable. There is no process to notify and obtain consent from individuals whose PII is in the system as a result of program participation.

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 seeking to amend a record about themselves in this system of records may address the request for amendment to the System Manager. The request should (1) include the individual's name, Alien Number, date of birth, telephone number, and/or email address, and should be signed; (2) provide the name or other information about the project that the individual believes contains his or her records; (3) identify the information that the individual believes is not accurate, relevant, timely, or complete; (4) indicate what corrective action is sought; and (5) include supporting justification or documentation for the requested amendment. Verification of identity as described in HHS's Privacy Act regulations may be required. 45 CFR 5b.5

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

Data Integrity: On a quarterly basis, a log file is generated and a summation of all PII records created and modified by all users is inspected for abnormally high record creation or modification. Quality control standards are built into the application and tested with each new release, which ensure that PII data is entered in a usable and correct form. If ORR staff identify a record as incorrect and in need of remediation, an email trail is kept reflecting this change. In addition, every RADS query and transaction is stored with time stamp and user ID. These logs are reviewed on a quarterly basis to determine if possible inappropriate use of the system has occurred. All PII records are stamped with the user who first created the record and the user who modifies the record, as well as the time stamp of the action.

Data Availability: Daily backups ensure that the data may be restored in any event.

Data Accuracy: PII data in the Arrivals Module is reviewed for accuracy by overlaying annual reconciled data over original submissions. The reconciled data is supplied once a year for the prior fiscal year and contains any updates that may have occurred. URM module data is verified manually through the approval process required by an ACF agent. The ACF agent reviews cases, case progress reports, and case placement reports. Only after information is verified, does the record get approved.

Data Relevancy: The relevancy of the data is maintained by following the specific retention and

destruction schedules. In addition, user accounts are disabled after 60 days of non-use.

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

Users:

Users have access to PII for their respective cases and state match uploads or for those cases in which they have a business need. Internal users will have access to RADS for data analysis through Tableau.

Administrators:

Administrators have access to all PII in order to manage the RADS database.

Contractors:

Indirect contractors make up the administrators which have access to PII for database management and the technical team that supports data uploads.

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

For access, the RADS Program Manager (PM) determines and grants administrator access depending on need. For users required to have elevated privileges access to RADS data, the appropriate background investigations are completed by OMB.

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.

All access is controlled through the user's role and organization designation, limiting what data is accessible on the system. Access is controlled with mandatory (system enforced) controls within the application to ensure user access is limited to the minimum data required.

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 RADS users must review and sign the acknowledgment of the Health and Human Services (HHS) Rules of Behavior (RoB) prior to login. This acknowledgment must be completed annually.
All RADS users must acknowledgment that they have had yearly security and privacy training during login. The HHS Cybersecurity Awareness Training for ACF employees and contractors is accessible from the acknowledgment page. This acknowledgment must be completed annually.
Federal and direct contractor staff are required to complete annual HHS Cybersecurity Awareness training and sign the HHS RoB upon on-boarding. Indirect contractors who are users of the system are also required to complete their company's Security and Awareness Training as indicated in the contract with HHS.

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

Security and privacy awareness training is available from the RADS application during login and must be acknowledged every year. URM users are provided general user training for submitting forms via RADS for unaccompanied refugee minors.

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.

The data for RADS follows a specific retention and destruction schedule approved by the National Archives and Records Administration (NARA), DAA-0292-2016-0012-0014. All data within in RADS is considered permanent.

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

All data is stored in an Oracle database and accessed through the RADS application. Access is

controlled through the application based on user role and organization. The system is hosted in the ACF Amazon Web Services environment.
PII is secured using the following controls:
Administrative: Every RADS menu item and access level is associated with a system resource. System resources are assigned to predefined application roles, which users get assigned to. Access to PII data is tightly controlled through this resource/role methodology. The system enforces a yearly HHS RoB certification from all users and tracks compliance within the application.
Technical: Multiple tiers of security including advanced and monitored demilitarized zone (DMZ) server, firewalls, hardened web servers, hardened application (developed with anti-hacking techniques/avoiding vulnerabilities), and use of a 256-bit Secure Sockets Layer (SSL) encryption key. Server configuration adheres to contractor's strictest hardening guidelines. Data at rest in the Oracle database is encrypted.
Physical: Physical Access to Servers requires general employee badge access, data center badge access, and a key to the rack housing RADS hardware.