US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/30/2023

OPDIV:

ACF

Name:

Anti-Trafficking Information Management System (ATIMS)

PIA Unique Identifier:

P-6072033-600492

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?

Yes

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 Anti-Trafficking Information Management System (ATIMS) consist of the Grant Performance Module and the Shepherd Module. The Grant Performance Module will be used to collect and ingest data from grantees and subrecipients, from which Office on Trafficking in Person (OTIP) will build a comprehensive information management capability to assess program performance, conduct data analysis, and create dynamic reports. This will inform funding decisions and policy development to evolve their programs and services that combat human trafficking. The Shepherd Module is for certification and eligibility determination of potential victims of human trafficking.

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

The system will collect, maintain (store), or share information for multiple user types. This includes name, date of birth, email, phone numbers, alien number, country of origin, certification authority (e. g., T1 Nonimmigrant Status), mailing addresses, i certification and eligibility determination of potential victims of human trafficking. ATIMS does not include data fields for passport numbers, photographic identifiers, or legal documents; however, this information may be included in files

uploaded as part of the request for eligibility or certification. For access, ATIMS collects names, email, responses to preset security questions, and password to generate user accounts. Internal access to ATIMS modules is restricted to HHS federal staff and direct contractors with HHS user credentials (e.g., PIV card).

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

End users of the new ATIMS are able submit a request for certification and eligibility determination through the web portal. OTIP case specialists then review and prepare recommendation for the OTIP Director approval. Once the case review is completed, a notification of the case determination is sent to the requestor via email and mail. Other functions include the submission of immigration relief and visa documents from DHS; notification and requests of case consultations from law enforcement and Non-Governmental Organizations (NGOs); and the coordination of referrals for case management if appropriate. The inclusion of the new Grant Performance Module enables the submission and approval of performance reports. Information collected, maintained, or shared includes name, data of birth, and alien number, country of origin, certification authority (e.g., T1 Nonimmigrant Status), phone number, mailing address to process requests for certification and eligibility within the Shepherd Module. ATIMS does not include data fields for passport numbers, photographic identifiers, or legal documents; however, this information may be included in files uploaded as part of the request for eligibility or certification. ATIMS collects name, email, phone number, address, responses to preset security questions, and password to generate user accounts. Internal access to ATIMS modules is restricted to HHS federal staff and direct contractors with HHS user credentials (e.g., PIV card).

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

Yes

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

Demographic data, Employee Records, Training records, Insurance Information

Immigration certificate type (Certification Authority)

Country of Origin

User Credentials

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

Foreign Nationals who are, or may be, victims of trafficking

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose of the PII in ATIMS is to identify and verify victim eligibility to apply for benefits

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

The secondary uses of PII include connecting minors with law enforcement (as requested); connecting victims with case management services e.g. Trafficking Victim Assistance Program (TVAP) service providers, as requested); providing attorneys with case files (as requested) for criminal or civil litigation purposes or in response to a discovery request; and for the purposes of user management

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

Trafficking Victims Protection Act of 2000 (22 U.S.C. § 7105 (b))

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

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Request for Assistance for Child Victims of Human Trafficking
OMB Control Number: 0970-0362
Expiration Date: 09/30/2024

Information Requested for Foreign Adult Human Trafficking Victims Seeking HHS Certification
OMB Control Number: 0970-0454
Expiration Date: 04/30/2025

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.

There is an Information Sharing Agreement (ISA) that authorizes the sharing of information between ATIMS and the Amazon Web Services (AWS) Application Management System (AMS) is being developed

Describe the procedures for accounting for disclosures.

There are no records in the system which are subject to the Privacy Act, therefore an accounting of disclosures is not applicable. Attorneys can request records pertaining to certification and eligibility applicants with their consent, or the consent of their guardian in the case of minors under the age of 14. Attorneys must submit a request in writing to childtrafficking@acf.hhs.gov with the reason for the request, name of requestor, duration of request, and required supporting documentation including an Authorization for Release of Confidential Records and
G-28, Notice of Entry of Appearance as Attorney or Accredited Representative.
EOIR-27, Notice of Entry of Appearance as Attorney or Representative Before the Board of Immigration Appeals; or
EOIR-28, Notice of Entry of Appearance as Attorney or Representative Before the Immigration Court

If record is requested by an attorney, they are required to provide the following information before a record is shared:

Information:
- Individual's name, aliases, date of birth, nationality and alien number or numbers
- Name of the requestor
- Reasons why the case files are being requested

Required Supporting Documentation:
- A copy of the signed and executed G-28, Executive Office for Immigration Review (EOIR) -27 or EOIR-28. These forms are not required for attorneys who work for, or volunteer pro bono services for, non-profit legal services providers funded by the VERA Institute of Justice for Operational Readiness Review's (ORR) custody
- An Authorization for Release of Confidential Records on the law firm/legal agency's letterhead stationery signed by the individual if the person is 14 years of age or older, or

signed by the minor's parent or legal guardian if the minor is not in ORR's custody
- The authorization must specify to whom the documents should be released and the duration of the authorization.
- If the record is shared, OTIP records all these details and correspondence and information in the record. All record are considered permanent at this (still under NARA review).

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

All users of the system are made aware that personal information is collected as part of the user account registration. Potential trafficking victims and/or their requesters voluntarily provide information in order to submit requests for certification and eligibility determinations allowing them to apply for benefits and services to the same extent as a refugee, therefore prior notification of collection does not occur. However, during the information collection process all individuals are notified of the uses and potential disclosure instances of their information and required to give verbal consent which is then recorded in ATIMS by the case requester.

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 trafficking victims to opt-out to the collection and use of their PII. If the individual chooses to opt-out of the collection or use of their PII, the individual will not be able to request a determination of certification or eligibility. Any user who wishes to opt-out will not be granted a system account; however, this may not be an option if the user's job duties require access to the system.

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

All users of the system are notified of any system modifications (major or routine) through an announcements banner located on the system homepage. Individuals may request the latest disclosure information via a FOIA request.

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.

Trafficking victims who have their information in the system will be directed to contact their case requesters if they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. Case requesters are then provided contact information located on the web page login page to address concerns. A helpdesk member will then ensure the concern is communicated to OTIP staff for further assistance as needed. OTIP is currently working to develop processes for notifying victims of this process.

All other users can contact the system's helpdesk directly for assistance. The helpdesk staff will evaluate the issue on a case-by-case basis and notify OTIP staff if it is determined that this is an issue of unauthorized obtainment, us, or disclosure. All OTIP staff are responsible for notifying they ACF Incident Response Team (IRT). The ACF IRT will follow standard operating procedures for handling a privacy incident that involves a breach of PII. In the instance, that a request is made to correct inaccurate data, a system or application administrator will be able to make updates as needed. In addition, users may update their own user profiles as they see fit

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 Availability is handled by the infrastructure. The system is hosted in Amazon Web Services (AWS) which provides high availability using their multiple availability zones, the database is live synced and backed-up daily.

Data Integrity is ensured through role-based access control which limits the number of users that have write capability. Roles are separated by User Type within the system. Additionally, log files are maintained for any changes that occur within the system, time-stamped, and monitored by system and application administrators.

Data Relevancy is maintained by following the specific retention and destruction schedules currently being developed for approval by NARA.

Data accuracy is ensured through built in quality control standards requiring all data be entered in a correct and usable format.

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.

ATIMS includes a user access request functionality in which all requests require a system administrator approval, excluding, case requesters. Only system administrators can assign and modify access privileges for system users. The initial system administrator role is granted by the OTIP director. In addition, an application administrator is assigned by the ACF Office of Chief Information Officer (OCIO).

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 ATIMS Enterprise Authorization and Authentication Services (EAAS) microservices supports RBAC (Role Based Access Control) and ABAC (Attribute Based Access Control) along with privileges and permissions for both internal and external users. This ensures access to only the minimum amount of information necessary for each user type and task to perform their job.

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 training -- All ACF/OTIP federal staff and direct contractors that use ATIMS are required to take annual security awareness training provided by HHS.

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

In addition to the required HHS training, system users receive system-specific training documented in the Training Plan, learning aids to include the ATIMS User Manual and System Administration Guide, and other training course materials content to support users and system administrators as

they incorporate new capabilities into their day-to-day activities.

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.

A disposition was approved with the National Archives and Records Administration (NARA) on September 20, 2021. Disposition number is DAA-0292--2020-0001. The record schedules for the ATIMS database, Child Eligibility – Request for Assistance information, Adult Certification information, Periodic Reporting and Case Trend Analysis and the Policy Precedent Files is 5years respectively.

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

Physical Controls are inherited from the hosting platform, Amazon Web Services (AWS) and include nondescript facilities, with security staff controlling both the perimeter and various ingress points within the building, video surveillance, intrusion detection systems, fire detection and suppression, uninterruptible power supply (UPS), and climate control; all individuals accessing the building require two-factor authentication a minimum of two times and any visitor or contractor must sign in and be escorted at all times by an authorized individual. Technical controls include role-based access, user Identification, passwords, firewall, encryption, intrusion Detection System provided by Amazon Web Services (AWS) and managed by ACF Office of the Chief Information Security Officer (OCIO). Administrative controls include HHS security training provided to Federal and direct contractor staff, and non-disclosures (NDAs) are in place for direct contractor staff.

Identify the publicly-available URL:

shepherd.otip.acf.hhs.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

Yes

Is there a unique privacy policy for the website, and does the privacy policy address the process for obtaining parental consent if any information is collected?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null