US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

11/05/2024

OPDIV:

ACF

Name:

Technical Assistance Tracker (TAT)

PIA Unique Identifier:

P-9741065-605020

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.

Contractor

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.

Technical Assistance Tracker (TAT) is used to collect, track and report on the Technical Assistance (TA) requests received by the Office of Child Care (OCC) from Lead Agencies funded under the Child Care and Development Fund (CCDF) block grant program, and activities conducted to respond to these requests. It is also used to address a wide variety of topics in support of understanding the agency mission-specific functions (such as how best to implement phase-out eligibility or meet background requirements), This data is used to assist CCDF grantees in meeting CCDF requirements, report technical assistance efforts to Congress and meet other departmental reporting purposes.

TAT is hosted on ServiceNow, a Platform as a Software as a Service, with wide use throughout Health and Human Services (HHS). ServiceNow is a platform that allows for workflow and custom applications to be built efficiently and align with Federal Information Technology (IT) and Digital Transformation best practices. The Platform has achieved Federal Risk and Authorization Management Program (FedRAMP) High Certification verifying that USG security standards are

being followed. TAT is leveraging the Customer Service Management (CSM), dashboard and reporting functionality.

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

TAT collects, tracks, and reports on the TA requests from states, territories, and tribes; approvals of TA requests; assignments to partners (funded by OCC) for provision of TA; activities/actions related to that TA requested, such as a webinar or a TA site visit, and closing requests when completed; and reports on requests, activities, actions taken.

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

TAT collects TA requests from CCDF grantees (states, territories, and tribes) that need assistance to meet CCDF Block Grant requirements. It also collects approval of requests, assignments to partners that will provide the TA, and actions taken to meet the needs of the CCDF grantees.

The following information is maintained on a TA Request/Activities/Events:
Entity Type: (Choice list between Tribe, State/Territory, Regional Office, National Center, All Grantees or All), Requesting and Recipient Entities,
Contacts, Telephone number, Regions associated with the request (Automatically determined by Entities), Title, Description. Staffing for partners (funded by OCC) and partner staff (Assigning the request), Categorization of Goals, Strategic Areas and TA Focus, Invited contacts, Organizers, Attendees, who received it, OCC Approvers, and partner staff Reviewers. User accounts are created that include email address, name.

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
User credentials

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Identifying the state, territory, and tribal points of contact for technical assistance and user credentials

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

Not Applicable – there are no secondary uses of Personally Identifiable Information (PII) in the system.

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

Child Care and Development Block Grant (CCDBG) Act, 42 U.S.C. 9858 et seq.

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Government Sources

Within the DOC

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

Not Applicable

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.

A notification banner is in place on login to notify users of the system that their personal information will be 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.

There is no opt-out of the collection or use of their PII as their credentials are used to access the TAT system. If requested, the user can request his/her account to be disabled.

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

A notification banner is in place on login to notify users of the system that their personal information will be collected and if there are any changes to the 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.

If an individual has a concern with their information, they can make changes within the TAT automated User Edit Details section that is accessible by any user to change the information attached to their account. Managers can change a user's TAT information for anyone in the system. This is achieved by making a request from the user's dashboard. TAT Admins can update any user account upon request by the system owner

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: Data integrity of the PII collected in security artifacts is maintained by restricting edit privileges for all artifacts to those users who have been approved. Privileges are set to control access by user type and is maintained by themselves and the National Centers Manager (these are the partners funded by OCC) with oversight from the Project Manager. All user account requests to add and modify users can be submitted by anyone with access but require approval from the National Center (partner funded by OCC). Requests for Removal can only be submitted and

approved by a National Center Manager (partner funded by OCC).

Availability: Data availability is inherited by the ServiceNow GovCommunityCloud (GCC) architecture which hosts this application. The GCC Service Level Agreement states that the GCC will provide a monthly up-time percentage of at least 99.9%. The GCC consists of co-located data centers where production data is replicated daily.

Accuracy/Relevancy: As part of continuous monitoring, the Information Systems Security Officers (ISSOs) / System Owners are responsible for updating all security artifacts for each system. If a user finds information that is incorrect regarding PII, they should make a user edit request immediately for approval from their National Center (partner funded by OCC). An annual audit for PII is done to ensure that all changes required have been made and are indeed accurate. The system will automatically disable accounts of users who have been inactive for 60 days, ensuring relevancy. Additionally, TAT data should follow the specific retention and destruction schedule in accordance with National Archives and Record Administration (NARA) disposition authorities.

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.

TAT collects two types of PII: 1) User credentials and 2) non-sensitive PII for every technical assistance request (such as name of person requesting TA, business phone number, and business email address).

The non-sensitive PII (name, business email and business phone number) is strictly used to reach out to the person receiving technical assistance. All users can access the non-sensitive PII, which is part of each TA request, as part of their daily duties. User credentials are only accessed by the TAT users who are defined by the System Owner and Security Lead as roles responsible for administering user accounts.

All System Administrator users have the same relationship with the application's PII. All Developer users have the same relationship with the application's PII. All System Administrator and Developer positions are filled by government contractor staff so there are no contractor-specific procedures related to PII which differ. TAT users can be contractor staff or government staff, but all people with TAT user role have the same relationship with the application's PII.

All System Administrators and Developers (which are vendor/contractor staff) can view or edit PII of TAT users in the course of performing application troubleshooting or enhancements. All TAT users must authenticate to access the application; all TAT users can view non-sensitive PII of other users (name, business phone, business email) while creating and managing TA request records. These TAT users select a person's name (another TAT user) from a pick list of values, in order to associate a record with the staff person primarily responsible for delivering technical assistance, or a staff person collaborating on delivering technical assistance. Also, a TAT user can select a person's name from a pick list of values, or create a new record for a person, in order to associate a record with the person requesting technical assistance. TAT users can also perform queries within the

application to create reports or dashboards; the fields queried and returned can include First Name/Last Name of person requesting or delivering technical assistance.

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.

TAT collects two types of PII: 1) User credentials and 2) PII for every technical assistance request (such as name of person requesting TA and their email address). The TAT System Owner and Security Lead review the established TAT roles annually to define who has access to user credentials as part of their duties to administer TAT user accounts. Database access is limited to those individuals responsible for the maintenance of the database through user names and passwords.

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.

Both Federal and contactor staff (funded by OCC) are required to complete annual privacy and security training as mandated by HHS. Contractors sign a non-disclosure agreement that states the unauthorized disclosures are punishable by pertinent Federal laws; a standard system security notice/banner is in place for all TAT users.

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

Help Desk/IT Support/User Training staff are given training based on their role and responsibility, such as, responding to questions about the functionality of the TAT; helping system users' login when they encounter issues.

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.

TAT adheres to the following records retention schedules: DAA-GRS-2017-0002-0001 and DAA-GRS-2017-0002-0002.

Records for TAT users who have been active at any time are not removed or deleted from the application. Records for TA requester people are not removed or deleted from the application. This is because active and archived technical assistance request, activity and delivery records would not remain whole if the TAT users and TA requesters associated with them were not present in the application. Also, logs of system actions would not remain whole if System Administrator and Developer users associated with them were not present in the application. The application is configured to archive and delete records of technical assistance request, activity, and delivery at the time intervals specified by the records retention schedules. Per National Institute of Standards and Technology (NIST) Access Control (AC-2), the application automatically disables accounts that are inactive for 60 days and System Administrators permanently disable TAT user accounts that are inactive for 365 days, after review, through a manual action.

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

Administrative: PII will only be accessible to users if they have approved user accounts within the system. There is also annual security awareness training for all users holding accounts for the system.

Technical: All traffic will be between end users and the authorization boundary will be sent with HTTPS over port 443. Authentication will be provided using the Now Multi-Factor Authentication

Solution. 60-day password change interval, and a maximum failed login attempt of 3 is enforced by the system. System and application logs will be reviewed and analyzed on a monthly basis from the automated auditing system is set up using Splunk. Virus Scans are available on demand from the Now Platform ISC.

Physical: The physical controls will all be inherited by the GCC platform and include the following: Restricting physical access to the data center both at the perimeter and at building ingress points through the help of video surveillance, intrusion detection systems, and 2 rounds of two-factor authentication for everyone accessing a data center floor. Visitors and contractors are required to have Identification (ID), sign-in with building security, and be always escorted by an authorized staff; Fire detection and suppression systems; Uninterruptible Power Supply (UPS); Climate and Temperature control; and Preventative maintenance are all completed to Fed Ramp High Standards. Please see Now GCC documentation for more information.