

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/29/2024

OPDIV:

ACF

Name:

Tableau Enterprise Server

PIA Unique Identifier:

P-6712132-826919

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Test

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.**

Tableau Enterprise Server is a shared service used by offices in the Administration for Children and Families (ACF) to create program and operations monitoring and analysis dashboards, visualizations for operational, research, and storytelling purposes. ACF's Enterprise Tableau is a data visualization platform that enables offices to explore and share insights in their data.

By having an enterprise Tableau Enterprise Server hosted in in ACF's secure cloud environment, ACF streamlines platform management and governance. An Enterprise Tableau Server also reduces cost for ACF as existing ACF data systems that do not have a data visualization layer can directly integrate to the Enterprise Tableau Server, rather than needing a separate data visualization software.

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

Tableau will be used by Program Offices to visual their data in varies formats such as dashboards,

graphs, and charts from administrative, research or evaluation data. The visualized information will mostly be summaries of individual-level data, where the data is loaded onto the Tableau server in an aggregated format (i.e., not specific to an individual person). In some cases, such as operational dashboards, Personally Identifiable Information (PII) may be included, which may include name, email address, phone number, or mailing address may be included in charts to enable easier follow-up or do reporting by person.

Data loaded into Tableau can be done through a variety of formats including comma-separated values (CSV), Excel, or database connections. Any database connections are done through secure integrations such as virtual private networks (VPN) that are included within both the authority to operate for ACF's Tableau enterprise environment and the system that hosts the database. The dashboard developers specify what data is used to build the visualizations.

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

In Tableau, users are able to build and share visualizations/dashboards with other users in ACF's enterprise Tableau environment.

Tableau is a tool used to create visualizations and dashboards that can be published to ACF's Tableau enterprise servers. Tableau is licensed as role-based term licenses that grant a range of capabilities. ACF requires the following role-based term licenses that can be used to activate or deactivate

Tableau Server:

Viewer licenses – Allows users to view and interact with dashboards and visualizations including downloading summary tabular data displayed in the visualizations. Viewers are not allowed to download full underlying datasets.

Explorer licenses – Allows users to view and explore trusted data and includes self-service analytics.

Creator – Allows for the creation and publishing of content, dashboards, and visualizations.

ACF Tech also has a Tableau 8-core public server license that imposes no constraints on the number of user accounts in Tableau Server to allow ACF to publish dashboards and visualizations to the web.

As an ACF enterprise tool, Tableau is used to visualize a variety of data ranging from program administrative data to survey data to internal operational data to public data. These visualizations can be for communication or storytelling purposes to both ACF and wider audiences, which can include other Federal agencies and the public, as well as reporting and internal management purposes. In many cases, the data visualized are in aggregate form, without PII. For some internal or external reporting and management purposes, PII may be included, which can include name, email address, phone numbers, mailing address, and usernames (which are the user's email addresses). For instance, a dashboard can show the status of policy questions sent from grant recipients to a program office, filterable by program specialist name assigned to respond to the questions. Another example, an operations dashboard tracking clearance requests can include names and contact information in drill-down views. In these instances, PII that is not indicated in Question 15 are not allowable in ACF's enterprise Tableau.

General Records Schedule (GRS) 6.5 Public Customer Service Records - Item 20 applies. Tableau workbooks are retained until they are superseded, obsolete, or otherwise requested by the users. By

default, offices determine when Tableau workbooks they have created are superseded or obsolete. ACF Tech's server admins periodically check workbook usage, at minimum every six months. If data sources or workbooks have not been used in 6+ months, an admin may reach out to ask about either archiving or fully deprecating the content (remove from the system).

Username and email addresses are included in Tableau for authentication / administrative purposes, and only as long as users are active in the system.

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
Mailing Address
Phone Numbers
Usernames

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?

PII is used for system authentication and administrative purposes. ACF staff request access to Tableau for themselves and/or their team members to the license administration team. If a contractor working on behalf of ACF directly requests access for themselves, they must have the federal ACF employee they work with on their request for verification.

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

N/A

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

5 USC 301, Departmental Regulation

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

No

Identify the sources of PII in the system.

Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

Not Applicable

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.

Information sharing agreements are established on an as-needed basis with ACF offices, the type of which will be determined based on the use case. When the ACF enterprise Tableau is directly integrated to another system (e.g. via a database connection), the Authorization to operate (ATO) for both ACF's enterprise Tableau and the other system is adjusted accordingly. Tableau can be used to publish visualizations using static data sources, e.g., CSV files.

Presently, ACF's enterprise Tableau has a memorandum of understanding (MOU) with the Office of Child Care's Automated Reporting System (CARS) as part of a direct integration between the CARS database into the ACF enterprise Tableau as a data source for visual reporting. There are tentative plans to also establish MOUs for integrations with several other data systems within ACF including the Children's Bureau's data warehouse and Office of Head Start's Training & Technical Assistance Hub application and database of Program Information Reports.

Describe the procedures for accounting for disclosures.

In the event of unintentional PII disclosure, the ACF office that owns the relevant dashboard will assess the impact of the disclosure and notify affected individuals.

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 direction notification from Tableau as it is not the source of collection. Any PII visualized in Tableau dashboards are collected by other systems that have their own authorities to use / operate as well as notification processes. Notification of collection of PII is done within these upstream systems.

For ACF enterprise Tableau users, because authentication is via ACF's single sign-on system or Login.gov, email address must be provided to be granted a license. There is no opt-out option for ACF enterprise Tableau users on providing email address. Users request licenses to ACF's enterprise Tableau via email and upon granting of license, they are provided login instructions, including that their email address is their username. The email addresses are used for users accessing the system and notifying users of system outages.

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.

For Tableau user authentication, the email addresses of users are required for Tableau to sync with single sign-on. While name is technically optional, the ACF formula for email addresses is firstname.lastname@acf.hhs.gov, so names are essentially collected with the email addresses.

Regarding the data sources that are visualized within Tableau, Tableau is not a data collection tool and does not directly collect data. Individuals cannot opt-out of the collection of PII in Tableau, as the information is collected from other sources. Back-end users that wish to opt-out, will not receive

access to the system.

Any PII visualized in Tableau dashboards are collected by other systems that have their own policies and procedures for opt-out of collection or use of their PII.

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

ACF's enterprise Tableau is not a data collection tool and is not the system of records. Consent for usage of any PII is obtained from the system of record, which have established policies and procedures for notifying persons of any disclosure or re-use of PII. The ACF enterprise Tableau system does not have a formal notification or consent process in place.

When a user requests a license to ACF's enterprise Tableau environment to either build or view visualizations, they must provide their email address to enable authentication into the system through either ACF's single sign-on system or Login.gov, both of which associate login with email addresses. The user email addresses within Tableau are only accessible to system administrators for the purposes of setting permissions.

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.

No process is in place for users to resolve their concerns, the PII in Tableau. As described in question data is collected directly from other sources,

If an individual believes their information is inaccurate, the processes to voice and resolve concerns are tied to the systems of record, i.e., the systems where the data are originally collected, not Tableau. The ACF Tableau administrators can support offices in removing content from the Tableau server if needed.

If a user's metadata (name, email address) is incorrect, they can directly correct the information in the Tableau server or email datatools@acf.hhs.gov for help correcting.

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

We anticipate that PII is included in Tableau dashboards in a minority of cases that are relevant to internal operations and reporting. By definition, such reports are only useful if the data is available, accurate, and relevant. As with all content on Tableau inclusive of those that do not involve PII, ACF Tech's server admins periodically check workbook usage, minimum once every six months. If data sources or workbooks have not been used in 6+ months, an admin may reach out to ask about either archiving or fully deprecating the content (remove from the system).

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.

Tableau Administrators see all content in the system including user lists and data sources loaded into and visualized on the Tableau servers. This is how Tableau designed administrator rights.

There are two relevant buckets of Users: those creating dashboards and those viewing. The dashboard creators see any PII included in their dashboard data sources. They can specify who views the dashboard itself. Ability to view a dashboard can be restricted to just users within a specific audience and as needed by use cases, viewership can be even further restricted down to row-level security.

Contractors and other partners such as grant recipients are only involved as needed. Some ACF offices acquire contractor support to build dashboards. Some ACF offices deliver services through cooperative agreements and grants and may want to use Tableau as an internal reporting system with their grant recipients. Contractors and Other partners are a subset of Users.

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.

Ability to view content in Tableau can be restricted down to row-level security on datasets powering a dashboard, and viewership can be set at on a dashboard-by-dashboard basis.

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.

Federal staff complete annual privacy training as mandated by HHS. Direct Contractors sign a non-disclosure agreement which states that unauthorized disclosures are punishable by pertinent Federal laws. A standard system security notice/banner is in place for all users. The Office of the Chief Information Officer (OCIO) provides annual privacy training to contractor staff.

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

ACF has developed a Creator Handbook and System Administrator Handbook to cover governance topics. Everyone who is granted permissions to build and publish dashboards on ACF's Tableau servers attend an onboarding session to review these processes.

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.

For all instances PII is used in reports published on ACF's enterprise Tableau environments, GRS 6.5 Public Customer Service Records - Item 20 applies. Tableau workbooks are retained until they are superseded, obsolete, or otherwise requested by the users. By default, offices determine when Tableau workbooks they have created are superseded or obsolete. ACF Tech's server admins periodically check workbook usage, at minimum every six months. If data sources or workbooks have not been used in 6+ months, an admin may reach out to ask about either archiving or fully deprecating the content (remove from the system).

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

Administrative

Ability to view content in Tableau is set by the ACF Tech administrators and can be restricted down to row-level security on datasets powering a dashboard, and viewership can be set at on a dashboard-by-dashboard basis.

Technical

Users must authenticate into ACF's enterprise Tableau environment through either Personal Identity Verification or Login.gov Single Sign On.

Physical

ACF's enterprise Tableau environment is hosted within ACF Tech's General Support System (GSS), an Amazon Web Services (AWS) cloud environment maintained by ACF Tech's Operations Division in partnership with ACF Tech's Cybersecurity and Privacy Division. GSS is located in the AWS East/West Public Cloud Environment. Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens. AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff. For more details on AWS's security practices, please refer to <https://aws.amazon.com/compliance/data-center/controls/>

Identify the publicly-available URL:

<https://tableau-public.acf.gov/>

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

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 under the age of thirteen?

No

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

Yes

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

No