US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

09/29/2016

OPDIV:

ACF

Name:

SSBG Data Portal

PIA Unique Identifier:

P-8492178-846439

The subject of this PIA is which of the following?

Electronic Information Collection

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)?

No

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

Describe the purpose of the system.

The Social Services Block Grant (SSBG) Data Portal is an electronic data collection system for recipients and expenditures for the following SSBG service categories: adoption, case management, congregate meals, counseling day care-adults, day care-children, education and training, employment, family planning, foster care-adults, foster care-children, health-related, home-based, home-delivered meals, housing, independent/transitional living, information and referral, legal, pregnancy and parenting, prevention and intervention, protective services-adults, protective services-children, recreation, residential treatment, special services-disabled, special services-youth at risk, substance abuse, transportation, and other (if applicable).

The SSBG Data Portal is also currently used for State submission of Hurricane Sandy SSBG Supplemental Funding expenditure and recipient data. This data comprises expenditures of and recipients of supplemental disaster recovery funding, which was added into the SSBG program in 2013, and which will cease use in 2017. Expenditure data is collected for each of the same service categories above, though for only the single funding source of the Hurricane Sandy SSBG Supplemental Funds.

Recipient data for the Hurricane Sandy funds is collected in a format identical to that described for the normal SSBG funds as described above.

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

Each year, the Federal government allocates funds to states to support social services for vulnerable children and adults through the Social Services Block Grant (SSBG) program. States submit the expenditures and recipient data via the SSBG Data Portal to the federal Office of Community Services (OCS) which administers the program. The SSBG Annual Report reviews SSBG expenditures and the number of recipients of services during the fiscal year. The data collected is based on the 29 service categories (adoption, case management, congregate meals, counseling day care-adults, day care-children, education and training, employment, family planning, foster care-adults, foster care-children, health-related, home-based, home-delivered meals, housing, independent/transitional living, information and referral, legal, pregnancy and parenting, prevention and intervention, protective services-adults, protective services-children, recreation, residential treatment, special services-disabled, special services-youth at risk, substance abuse, transportation, and other (if applicable)) and can contain any or all of the following data points: SSBG allocation, funds transferred into SSBG (and which block grants the funds were transferred from), expenditures of all other federal, state, and local funds (and their source), provision method (public or private), number of children serviced, number of adults serviced aged 59 or younger, number of adults serviced age 60 or older, and number of adults serviced with unknown age.

The following PII is collected for and from authorized SSBG federal and state users solely for the purpose of user credentials and multi-factor authentication login methods: First and Last name, phone number, email address, and user credentials. User office addresses are also captured and stored in the system. Direct contractors have user credentials for the SSBG Data Portal in order to perform administrative functions.

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

Each year, states must report SSBG expenditures, expenditures of other sources of funds, and total expenditures using a standard post-expenditure reporting form (Office of Management and Budget (OMB) No. 0970-0234). On this form, states report data on the amount expended for each service category (expenditures) and the total number of adults and children served (recipients). The data is currently kept on a permanent basis to undergo trend analysis from previous years, though may be subject to editing (with Federal/Direct Contractor approval) if States wish to provide updated information.

The following PII is collected for and from authorized SSBG federal and state users solely for the purpose of user credentials and multi-factor authentication login methods: First and Last name, phone number, email address, and user credentials. User office addresses are also captured and stored 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

Phone Numbers

User credentials

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?

100-499

For what primary purpose is the PII used?

User PII is used for generating and maintaining user accounts and user access to the SSBG Data Portal.

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

There is no secondary use of user PII information.

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?

No

N/A

Identify the sources of PII in the system.

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

OMB NO.: 0970-0234; EXPIRATION DATE: 11/30/2017

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.

For the SSBG Data Portal, State and Federal staff are instructed to provide their name and work email address via phone or email. Users provide their phone numbers and work addresses in the course of creating their user profiles and establishing multi-factor authentication within the SSBG Data Portal. There is no official notice given as the collection of this information is required to create the system user account.

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.

System administrators (ACF employees and direct contractors) and State and Federal staff may opt out of having a user account to access the SSBG Data Portal. However, if they do not provide the information, they will not be granted access to the SSBG Data Portal.

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

SSBG is subject to the Office of Management and Budget approval process to renew the authority to collect data using existing data elements and to add new ones. This process occurs every 3 years. During the clearance and approval process the authority of SSBG to continue to collect data and any potential changes are reviewed by the Office of Management and Budget, the ACF Clearance Officer, the states, and the general public.

If major changes should occur within the system regarding topics such as disclosure of data and/or data uses, users will be notified via email. Such messages will describe the nature of the changes and the expected date of implementation. Users will be notified of the SSBG Technical Team's contact information (SSBGsupport@wrma.com), should users have any concerns about how their data will be affected.

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 State or Federal staff person may contact an SSBG team member with concerns about or updates to PII via phone or email. The SSBG Data Portal contains a 'Contact' page whereby users can access a hyperlink which opens an outlook email form to contact the technical team's general service email address - SSBGsupport@wrma.com. This is a group email address, and any email sent to this address will be forwarded to members of the technical team for follow-up. A member of the technical team is designated as the lead in responding to users' assistance requests, though other team members may respond if the lead TA assistant is out of the office or otherwise unavailable. A footer is also available on virtually every page of the SSBG Data Portal, which states "For technical assistance, please contact the SSBG Technical Team at SSBGsupport@wrma.com"

Upon receiving a user's inquiry, the technical team evaluates the seriousness of the concern and examines any specifics of the portal's functionality related to the inquiry. If the user's PII is noted to be inaccurate, the team provides the user with any technical assistance necessary to correct their PII. If a user is concerned about their PII being inappropriately obtained, used, or disclosed, site administrative staff will evaluate site logs to determine if and how any such misuse occurred, and will follow-up with the user as appropriate.

Should instances arise that a user's PII has been inappropriately obtained, used, or disclosed, the technical team will immediately inform ACF of any breaches to the site that may have contributed to this misuse. The technical team will then work with ACF to determine any other potential misuses of PII, and will contact any effected users to describe the nature of any possible misuse and inform these users of the possible effects and intended follow-up on the part of the technical team and ACF. Upon resolving any pathways that may have led to such misuse, the technical team will coordinate with ACF to provide technical assistance to the SSBG Data Portal user base to describe the problem that occurred, the solution that was implemented, and steps users can take to ensure similar misuses do not occur in the future.

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

State staff may update their work emails, work phone numbers, and office addresses through user profile settings within the SSBG Data Portal itself, or may contact a member of the SSBG team via phone or email for assistance in doing so. The accuracy of state staff contact information is checked and updated annually. Outdated, irrelevant, and inaccurate accounts are removed from the system.

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

Users:

System users have a profile page that allows them to view and edit some of their personal PII (i.e. phone number)

Administrators:

The administrators are direct contractors.

Contractors:

Direct contractors act as IT system administrators and developers for maintenance, technical assistance, and updates to the system.

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

System users have access to ONLY their personal PII via a profile page after login. This page displays and allows for minimal editing of their personal PII.

System administrators have access to all PII contained in the system per their job function of system maintenance, user and technical assistance, and system updates.

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.

Access is limited to the functions and information which is essential to complete their job functions. Administrator access to systems is only provided to privileged access. Data storage access is restricted to authorized users.

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.

SSBG collects information from public agencies that have their own policies regarding training and system access. Federal staff and contract support staff are required to take annual security training. The training includes sensitivity to PII.

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

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

No

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Given that the PII contained in the SSBG Data Portal is specific only the system user accounts, the PII is retained only as long as that user is an active employee requiring access as part of their required job duties. Once this ceases to be true, then the records are removed from the system. We are currently working with the ACF Records Manager to determine the specific National Archives and Records Administration (NARA) retention schedule that would apply to the SSBG Data Portal.

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

Administrative controls, including but not limited to:
System security plan (SSP), File backup/archive, User manuals, Contractor Agreements

Technical Controls:
User Identification and Authorization, Passwords, Firewalls at hosting site, Monitoring and Control scans

Physical controls:
The SSBG Data Warehouse is hosted on the FedRamp certified Microsoft Azure Cloud platform.