US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/17/2017

OPDIV:

ACF

Name:

MonAFI

PIA Unique Identifier:

P-4324210-446513

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.

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.

MonAFI is a system accessed through a dual authentication security protocol that supports core functions of the Assets for Independence (AFI) program: Coordinating Customer Service through Customer Relationship Management (CRM). A number of people and organizations interact with AFI grantees and other stakeholders. In addition to—and at the direction of—federal staff, direct and indirect contractor personnel from several different organizations interact with grantees and other stakeholders on behalf of the program. Using MonAFI' s CRM capabilities, AFI staff and direct and indirect contractors use customer service cases to log telephone and email interactions with grantees, as well as AFI technical assistance site visits. This supports coordinated and consistent customer service; Tracking Grant Performance. The system contains grantee's self-reported data on grant performance, as reported in the grantees' annual data reports. Reports and dashboards on grant performance are used by program staff and direct and indirect contractor to trouble spot and allocate technical assistance resources (such as site visits) among grantees; performing Federal Reviews on Grant Applications.

AFI staff enter information on the contents of the application as part of their due diligence “federal review” process to ensure the application is compliant. MonAFI’s screens for this function are highly customized to the program’s extensive requirements. Using the system ensures that this federal review is not only efficient, but also consistently applied; Managing IDAresources Content. (IDA stands for individual development accounts, which are the types of bank accounts that AFI grantees open for participants.) HTML content and static resources for idaresources.acf.hhs.gov are managed through the system.

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

The MonAFI System contains the following information types:Organizational Contact Information. MonAFI contains contact information for grantees and other organizations that have interacted with the AFI program as potential applicants or other types of stakeholders. Grantee/Organization-level contact information includes organization address, phone numbers, and website information. The names of individuals with those organizations are also contained in the system along with individuals' email addresses and phone numbers. Grant Award and Performance Data. MonAFI contains the grant numbers, award amounts, and other basic information about grant awards. In addition, the system contains grantee’s self-reported data on grant performance, as reported in the grantees’ annual data reports. All performance data are aggregated at the level of the grant and no personally identifiable information (PII) is included. Representative data items include a) the number of participants enrolled in AFI under a given grant and b) the number of assets purchased by participants through their participation in the program; Grant Application Data. Basic data from applicant’s SF-424 grant application are contained in MonAFI, including the amount requested. AFI staff enter information on the contents of the application as part of their due diligence process to ensure the application is compliant; Customer Service Records. Customer service cases log telephone and email interactions with grantees, as well as AFI technical assistance site visits; IDAresources Content. HTML content and static resources for idaresources.acf.hhs.gov are managed through the system; Login Credentials. The system contains users names, email addresses, and passwords.

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

MonAFI is a system accessed through a dual authentication security protocol that supports core functions of the Assets for Independence (AFI) program. The MonAFI System contains the following information types: Organizational Contact Information. MonAFI contains contact information for grantees and other organizations that have interacted with the AFI program as potential applicants or other types of stakeholders. Grantee/Organization-level contact information includes organization address, phone numbers, and website information. The names information of individuals with those organizations are also contained in the system along with individuals' email addresses and phone numbers; Grant Award and Performance Data. MonAFI contains the grant numbers, award amounts, and other basic information about grant awards. In addition, the system contains grantee’s self-reported data on grant performance, as reported in the grantees’ annual data reports. All performance data are aggregated at the level of the grant and no personally identifiable information (PII) is included. Representative data items include a) the number of participants enrolled in AFI under a given grant and b) the number of assets purchased by participants through their participation in the program; Grant Application Data. Basic data from applicant’s SF-424 grant application are contained in MonAFI, including the amount requested. AFI staff enter information on the contents of the application as part of their due diligence process to ensure the application is compliant; Customer Service Records. Customer service cases log telephone and email interactions with grantees, as well as AFI technical assistance site visits; IDA resources Content. HTML content and static resources for idaresources.acf.hhs.gov are managed through the system.

The information is maintained temporarily; the length of time is variable as the information is retained only as long as is necessary for business use. For example, user credentials are removed once an employee departs or changes job functions.

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

Employer Information

User Credentials

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

Employees

Public Citizens

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Grantee personnel contact information is used to facilitate customer service to grantees. Individuals' contact information is used to facilitate response to individuals' request for information. Contact information is also used to make program-related announcements to stakeholders.

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

There is no secondary use for PII.

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

5 USC 301, Departmental regulations: This authority states that the head of an Executive department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. In other words, each agency has some authority to create and maintain records in order to carry out the work of that agency. / OMB M-03-22 Attachment A, Section C

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.

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Other

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

AFI PPR OMB Control Number: 0970-0483; Expiration date: 08/31/2019 // SF-424 OMB Control Number: 0915-0375; Expiration date: 01/31/2017

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.

Individuals proactively provide their information for the purposes of receiving customer service from the AFI Program, therefore no prior notice is needed. For system administrators and users, the privacy training contains a notification that their personal information is collected by the system.

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.

Individuals proactively provide their information for the purposes of receiving customer service from the AFI Program, therefore the "opt-out" option would be the individual choosing to not reach out to the AFI Program. or system administrators and users, the privacy training articulates a process for opting out of the collection.

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

There have not been major system changes to date that would require that notification. If there were, ICF would work with the Office of Community Services (OCS) to send an email communication offering users an option to delete their information from the MonAFI system.
Note: "ICF" is not an acronym. Rather, these three letters are the name of the company.

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.

The process consists of convening a meeting of ICF, Office of Community Services (OCS), and the Office of the Chief Information Officer (OCIO) personnel within one business day to review the concerns. The subsequent discussion would include an assessment of the scope of the concerns (whether additional individuals are involved or affected). In accordance with OCS, and OCIO guidance, ICF will proceed with the removal of specific information or the installation of new procedures or security features.
Note: "ICF" is not an acronym. Rather, these three letters are the name of the company.

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

MonAFI users continuously monitor the data's integrity, availability, accuracy and relevancy through usage of the information and updating. In addition, built-in validation checks support data integrity and accuracy. To prevent improper or inadvertent modification or destruction of data, MonAFI uses profile-based security to make PII data read only when non-administrator users do not need to edit it. MonAFI uses field history tracking to ensure that individuals who provide or modify PII cannot repudiate their actions. That tracking records a history of when PII fields value change, who made the change, what the field value was prior to the change, and what the field value was after the change.

The salesforce system maintains backup servers to ensure that information is readily available, even if a main server fails. To ensure that the PII is sufficiently accurate for the purposes of the system, MonAFI users are assigned responsibility for the accuracy of the information on external points of contacts in their portfolios. They update the information on a continuous basis in the course of their work. Administrators are responsible for the PII on users and update the information on a continuous basis based on direct work with the 25 users. Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system in a similar way by system users on a continuous basis.

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

Users:

Access to PII pertaining to providing accurate customer service.

Administrators:

Perform tasks in support of system operations and maintenance.

Developers:

Perform tasks in support of system operations and maintenance.

Contractors:

Direct and indirect contractors make up the pool of developers and administrators, and some system users.

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

The system owner determines which users may access PII based on their need to access that information for their fulfillment of tasks assigned by the Office of Community Services (OCS). Currently, all MonAFI users utilize PII in their fulfillment of OCS-assigned tasks. OCS (through their instructions to ICF) denies login credentials to the system for individuals that do not need to utilize the information.
Note: "ICF" is not an acronym. Rather, these three letters are the name of the company.

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 Office of Commmunity Services (OCS) (through their instructions to ICF) denies login credentials to the system for individuals that do not need to utilize the information.
Note: "ICF" is not an acronym. Rather, these three letters are the name of the company.
Currently, all MonAFI users need access to the full set of PII contained within the system (contact information for individuals as stated above). So all users have access to the same PII information.
Upon system usage changes initiated by the Office of Community Services, ICF re-evaluates whether using role assignments for "least privilege" are practicable.

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.

System users from Office of Community Services (OCS) and ICF undergo information security training that covers handling of PII. All employees complete annual Health and Human Services (HHS) security awareness and privacy training in addition to signing the HHS Rules of Behavior upon employment. A supplemental MonAFI-specific security awareness training articulates responsibilities for protecting the information.
Note: "ICF" is not an acronym. Rather, these three letters are the name of the company.

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

A supplemental MonAFI-specific security awareness training articulates responsibilities for protecting the information.

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.

In the master database (MonAFI), unneeded information is deleted / overwritten immediately on receipt of new information by system users. Information that is not deleted or overwritten in the course of program business processes is retained as long as supported by its business use. As Program (Mission) Records, the information in the data base is not covered by a National Archives and Records Administration (NARA) general records schedule, https://www.archives.gov/files/records-mgmt/grs/general-faqs.pdf (FAQ 5). However, the General Records Schedule (GRS) 4.3 covers Input Records, Output Records, and Electronic Copies.

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

System platform vendor Salesforce.com provides the dual-authentication credentialing system used to prevent unauthorized access to the information. Within the system, the security settings associated with user profiles are used to block unnecessary access to PII. An intrusion detection system monitors potential security breaches. Other measures include anti-malware protection, file integrity monitoring, network and web application vulnerability assessments, encryption, and external firewalls configured to “deny all – allow by exception.” Physical access controls, including badge readers, biometric devices, and security guards limit access to data center facilities to authorized personnel.

Identify the publicly-available URL:

ldaresources.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.

Session Cookies that do not collect PII.

Persistent Cookies that do not 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?

Yes