# US Department of Health and Human Services

## Privacy Impact Assessment

### Date Signed:

08/31/2016

### OPDIV:

ACF

### Name:

Audit Resolution Tracking and Monitoring Systems

**PIA Unique Identifier:**

P-7726700-559652

**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?**

No

**Does the system include a Website or online application available to and for the use of the general public?**

No

**Identify the operator.**

Agency

**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 Single Audit Act (SAA) of 1984 established single financial audit requirements for State and local governments receiving Federal assistance in any fiscal year above a designated level (currently $750,000). The Code of Federal Regulations (CFR) TITLE 2, CHAPTER II, PART 200, Subpart F—Audit Requirements as the implementing regulation established standards for consistency and uniformity among Federal agencies' audits of non-Federal entities expending Federal awards. It requires auditees to prepare two documents subsequent to the audit and submit them to the Federal Audit Clearinghouse, Bureau of the Census (FAC): the audit reporting package; and the Form SF-SAC. One the audit reporting package includes: auditor’s report; Management Discussion and Analysis (MD&A); financial statements; schedule of federal award expenditures; schedule of findings and questioned costs; and a summary schedule of prior audit findings and a corrective action plan for current year audit findings. Second the Auditees submit Form SF-SAC (Data Collection Form for Reporting on Audits of States, Local Governments, and Non-profit Organizations) to the FAC, which states whether the audit was completed in accordance with the regulation and provides information about the auditee, its Federal programs, and the results of the audit.

The FAC, OMB's designated clearinghouse provides a central repository of record where non-Federal entities transmit the audit reporting packages required by CFR 2: Subpart F. Federal agencies access the FAC and download the single audit reporting packages. The regulation requires Federal entities to: ensure that audits are completed and reports are received in a timely manner and in accordance with the regulation; and follow-up on audit findings ensuring recipients take appropriate and timely corrective action. Federal awarding agencies are responsible for issuing a management decision within 6 months after formal receipt of the audit report for recommendations that relate to its awards. Pursuant to the Inspector General Act of 1978, 5 U.S.C. App., the Office of Inspector General (OIG), HHS conducts audits of internal HHS and ACF activities, as well as activities performed by ACF grantees and direct contractors. The OIG, HHS downloads the single audit reporting packages from the FAC. OIG's National External Audit Review Center (NEAR) reviews single audit reports for compliance with CFR TITLE 2, CHAPTER II, PART 200, Subpart F and for conformance with professional accounting standards. NEAR reviews the findings, determines which findings merit actions, assigns each audit finding an internal, tracking Recommendation Code (REC) Number, and sends the audit report and findings in hard-copy to the responsible HHS and ACF organizations.

The Division of Financial Integrity (DFI), ACF functions as liaison with OIG, HHS for addressing audit findings. Data is extracted from NEAR into a temporary holding file where the audit packages are screened for findings and Rec Code. Audit Resolution Tracking and Monitoring Systems (ARTMS) auto searches and identifies audits with findings and associated Rec Codes that are uploaded to ARTMS. Once completed the data in the temporary holding files is deleted. DFI staff review the individual audit files within ARTMS that have been uploaded as only audits with findings and associated Rec Code are uploaded to ARTMS and assign a responsible official for addressing the findings.

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

The HHS OIG downloads the single audit reporting packages from the FAC. OIG's NEAR reviews the findings, determines which findings merit actions, assigns each audit finding an internal, tracking REC Number (there may be several Rec Codes for each finding), and sends the audit report and findings in hard-copy to the responsible HHS and ACF organizations. The Audit Report File (in text format) and Findings (in text format) are uploaded into searchable data fields within ARTMS; and Attachment A (Microsoft Word Format) that contains the Rec Codes and Rec Code Narratives are included as attachment to the individual audit records. The packages are uploaded to ARTMS in order to streamline financial activities to reconcile audit findings.

Information uploaded to ARTMS that is collected, and maintained but not shared or disclosed outside the ACF organization includes: PII as general audit information: auditee Information: auditee name, organizational name, address, auditee point-of-contact and contact information (phone number, email address); audit firm Information: organizational name, address, Employer Identification Number (EIN), primary auditor point-of-contact and contact information (phone number, email address); and non PII data includes: type of report issued by the auditor of the financial statements of the auditee (e.g. qualified, adverse or disclaimer opinion); where applicable a statement of deficiencies in internal controls that were disclosed by the audit and whether any such conditions were material weaknesses; statement of disclosure of noncompliance which is material; where applicable a statement of significant deficiencies in internal controls over major programs – whether any are material weaknesses; the type of report issued by the auditor on compliance for major opinions or disclaimer; list of Federal award agencies which receive a copy of the reporting package; dollar threshold; the name of each Federal program and identification of each major program, and corrective action plan. ARTMS was designed to limit the number of ACF's overdue audits by implementing responsibility and accountability for resolving each audit and focusing on audit findings. The audit resolution process is 180 days before the audit becomes overdue by the OIG. Using ARTMS reduces the number of audits that shows up on ACF steward report for OIG and enables oversight and management to resolve audits within the 180 day limit. ARTMS provides on-line processing and real time tracking of ACF's audit workload facilitating follow up and resolution of audit findings.

PII collected from system users (federal staff and direct contractors in the form of program support staff, administrators and developers) in order to access the system, consists of user credentials (i.e. username, password,Personal Identity Verification (PIV) card). Users/system administrators that include ACF employees and direct contractors use HHS user credentials. In rare situations where end user's PIV may not be accessible, an alternative access method is available where end users use the GrantSolution's Single Sign In (SSI) application/module to generate a username, password, and One-Time Password (OTP)/authentication code for access control and identity management.

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

The HHS OIG downloads the single audit reporting packages from the FAC. OIG's NEAR reviews the findings, determines which findings merit actions, assigns each audit finding an internal, tracking REC Number (there may be several Rec Codes for each finding), and sends the audit report and findings in hard-copy to the responsible HHS and ACF organizations. The Audit Report File (in text format) and Findings (in text format) are uploaded into searchable data fields within ARTMS; and Attachment A (Microsoft Word Format) that contains the Rec Codes and Rec Code Narratives are included as attachment to the individual audit records. Information uploaded to ARTMS in the audit report and findings includes: PII as general audit information: auditee Information: auditee name, organizational name, address, auditee point-of-contact and contact information (phone number, email address); audit firm Information: organizational name, address, Employer Identification Number (EIN), primary auditor point-of-contact (POCs) and contact information (phone number, email address) are used to provide contacts for audit resolution purposes; and non PII data: type of report issued by the auditor of the financial statements of the auditee (e.g. qualified, adverse or disclaimer opinion); where applicable a statement of deficiencies in internal controls that were disclosed by the audit and whether any such conditions were material weaknesses; statement of disclosure of noncompliance which is material; where applicable a statement of significant deficiencies in internal controls over major programs – whether any are material weaknesses; the type of report issued by the auditor on compliance for major opinions or disclaimer; list of Federal award agencies which receive a copy of the reporting package; dollar threshold; the name of each Federal program and identification of each major program, and corrective action plan.

ARTMS also enables direct download of the entire single audit files from the FAC providing the ability to gather greater details on the identified audits and findings downloaded from the NEAR. ARTMS was designed to limit the number of ACF's overdue audits by implementing responsibility and accountability for resolving each audit and focusing on audit findings. ARTMS facilitates and simplifies the audit resolution process through identification and collection of corrective actions, and tracking and monitoring follow-up to resolve audit findings. The audit resolution process is 180 days before the audit becomes overdue by the OIG. Using ARTMS reduces the number of audits that shows up on ACF steward report for OIG and enables oversight and management to resolve audits within the 180 day limit. ARTMS provides on-line processing and real time tracking of ACF's audit workload by facilitating follow up and resolution of audit findings. PII collected from users/system administrators (federal staff and direct contractors in the form of program support staff, administrators and developers) in order to access the system, consists of user credentials (i.e. username, password, Personal Identity Verification (PIV) card, authentication code). Users/system administrators that include ACF employees and direct contractors use HHS user credentials. In rare situations where end user's PIV may not be accessible an alternative access method is available where end users use the GrantSolution's Single Sign In (SSI) application/module to generate a username, password, and One-Time Password (OTP)/authentication code for access control and identity management.

**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

HHS User Credentials

Username, password, and One Time Password (OTP) or authentication code.

Employer Identification Number (EIN)

Financial Statements

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

Employees

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

Vendor/Suppliers/Contractors

Employee includes direct contractors.

**How many individuals' PII is in the system?**

<100

**For what primary purpose is the PII used?**

PII (HHS User Credentials) and Username, password and OTP/authentication code is used for authentication. Data contained in the individual grants records to include: auditee Information: auditee name, organizational name, address, auditee point-of-contact and contact information (phone number, email address); audit firm Information: organizational name, address, Employer Identification Number (EIN), primary auditor point-of-contact and contact information (phone number, email address) are used to provide points-of-contact for audit resolution purposes.

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

Not Applicable (N.A.)

**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?**

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 09-90-0100; System name: Civil and Administrative Investigative Files of the Inspector

**Identify the sources of PII in the system.**

**Directly from an individual about whom the information pertains**

In-Person

Online

**Government Sources**

Within OpDiv

Other HHS OpDiv

**Identify the OMB information collection approval number and expiration date**

N/A

**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.**

System users/system administrators that include ACF employees and direct contractors will be! notified that their information is collected for the purpose of creating a system user account to access! the system. This notification will occur prior to/at the time of account creation. PII collected from! Auditees and Auditors is collected during and for the purpose of completing the single audit process,! the responsibility for notification resides with the auditee, auditors and FAC when the information is! 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.**

Users/system administrators that include ACF employees and direct contractors implicitly consent to the collection and use of their PII and may opt out of having a user account to access the ARTMS. If they do not provide the information they will not be granted access. PII collected from Auditees and Auditors is collected during and for the purpose of completing the single audit process, the responsibility for notification and the options to opt out would resides with the auditee, auditors. and FAC when the information is collected.

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

End users (that use the HHS credential for logon) that include ACF employees and direct contractors! account PII is collected by Information Technology Infrastructure and Operations (ITIO), HHS for the! purpose of creating a credential for network and computer logon. Any notification for the purpose of! obtaining consent from the individuals whose PII is contained in the originating system when major! changes occur to the system would be provided by ITIO, HHS.!End users (that use the SSI credential for logon) that include ACF employees and direct contractors!account PII is collected in the SSI module for the purpose of creating a credential for application!logon. Any notification for the purpose of obtaining consent from the individuals whose PII is!contained in the system when major changes occur to the system would be provided by ARTMS!System Administrator and ARTMS lead. PII collected from Auditees and Auditors is collected during!and for the purpose of completing the single audit process, the responsibility for notification and!obtaining consent resides with the auditee, auditors and FAC when the information is collected.

**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.**

End users (that use the HHS credential for logon) that include ACF employees and direct contractors account PII is collected by ITIO, HHS for the purpose of creating a credential for network and computer logon. It is the responsibility of ITIO, HHS to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. End users (that use the SSI credential for logon) that include ACF employees and direct contractors account PII is collected in the SSI module for the purpose of creating a credential for application logon. It is the responsibility of the ARTMS lead to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. PII collected from Auditees and Auditors is collected during and for the purpose of completing the single audit process, the responsibility for resolving issues resides with the auditee, auditors. and FAC when the information is collected.

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

End users (that use the HHS credential for logon) that include ACF employees and direct contractors account PII is collected by ITIO, HHS for the purpose of creating a credential for network and computer logon. Any notification and follow up activity for the purpose of periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy would be provided by ITIO,HHS.

End users (that use the SSI credential for logon) that include ACF employees and direct contractors account PII is collected in the SSI module for the purpose of creating a credential for application logon. Any notification and follow up activity for the purpose of periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy would be provided by the ARTMS lead.

PII collected from Auditees and Auditors is collected during and for the purpose of completing the single audit process, the responsibility for notification or periodic review resides with the auditee, auditors. and FAC when the information is collected.

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

**Users:**

Federal employees and direct contracts in support of the program offices, for identifying! auditees for the purpose of oversight and management efforts to address identified audit! findings; and to ensure auditees complete corrective actions to address individual audit findings! in a timely and effective manner.

**Administrators:**

Direct Contractors will have access to create and manage end users accounts.

**Contractors:**

Direct Contractors will have access to create and manage end users accounts.

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

The ARTMS lead determines ARTMS team member roles and responsibilities, and authorizes and approve ARTMS Team member access to the ARTMS. Role based access ensures that the levels of access are restricted to job function. Access levels are assigned on a need to know basis, only the necessary application access required to perform their duties.
End users (that use the HHS credential for logon) that include ACF employees and direct contractors account PII is collected by Information Technology Infrastructure and Operations (ITIO), HHS for the purpose of creating a credential for network and computer logon.
End users (that use the SSI credential for logon) that include ACF employees and direct contractors account PII is collected in the SSI module for the purpose of creating a credential for application logon. Role -based account access is defined by the roles, responsibilities, and authorities approved by the ARTMS lead. ARTMS administrations will create end users accounts and access control for end users based upon role-base access defined and approved by ARTMS lead and team.

**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 ARTMS lead determines ARTMS team member roles and responsibilities, and authorizes and approve ARTMS Team member access to the ARTMS. Role based access ensures that the levels of access are restricted to job function. Access levels are assigned on a need to know basis, only the necessary application access required to perform their duties.

End users (that use the HHS credential for logon) that include ACF employees and direct contractors account PII is collected by Information Technology Infrastructure and Operations (ITIO), HHS for the purpose of creating a credential for network and computer logon.

End users (that use the SSI credential for logon) that include ACF employees and direct contractors account PII is collected in the SSI module for the purpose of creating a credential for application logon. Role -based account access is defined by the roles, responsibilities, and authorities approved by the ARTMS lead. ARTMS administrations will create end users accounts and access control for end users based upon role-base access defined and approved by ARTMS  lead and team.

**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.**

All Department users to include federal employees, and direct contractors users must review and sign an acknowledge statement of the HHS Rule of Behavior (RoB).  This acknowledgment must be completed annually thereafter, which may be done as part of annual HHS Information Systems Security Awareness Training.  All users of Privileged User accounts for Department information technology resources must read these standards and sign the accompanying acknowledgment form in addition to the HHS RoB before accessing Department data/information, systems, and/or networks in a privileged role.  ARTMS system end users are required to complete the following: Annual HHS Information Systems Security Awareness Training; Annual HHS Privacy Training; and Reading the Rules of Behavior for Use of HHS Information Resources and signing the accompanying acknowledgment.

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

N.A. System end users receive no system specific training.  An ARTMS Users Guide was developed and is available for end users.

**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.**

ARTMS management is in communications with the ACF Records Manager to determine the specific National Archive and Records Administration (NARA) retention schedule.  All records will be retained until a determination is made as to the final records disposition schedule.  Once established the records will be disposition consistent with the records disposition schedule.

**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 is conducted
User manuals
Contractor Agreements

Technical Controls:
User Identification and Authorization via separate access control software and separate network! operations Personally Identity Verification (PIV) card capabilities.
Firewalls at hosting site and Department firewall for federal staff computers
Monitoring and Control scans provided by hosting agency
PIV cards

Physical controls

The system server is hosted in a secure data center and can be physically accessed by only the authorized infrastructure staff from ACF/HHS can access.  Enforcement of established physical security capabilities (management walk-throughs and assessment of security locks, doors, desks, storage materials, Security Guards employing access controls to individuals requesting facility access:

Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.All physical access to data centers by employees is logged and audited routinely. Physical containment and isolation of Systems, Data bases, and Storage assets that collection, maintain, store, and share PII. Secured and limited access facilities: data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee. Compartmentalization and physical separation of system components (servers, cables, storage access, off-site backup facilities and storage). Employment of Locks, Fences, Geographic Isolation of physical system assets.