US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/21/2016

OPDIV:

ACF

Name:

Enterprise Reporting System (COE)

PIA Unique Identifier:

P-4512199-557653

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.

New Public Access

Describe the purpose of the system.

The Grants Center of Excellence (GCOE) delivers end-to-end grants management products and support to over 1200 programs in eight Federal departments. Managed by the Administration for Children and Families (ACF) within the U.S. Department of Health and Human Services (HHS) in partnership with the Denali Commission, our mission is to provide comprehensive and cost-effective grants management solutions for grantors, grantees, and the public.

GCOE provides comprehensive, cost-effective grants management solutions for both grantors and grantees. COE products support the entire grants management business lifecycle – from pre-award through post-award – for all types of grants, across all grant categories.
To provide these services the COE operates the GrantSolutions a comprehensive grants management system available to all Federal grant-making agencies as part of the Grants Management Line of Business (GMLoB) initiative. It services all types of grants (service, training, demonstration, social research, and cooperative agreements) across all grant categories (discretionary, formula, block, and entitlement).

The suite of GrantSolution core products covers all 14 stages of the grants management business including: Full life-cycle processing (pre-award through post-award) for all types of grants; Funds control integration with financial systems, financial reports, audit tracking; Flexible mechanisms for program-specific needs and performance reports; Standard system interfaces to Grants.gov and other external systems; and Electronic grantee interface to foster collaboration between grantor and grantee.

GrantSolutions also provides optional products of which is the Enterprise Reporting System (ERS) that provides additional functionality that allows partners to build their own custom reports to analyze grant data by leveraging the extensive business analytics tools within the Cognos platform (and is not a system but a reporting tool employed to support GrantSolutions grantors). ERS allows customers to view and print reports from the GrantSolutions and Online Data Collection systems. The reports can be saved and printed as Excel, PDF or Text file document. ERS offers several advantages to customers that include: Use of a stable and robust technology; Role-based controlled access to sensitive reports and data; and grantor selection and generation of standard reports from a report library. ERS staff can also create specific reports for grantors and information is emailed to customers in a variety of formats.

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

GrantSolutions also provides optional products of which is the ERS that provides additional functionality that allows grantors to build their own custom reports to analyze grant data by leveraging the extensive business analytics tools within the Cognos platform (and is not a system but a reporting tool employed to support GrantSolutions customers). ERS allows grantors to view and print reports from the GrantSolutions and Online Data Collection systems. The reports can be saved and printed as Excel, PDF or Text file document. ERS offers several advantages to grantors that include: Use of a stable and robust technology; Role-based controlled access to data; and grantor selection and generation of standard reports from a report library. ERS staff can also create specific reports for grantors and information is emailed to grantors in a variety of formats. PII collected from users/system administrators and grantors 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 only. Grantors use username and password.

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

GrantSolutions also provides optional products of which is the ERS that provides additional functionality that allows grantors to build their own custom reports to analyze grant data by leveraging the extensive business analytics tools within the Cognos platform (and is not a system but a reporting tool employed to support GrantSolutions customers). ERS allows grantors to view and print reports from the GrantSolutions and Online Data Collection systems. The reports can be saved and printed as Excel, PDF or Text file document. ERS offers several advantages to customers that include: Use of a stable and robust technology; Role-based controlled access to data; and grantor selection and generation of standard reports from a report library. ERS staff can also create specific reports for grantors and information is emailed to customers in a variety of formats. PII collected from users/system administrators and grantors 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 only. Grantors use username and password.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

HHS User Credentials

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

Employees

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

Employee includes direct contractors. Grantors include business partners.

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

PII (HHS User Credentials) and username and password is used for authentication.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within 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 (ACF employees and direct contractors), and grantors 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.

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.

End Users (ACF employees and direct contractors), and grantors implicitly consent to the collection and use of their PII and may opt out of having a user account to access the ERS. If they do not provide the information they will not be granted access. End Users can indicate that they opt out by selecting a check box on the account request screen.

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

End users 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.

Grantors will not be notified because it is the responsibility of ITIO, HHS to obtain consent from the individuals whose PII is contained in the originating system when major changes occur 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.

End users 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.

Grantors will notified the ERS administrator 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 system administrator will notify the System Manager. The System Manager will provide details back to the concerned individual relating to the standard Investigative and resolution process to address an individual’s concerns when they believe their PII has been inappropriately obtained, used, or disclosed.

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 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.

The need and requirement for data integrity, availability, accuracy, and relevancy will be identified by system users and can be rectified by contacting the system program manager or system help desk with concerns about their user account. Also should the end user require and update to the PII data in the end user account (e.g. name, email address, location (mailing address) or phone number change) the end user can contact the system program manager or system help desk with concerns about their user account.

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

Administrators:

ACF employees and Direct Contractors will have access to create grantor end users accounts.

Contractors:

ACF employees and Direct Contractors will have access to create grantor end users accounts.

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

The GCOE lead determines GCOE team member roles and responsibilities, and authorizes and approve GCOE Team member access to the ERS. 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 include ACF employees and direct contractors account PII is collected by ITIO, HHS for the purpose of creating a credential for network computer logon. Role -based account access is defined by the roles, responsibilities, and authorities approved by the GCOE lead.

ERS administrations will create end users accounts and access control for grantors based upon role-base access defined and approved by GCOE 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 GCOE lead determines GCOE team member roles and responsibilities, and authorizes and approve GCOE Team member access to the ERS. 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 include ACF employees and direct contractors account PII is collected by ITIO, HHS for the purpose of creating a credential for network computer logon. Role -based account access is defined by the roles, responsibilities, and authorities approved by the GCOE lead.

ERS administrations will create end users accounts and access control for grantors based upon role-base access defined and approved by GCOE 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, contractors, and other system 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.

The Enterprise Reporting 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.

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.

GCOE management is in communications with the ACF Records Manager to determine the specific 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 conducted by hosting agency (NIHCIT)

User manuals

Contractor Agreements

Technical Controls:
User Identification and Authorization via via separate access control software and separate network operations Personal 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