US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/13/2016

OPDIV:

ACF

Name:

Application Review Module

PIA Unique Identifier:

P-7769395-313052

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?

Yes

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 (COE) provides comprehensive, cost-effective grants management solutions for both grantors and grantees. COE products support the entire grants management business life-cycle – from pre-award through post-award – for all types of grants, across all grant categories.

The COE's highly configurable product options allow partners to streamline processes and drive standardization across their agencies without sacrificing the ability to meet unique needs. By combining core and optional products, partners can tailor the solution to meet their particular requirements.

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 GrantSolutions 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 Application Review Module (ARM) that streamlines, structures and tracks the competitive panel review process and supports remote panel reviews. These applications come from Grants.gov for grant award panel review for each program entity. Applications are scored and the results are sent to the program office for selection and grant award.

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

ARM provides functionality that streamlines, structures, tracks, collects and maintains (stores) grant application and application review scores information for grant award panel review for each program entity. Applications are scored and the results are sent to the program office for selection and grant award. The information contained in the review and resultant scores include the grantee organization name, a unique grant score identifier that is created in ARM and the score. The full application that is submitted to Grants.gov is uploaded into GrantSolutions and is accessible for viewing and reviewing via ARM, but ARM does no upload, collect, maintain, store or share any information for the individual grant applications.

Access to the ARM is restricted to authorized users (review panel members, and select program office staff) that provide the following information for account creation and access control: Name; email Address

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

ARM provides functionality that streamlines, structures, tracks, collects and maintains (stores) grant application and application review scores information for grant award panel review for each program entity. Applications are scored and the results are sent to the program office for selection and grant award. The information contained in the review and resultant scores include the grantee organization name, a unique grant score identifier that is created in ARM and the score. The full application that is submitted to Grants.gov is uploaded into GrantSolutions and is accessible for viewing and reviewing via the ARM, but ARM does no upload, collect, maintain, store or share any information for the individual grant applications.

Access to the ARM is restricted to authorized users (review panel members, and select program office staff) that provide the following information for account creation and access control: Name; email Address. The ARM collects no Personally Identifiable Information (PII) other than that required for end user account creation.

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

the system only collect end user account PII in the form of an email account for temporary account

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

Employees

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

E-mail address is captured from end users for account creation and access control.

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

Not Applicable

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

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not Applicable

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 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, by email.

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 cannot opt out of the collection of their information because the system collects the following PII data from end users for access control: e-mail address and is based upon consent of the end users for creating an end user account.

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

Accounts are temporary and are only created for the short duration of the grant award panel for the purpose of providing access for grant application reviews. Therefore, it is not necessary to provide notification or to obtain consent when major changes occur to the system to end users.

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.

Accounts are temporary and are only created for the short duration of the grant award panel for the purpose of providing access for grant application reviews. The likelihood of their Personally Identifiable Information (PII) being inappropriately obtained, used or disclosed is minimal.

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

Accounts are temporary and are only created for the short duration of the grant award panel for the purpose of providing access for grant application reviews. Therefore, the need for periodic reviews for data quality, integrity, availability, accuracy and relevancy is not necessary.

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

Users:

Accounts are temporary and are only create for the short duration of the grant award panel for the purpose of providing access for grant application reviews.

Administrators:

Administrators have access to create accounts

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

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the program. The authorized and approved account creation request is submitted to the ARM system, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides ID/Password and one time code is sent to phone to authenticate himself/herself enabling account access. Phone number is entered at the time of login and used to send code to user. The phone number is not maintained in the system.

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.

End user accounts are requested through the program office system owner/program manager who reviews, authorizes and approves the creation of the end user account based upon the individual end user's roles and responsibilities associated with the program. The authorized and approved account creation request is submitted to the ARM system, system administrator who creates the individual account and notifies the end user of the authorized, approved, and created account. The end user initially logs on, provides appropriate information (what PII?) to authenticate himself/herself enabling account access. End users will review grant proposals and score based on content. Grant proposals contain organizational information for the entity applying for the grant.

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. ARM 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).

Not Applicable

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.

Accounts are temporary and are only create for the short duration of the grant award panel for the purpose of providing access for grant application reviews and do not fall within the constraints of record management retention and destruction guidelines.

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

The system is hosted in the Amazon Web Service (AWS) environment the following security controls are established:

Administrative controls, including but not limited to:
System security plan (SSP)
File backup/archive conducted by hosting agency National Institutes of Health, Center for Information Technology (NIHCIT)
User manuals
Contractor Agreements

Technical Controls:
User Identification and Authorization
Passwords
Firewalls at hosting site and Department firewall for federal staff computers
Monitoring and Control scans provided by hosting agency
Personal Identity Verification (PIV) cards

Physical controls
The system servers are 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 loacks, Fences, Geographic Isolation of physical system assets.