US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/08/2017

OPDIV:

CMS

Name:

Acquisition and Grants Exchange

PIA Unique Identifier:

P-6978702-432788

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?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Describe the purpose of the system.

The Office of Acquisition and Grants Management (OAGM) Intranet Web Portal, which is also known as the Acquisition and Grants Exchange (AGX), is a web-based application that provides the Office of Acquisition and Grants Management (OAGM) with the tools needed to present links to resources, documents, and other information in an organized manner. AGX is a website application that groups resources together so that users can access these resources from a single website/portal. The portal has six different communities meant to offer unique links and resources for contracting officers, contracting officer representatives (CORs), grants, acquisition policy, project managers and other.

The links presented are limited to internal use on the CMSnet intranet. Examples of resources/documents include OAGM policies, contract checklists, training documents for the acquisitions system, and general OAGM announcements.

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

The system will primarily just host various federal links to other websites. The system will also be able to store various documents that users can upload. Information will be limited to OAGM internal processes and procedures, training info, etc. No personal information about OAGM staff or the general public will be contained in these documents. Links may include the Federal Acquisition Regulation (FAR), a link to the latest Requisition policy, or a link to a new OAGM training. Documents include acquisition training presentations, contract templates, etc. Documents can include Word, PowerPoint, Excel, Visio, and jpgs. No information is collected from the documents - they are just stored in the system with a title. AGX utilizes user permissions so that only certain users can upload and other users approve documents. To control access, AGX collects the user's name and email utilizing active directory.

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

The system will primarily host various federal links to other websites. The system will also be able to store various documents that users can upload.

The system will not house PII-related information. Types of documents supported or Word, PowerPoint, Excel, Visio, PDF. Information will be limited to OAGM internal processes and procedures, training info, etc. No personal information about OAGM staff or the general public will be contained in these documents. The reason that the portal will collect this information is to act as a resource library for OAGM users (a one-stop-shop).

Only certain users can upload documents which are controlled by the system user privileges. All documents will also have to be approved by an OAGM approver role.

The Portal system will not require a separate login. Users are authenticated to the system using Active Directory. To do this, Active Directory does collect Name and E-mail. This information is not shared and is only collected temporarily to authenticate users. Each type of document is collected to provide acquisition resources to OAGM - a user decides if they want/need to upload a particular document and that document must be approved by a separate user. There are only two types of resources: links and documents. Links are used to support transporting users to other websites; documents provide acquisition-related information to the users.

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

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?

100-499

For what primary purpose is the PII used?

To authenticate users to the application and for user security priviledges. Users are authenticated to the system using Active Directory. To do this, Active Directory does collect Name and E-mail. This information is not shared and is only collected temporarily to authenticate users. The Name/Email authenticates a user and then that information correlates an individual to a security group with different privileges. Use of PII is not disclosed in the system because PII is only used to authenticate users and assign them security privileges. Users cannot see other users' PII.

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

N/A

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

Title 5 (TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES) 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

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.

No process exists because our application does not store PII data, it is only used to authenticate the user and the PII is not being retrieved by one or more PII element. PII collection in AGX is not subject to the Privacy Act because it is only authenticating the user.

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.

There is no option to opt out because the PII is used to authenticate to the application. The user can decide if they do not want to use the application. PII collection in AGX is not subject to the privacy act because it is only authenticating the user.

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

The individual does not receive notification when changes occur in the system. No PII is disclosed; the only information collected is the name/email for authentication. There is no functionality in the system that provides this information. An update to the system will have no impact on this information. PII collection in AGX is not subject to the Privacy Act because it is only authenticating the user.

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.

No process exists because our application does not store or disclose PII data, it is only used to authenticate the user. PII collection in AGX is not subject to the privacy act because it is only authenticating the user. If the user feels that the PII is inaccurate, they may contact the system administrator and revise the information within Active Directory. However, if the name and email address were incorrect, access would not be possible to the system AGX.

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

Under the process of requesting access via Active Directory through a System Administrator, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from AGX. The PII is available as needed, and is sufficient (minimum required) for the purposes needed. The PII fields are locked and cannot be changed; The process to ensure that individuals who provide or modify PII cannot repudiate that action is done within the source system. The process to ensure PII is available when needed is by having nightly updates run between Active Directory and AGX; the process to ensure that PII is sufficiently accurate for the purposes needed is ensured when the nightly updates are sync. Users, can at any time, request that their PII (access) be deleted, by contacting their System Administrator, who in turn, would take the corresponding action via Active Directory.

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

Administrators:

Admins can see the user's name to assign them to a specific security group

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

AGX has different user groups - anyone in the admin group has access to PII (user name); The CMS Information Security System Officer (ISSO) will have admin access and can view a list of all active members in the admin group.The reason the administrator group needs access to the user name is so they can assign proper security privledges to the different user roles. The administrators will conduct a monthly audit of users to determine what security privledges are required and whether or not they are an active user.

Add new comment

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.

Users with PII access can only see the minimum information, in this case, the user's name, so they can assign them to a specific user group. Admins cannot do anything else with the information.

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.

Annual CMS Privacy and Security Awareness Training which describes the process for proper handling of PII.

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

None.

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.

PII (names/emails) are securely stored in the AGX database. The AGX team runs quarterly audit reports and removes users who are no longer at CMS. National Archives Records Association (NARA), General Records Schedule (GRS) 20 states that AGX will destroy/delete when 7 years 6 months, 10 years 6 months, or 20 years 6 months old, based on the maximum level of operation of the Certification Authority, or when no longer needed for business, whichever is later; and GRS 24 states that AGX will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes. The Active Directory that provides the database with PII to AGX destroys the data. When the nightly updates sync with the AGX, than the data that is no longer needed is removed from Active Directory and does not appear in AGX.

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

PII data is not stored in the system, it is only used for authentication; only administrators have access to seeing user names; all information is stored in the database which is secured in the Baltimore data center. Only a data base administrator (DBA) can access the information with an approved script through the change control process. No one can access the database through the application. The AGX team runs quarterly audit reports and removes users who are no longer at CMS.