US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/22/2016

OPDIV:

CMS

Name:

Enterprise Website Supporting Tool

PIA Unique Identifier:

P-6815566-324416

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The purpose of the Enterprise Website Support Tools (EWST) is to maintain and assist with configuration management of the code and documentation of the following systems: Exchange Consumer Web Services (ECWS); Find Local Help (FLH); and Premium Estimation Tool (PET). These systems are subject to the Federal Information System Management Act and have their own Privacy Impact Assessments. EWST is made up of the following tools that maintain and assist with the configuration management of the code and documentation for the systems listed above: GitHub Enterprise Server; Jira ; Confluence; Crowd; Splunk; MapBox; and HipChat. EWST is hosted on the Amazon Web Services (AWS) data center.

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

EWST collects login credentials for both CMS employees and contractor support which consists of login user ID and password. Name and email address is also maintained.

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

EWST maintains and assists with the configuration management of the code and documentation of tools. It does not collect, maintain or store any information other than CMS employee and contractor support user ID, password, name and email address. This information is required to create a user account within EWST which allows the user to access the application for purposes of conducting configuration management of the code and documentation of the system.

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

Other - Login credentials- user ID and password

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?

EWST collects name, email and login credentials for both CMS employees and contractor support. This information is required to create a user account within EWST which allows the user to access the application for purposes of configuration of code and documentation.

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

None

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

5 U.S.C. 301 Department 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.

09-70-0538, Individuals Authorized Access to CMS Computer Services

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A for user credential information collection.

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 prior notice is given by EWST, as the PII is collected by another CMS application.

The individual requesting access to EWST contacts their CMS component's CMS Access Administrator (CAA) via email, providing the CAA with their Name, User ID, and email address. The CAA, in turn, enters the data into the Enterprise User Administration (EUA) system, requesting approval for access to the appropriate user job code. This action initiates an email to the EWST System Administrator (SA), requesting his/her approval in EUA. Upon approval, EUA notifies the individual, that their request has been granted. In turn, the SA builds the new user record in EWST, which permits
the individual access.

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.

The PII that is collected is in a separate application, which is the EUA, therefore there is no ability to opt-out.

If the user requires access to EWST, they cannot 'opt-out' of providing their PII to EUA, as the User ID, Name and Phone Number are the identifiers used to create the user within the application's security module.

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

The collection of PII (user credentials) is not done by EWST so there is no notification process. EWST receives the PII via another CMS application, EUA .

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 login credentials, name and email address within this system are not collected by EWST. The PII is collected from the individual by another CMS system which is Enterprise User Administration (EUA). The EUA PIA describes 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. Individual's concerns involving their PII (user credentials), are addressed by the EUA team (a function of the maintenance contractor, Lockheed Martin).

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

In order to maintain the integrity, availability, accuracy, and relevancy of the PII stored within the database, the System Administrator, semi-annually, performs a
crosswalk between the EUA listing of individuals with the appropriate job code and EWST's listing of active users. Any anomalies (i.e. name change, or mismatch) is addressed and resolved by contacting the user, and modifying their user data, or by removing their access to EWST, if no longer required under their current job description.

Under this process, outdated, unnecessary, irrelevant, and inaccurate PII is identified and deleted from EWST. 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 (EUA) system. The process to ensure PII is available when needed is by having nightly updates run between the EUA systems and CROWD; 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 CAA, who in turn, would take the corresponding action via EUA.

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

Users:

Users (CMS employees and contractors) require access to EWST to assist with configuration management of code and documentation.

Administrators:

Administrators (CMS employees and contractors) require access to operate and maintain the system. They also have the ability to create and modify user account.

Contractors:

Contractors as administrators require access to operate and maintain the system. They also have the ability to create and modify user account.

Contractors as users require access to EWST to assist with configuration management of the code and documentation.

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

Access to EWST is provided through EUA. Prospective users must request a CMS ID which must be approved by the employees' manager. After the CMS ID is received, the individual requests access through the EUA system. Access requests for User or Administrator roles for various tools are directed to the manager for approval.

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.

EWST uses the principle of least privilege as well as a role based access control to ensure administrators and users are granted access on a need-to-know/minimum necessary, commensurate with their assigned duties.

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.

Both employee and contractor staff are required to complete the annual CMS Security and Privacy Awareness training provided annually as Computer Based Training (CBT) course.
Individuals with privileged access must also complete role-based security training commensurate with the position they are working.

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

Contractors also complete their own annual corporate security 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.

National Archives and Records Administration (NARA), General Records Schedule (GRS) 20 states

that EWST 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 EWST will delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes.

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

The EWST system is located in a Tier-1 network data center (Amazon Web Services) which provides premier physical control protections.
Physical controls are in place such as security guards ensure that access to the buildings is granted to authorize individuals. Identification of personnel is checked at the data center. The EWST system is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied.

Personally Identifiable Information (PII) on the EWST system is secured administratively by ensuring that the system goes through the Assessment and Authorization (A&A) process, and all documentation is submitted to the Information Security & Privacy Group (ISPG) that supports the system and to comply with Federal Information Security Management Act (FISMA) regulations. The system is currently hosted at the Amazon Web Services (AWS) data center. The user identity data is stored in the centralized Lightweight Directory Access

Protocol (LDAP) store managed by Enterprise Identity Management (EIDM). EWST sends user Identity information to EIDM for user authentication and are required to authenticate to establish their identity and role as an individual or system interacting with the target system. EWST applies the principle of least privilege as well as a role based view on granting rights. All access for the groups are requested and approved before being granted. All Production access requires Manager Approval. Each user is assigned a role and each role's rights are restricted to only the data and server resources needed to perform their job.

Access requests are tracked via service request tickets. For planning, approving, and auditing, EWST utilizes a Roles and Responsibilities matrix to review and track what resources are accessible at the application level as well as the server level. A monthly audit is performed for system accounts and quarterly user driven validation of accounts is required. New EWST team members are processed through an on boarding process that defines their role and all information and approvals are archived in a track able service request.