US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2025

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

No changes within the PIA.

Describe the purpose of the system.

The purpose of the Enterprise Website Support Tools (EWST) is to offer shared services to the Centers for Medicare and Medicaid (CMS) applications. EWST includes GitHub Enterprise Server; Jira Data Center; Confluence Data Center; Slack, MiniOrange and SonarQube.

The EWST application is hosted in the CMS private cloud located in the Amazon Web Services (AWS) data center in the AWS East region (North Virginia). EWST depends upon AWS Infrastructure as a Service (IaaS) for its physical infrastructure and cloud components. On top of this, the CMS Office of Communication (OC) AWS Cloud Team provides AWS platform level management including providing security controls at the operating systems and Virtual Private Cloud (VPC) level.EWST offers shared services that are available over the public internet, but only from whitelisted IP addresses. Akamai acts as the webhost proxy system, providing a Domain Name

System (DNS) and a web application firewall. EWST, inside of Amazon Web Services (AWS), connects to the Akamai proxy through the public internet, but both sides whitelist each other and require public key infrastructure (PKI) certificates signed by VeriSign and validating the certificates with the Symantec Certificate Authority (CA).

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

EWST collects login credentials passed through Enterprise User Administration (EUA), for both Centers for Medicaid and Medicare (CMS) employees and contractor support which consists of login user ID and password. Akamai and Amazon Web Services (AWS) also collect within EWST (Jira) user ID, full name, email address, and mobile phone number for users, along with name and userID of CMS approvers. This information is required to create user accounts within the Akamai Control Center (ACC) and to create within AWS administrative accounts for testing. AWS also collects full name, phone number and email address of each key point of contacts for operational reasons. Akamai, AWS and EUA have their own PIA that can be referenced for further information.

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

EWST subsystems pass login credentials from their applications to Enterprise User Administration (EUA) for identification and authentication. Akamai and Amazon Web Services (AWS) also collect within EWST (Jira) user ID, full name, email address, and mobile phone number for users, along with name and user ID of CMS approvers. This information is required to create user accounts within the Akamai Luna administration panel, and to create AWS administrative accounts for testing. Public Website Shared Services (PWSS) collects within EWST (Jira), the user's full name, email address, organization name, and Short Message Service (SMS) phone number to issue GEO Application Programming Interface (API) encryption keys. AWS also collects the full name, phone number and email address of each Key Point of Contact for operational reasons. Physical Security System personnel who access or use the system do not use any personal identifiers to retrieve records held in the system. This system does not retrieve records using Personal identifiable information (PII) on individuals, but instead obtains those credentials from Enterprise User Administration (EUA) and maintains them.

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
Phone Numbers
Other: Login credentials- user ID and password; Organization Name.

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

Personally identifiable information (PII) is required for user identification and authentication, for Geographic (GEO) API key administration, for Key Point of contact (POC) contact lists, for user

registration to Luna and Amazon Web Services (AWS), and for other operational reasons.

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?

No

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Private Sector

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.

Both JIRA and Confluence have a login screen featuring a warning notice and the PII is collected by other CMS applications, which have other notifications in place such as AWS, Akamai and PWSS.

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 for users to opt-out of PII information collection since it is necessary for users to register to access GEO API, Luna and Akamai.

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. EWST receives the PII via another CMS application, Enterprise User Administration (EUA). EWST also collects the user registration information for other systems which also have PIA in place and are responsible for the PII they collect: Amazon Web Services (AWS), Akamai and Public Website Shared Services (PWSS).

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, phone number and email address within this system are not collected by EWST. All EWST users are CMS organizational users. 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) and this process is inherited by the EWST system. The PII is also collected from individuals for other systems that have PIAs in place that describe this process: Akamai, AWS, and PWSS.

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 databases, regular synchronization between EUA, Lightweight Directory Access Protocol (LDAP) and EWST systems occurs daily. 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 be repudiated since that action is done within the source EUA system. Users, can at any time, request that their PII (access) be deleted, by contacting their CMS Access Administrator (CAA), who in turn, would take the corresponding action via EUA. Data integrity is checked by the user when providing the information for user registration or by the system administrator when issuing accounts in Akamai Luna and AWS or when API keys are issued and distributed for PWSS.

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

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

Access to EWST is provided through EUA. Based on the user's role, 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 scheme to ensure administrators and users are granted access on a need-to-know basis (minimum necessary), commensurate with their assigned duties. CMS oversight and approval are required for a user to obtain an account in EWST.

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).

Direct 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.

The retention and destruction of EWST data is governed by the CMS Records Schedule. This schedule is aligned with the National Archives and Records Administration (NARA) guidelines for data retention and destruction. The following CMS Records Schedule Items apply:https://www.cms.gov/Regulations-and-Guidance/Guidance/CMSRecordsSchedule/index.htmlEnrollment RecordsDisposition Authority Number: DAA-0440-2015-0006-0001Cutoff Instruction: Cutoff at the end of the calendar year.Retention Period: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.Beneficiary RecordsDisposition Authority Number: DAA-0440-2015-0007-0001Cutoff Instruction: Cutoff at the end of the calendar year.Retention Period: Destroy no sooner than 10 year(s) after cutoff but longer retention is authorized.Provider and Health Plan RecordsDisposition Authority Number: DAA-0440-2015-0008-0001Retention Period: Destroy no sooner than 7 year(s) after cutoff but longer retention is authorized.Analytic and Research Files (restricted) Disposition Authority Number DAA-0440-2015-0009-0002Transfer to the National Archives for Accessioning: 20 year(s) after cutoff. Research and Program Analysis: Supporting RecordsDisposition Authority Number: DAA-0440-2015-0009-0003Cutoff Instruction: Cutoff at the end of the calendar year.Retention Period: Destroy 10 year(s) after cutoff or when no longer needed for agency business, whichever is later.In addition, the EWST application follows the Data Destruction Standards prescribed in NIST Special Publication (SP) 800-88.

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 EUA. EWST sends user Identity information to EUA for user authentication and users 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 is 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 service request.