US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2016

OPDIV:

CMS

Name:

Terremark PaaS Cloud Service Provider

PIA Unique Identifier:

P-4748345-584595

The subject of this PIA is which of the following?

General Support System (GSS)

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.

None

Describe the purpose of the system.

The Terremark Cloud Service Provider Platform as a Service (TRMK CSP4PaaS) is an extension of the Terremark Infrastructure as a Service (IaaS) system. It is a cloud computing service model that supports CMS' application design; application development, testing, deployment and hosting; and application services such as team collaboration, web service integration, database integration, security, scalability, storage, persistence, state management, application versioning, application instrumentation and developer community facilitation. The TMRK CSP4PaaS is a General Support System (GSS) that supports CMS computer systems.

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

The TMRK CSP4PaaS does not collect, maintain or share infromation besides access credentialing information. It is part of the information technology (IT) infrastructure that supports CMS applications, programs and systems that may collect, store and transmit information. It requires user credentials to administer/access the PaaS.

To obtain access to the system, a user needs to obtain authority from the CMS Collaborative Application Lifecycle Tool (CALT) or the Enterprise User Administration (EUA) system. Once access is approved, the user ID and password are required.

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

TMRK CSP4PaaS is a secured cloud-based Platform as a Service GSS. It does not collect, maintain or share information besides access credentialing information . It provides computer processor, memory and Storage Area Network (SAN) storage and is available through a custom Graphical User Interface (GUI) called Infinicenter. Management of this environment is conducted through the GUI.

To access the PaaS or the applications and systems hosted within the environment, user name and password are required. Access for these users is provided via a Secure Socket Layer (SSL) Virtual Private Network (VPN) solution. Both access methods use a two factor authentication solution for access. Terremark supports the PaaS platform from the primary, hypervisor level down to the core infrastructure that makes up the private Federal-only cloud.

User credentials are created in the CALT system or in the EUA system, both of which have their own PIAs for the PII that resides within it.

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

Yes

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

Other - User 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?

The primary use of PII is to create a user account and obtain access to the system.

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 Section 301, Departmental Regulations

Are records on the system retrieved by one or more PII data elements?

No

HEALTH INSURANCE EXCHANGE PROGRAM (HIX) .09-70-0560

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

Other

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.

Individuals are notified each time they attempt to log into the system by a "warning banner." The banner advises the user that they are accessing a Government owned system. The user must accept the terms and conditions of the banner to gain 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.

There is no option to 'opt out' of providing PII to access the TMRK CSP4PaaS system as it is necessary to perform their job functions.

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

When changes are meade to the system or platform, auto-notification emails are generated out by the Change Control Board (CCB) and /or Change Advisory Board (CAB) to inform of the upcoming events / changes.

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 PaaS Event Management Plan describes the process for reporting events related to improper handling or exposure of PII and the process to resolve that event. The workflow includes contacts for the CCB and CMS help desk support.

Upon completion and /or resolution of an event, auto-emails and notifications are generated to inform of status changes.

An individual can create a CALT help desk ticket to correct inaccurate PII that may have transferred to this system.

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

An automated system is in place to verify account activity and de-activate accounts which exceed established account inactivity thresholds. Periodic manual reviews also are completed to ensure compliance and validate the automated processing.

PII integrity is monitored by file permissions for access to the system or applications that reside on it. Availability is addressed through periodic data backup and monitoring of network activity. Data accuracy is done by cross-evaluating the user accounts with CALT and EUA. Relevancy is monitored by periodic data refresh with those systems and deletion of outdated user accounts.

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

Administrators:

Some administrators may have access to PII for specific functions, such as; account creation, modification, and deletion.

Contractors:

Specific contractors who support user account administrative efforts. Based on role based assignments as administrators or generic users.

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

Individuals designated as account management personnel are provided access to account management functionality via access controls in accordance with 'least privilege.'

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.

Based on user group assignments users are granted read, write and execute privileges to specific assigned data elements. Additionally, two-factor authentication and encryption provide technical controls and account access is monitored and logged.

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.

System personnel participate in CMS' Annual Security Awareness and Privacy training. Training on account management policies and procedures are provided for administrative, account management personnel.

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

Account use and maintenance documentation is provided to all users who receive an account. The documentation provides instruction on initial account setup and ongoing use.

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.

Accounts are checked weekly for activity. Accounts are initially deactivated after 60 days of inactivity and are permanently deactivated after 90 days of inactivity. The latter requires the new account request process to be followed for reactivation. Accounts records are maintained indefinitely for historical audit capabilities and are stored in compliance with the National Archives and Record Administration General Records Schedules 20, Item 2a4, which state: Destroy/delete 1 year after cutoff, or when no longer needed for Agency business, whichever is longer; and GRS 24, Item 13a1, which states:
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.

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

Administrative controls in place are access by "least privilege", request and approval of access through the CALT and EUA systems and role-based functions for individual users.

Technical controls used to secure PII are that accounts are maintained in an encrypted data store using Active Directory tools. Accounts are only accessible by administrative personnel who have established an encrypted connection to the private cloud environment (SSLVPN).

The physical controls include door locks, personnel badges and security guards at the data center where the system resides.