US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/16/2016

OPDIV:

CMS

Name:

Terremark IaaS Cloud Service Provider

PIA Unique Identifier:

P-6070651-393338

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.

Not applicable.

Describe the purpose of the system.

The Terremark Cloud Service Provider Infrastructure as a Service (TMRK CSP4IaaS) is an Infrastructure as a Service (IaaS) cloud computing service model. The TMRK CSP4IaaS provides CMS with on-demand access to network functionality for communications and data transmissions. This allows CMS to communicate internally and externally. The TMRK CSP4IaaS enables CMS with the flexibility and speed in deploying computing resources in the quantities and durations to meet their specific requirements.

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

TMRK CSP4IaaS does not collect, store or share information. It is the infrastructure that supports applications that may transmit information. However, user credentials are necessary to administer the system and maintain it. The credentials consist of name, phone number and email as well as user ID and password.

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

TMRK CSP4IaaS is the infrastructure that supports other systems and applications. It does not collect, store or share information. However, to maintain the system, users login with a user ID and password to support the system. The users must have a CMS Enterprise User Administration (EUA) account to have access to the system. The EUA account information is supplied to TMRK CSP4IaaS from the EUA system and is not created in this system.

The user ID and password is passed over secure socket connection in compliance with CMS standards for system access. The TMRK CSP4IaaS environment offers processor, memory and Storage Area Network (SAN) storage and is accessible to TMRK CSP4IaaS administrators via a custom Graphical User Interface (GUI) called Infinicenter. Management of this environment is conducted through the GUI.

Systems hosted within the environment also require remote access by administrative personnel, testers, developers, Database Administrators (DBAs) and other support personnel. Access for these users is provided via a Secure Socket Layer (SSL) Virtual Private Network (VPN) solution. Both access methods use two factor authentication.

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

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?

System access via a user ID and password is the primary purpose of the PII used by the system. To obtain access to TMRK CSP4Iaas, a user must request the profile code in EUA and is assigned to the system for access to administer the system and maintain it.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within OpDiv

Non-Governmental Sources

Private Sector

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.

Users are aware of a requirement to submit user credentials to obtain access to the system. A confirmation email is sent to the user to verify identity and create the system administrator account.

Additionally, at the login screen there is a warning message that the system is restricted to authorized users for business purposes only and that there is no expectation of privacy since it is a government system and that user activity may be monitored for administrative and security reasons.

System users must acknowledge acceptance of the terms of the warning banner by clicking on the acceptance button displayed beneath the warning banner prior to being allowed to move forward and access the system.

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 the use of user credentials (PII) because access to the system requires the input of user credentials in order to perform job duties.

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

When changes are made to the system, auto-notification emails are generated out by the Change Control Board (CCB) and /or Change Advisory Board (CAB) to inform of the upcomnig 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 IaaS event management plan describes the process for reporting events related to improper handling or exposure of PII and the process to resolve that event. This document contains the process for determining the path for problem management, change management, and incident management. The workflow includes contacts for Program Management,Configuration Control Board, and help desk support.

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

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 via file permissions and ownerships specific to the data owner as set by the operating system functions for read, write, and execute file functions. Availability is addressed by routine data backup and monitoring network availability. Data accuracy is done by the EUA system and updating the accounts with access to TMRK CSP4IaaS. Data relevancy is based on periodic data refresh with the EUA system to ensure data is current.

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

Administrators:

Administrators have access to PII for the management of users that have access to the system for account creation, modification and deletion.

Contractors:

Contractors, in their role as an Administrator, would have the access to PII for the management of users that have access to the system for account creation, modification and deletion.

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. Role assignment determines access control.

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 for potential access to PII.

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 security awareness training is required for all personnel. CMS supplies the training as part of new employee orientation and is required annually for the length of employment/access to CMS systems. 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 and are permanently deactivated after 90 days of inactivity. The latter requires a new account request process to be followed for reactivation. Per NARA approved records retention schedule: Delete/destroy when agency determines they are no longer needed for administrative, legal, audit or other operational purposes
(Disposition Authority: GRS 20, Item 1).

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

The administrative controls in place are: system access control in accordance with least privilege, request and approval for access through the EUA and role-based access function approvals. Technical controls used to secure PII are the use of encryption on stored PII and while it is beeing transmitted. Additionally, PII is only accessible by administrative personnel who have established an encrypted connection (SSL VPN).

The physical controls in place to secure PII include door locks, personnel badges, and assignment to specifica hardware components.