US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/14/2016

OPDIV:

OS

Name:

HSMP and SPS Infrastructure as a Service

PIA Unique Identifier:

P-9885524-216613

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?

New

Does the system have Security Authorization (SA)?

No

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

Describe the purpose of the system.

The purpose of the system is to provide secure hosting to Health System Measurement Project (HSMP) and Strategic Planning System (SPS) applications. The servers are hosted in a secure environment at an Amazon Web Services (AWS) facility.

The Health System Measurement Project (HSMP) brings together trend data on a limited set of key health system measures from multiple data sources to provide a picture of the status of the U.S. health system.

The Strategic Planning System (SPS) provides HHS senior leadership the capability to track progress on strategic plans, provide flexibly with varying workgroup structures, timelines and mandates, enhances the current planning and reporting process to make it simpler and less time-consuming, increases opportunity for coordination of effort to reduce duplication, and informs leadership about high-visibility plans on an ongoing basis. Plans are maintained and stored on the SPS website.

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

No information is captured by AWS, instead all data is stored at the child HSMP and SPS application level and Privacy Impact Assessments (PIA) exist for each application capturing the specific type of information stored and maintained.

The system collects and stores contractor system administrator user identifier, passwords, and email addresses (they are not considered "Direct Contractors". Contractor names are not separately stored in the system.

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

The Infrastructure as a Service System provides the hosting and maintenance for the HSMP and SPS applications for which separate PIAs have been submitted. The hosting is at an AWS facility. The type of hosting is referred to as Cloud hosting where connections to the applications that are being hosted are provided over the Internet. The hosting platform itself, beyond enabling Internet connections to the HSMP and SPS applications, does not store any information. It also provides the security boundaries for the applications.

Personally Identifiable Information (PII) is collected in the form of contractor user identifiers that are used as user names, passwords and email addresses (they are not considered "Direct Contractors"). This PII is deleted from the system for System Administrators that leave the project and for all System Administrators when the project ends. Contractor names are not separately stored in 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

System Administrator passwords

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

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

System Administration

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

System Maintenance

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

5 USC 301, Departmental regulations

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

No

N/A

N/A

N/A

Identify the sources of PII in the system.

Email

Online

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.

System Administrators are made aware via verbal notification that their email address and username are used for accessing the system when they first provided the login information and the personal information will be collected in 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.

System administrators understand that opting out is associated with their access credentials being terminated.

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

The contractor project manager notifies system administrators of any changes that will impact the existing access credentials or if additional credentials are needed that would require additional user names and passwords.

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.

In the event that PII has been inappropriately obtained, used, or disclosed, the affected person(s) would escalate this concern to the contractor project manager in writing. The contractor project manager would engage with the appropriate channels to investigate the root cause and work on a process to resolution.

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

The integrity, availability, accuracy and relevancy of the data is ensured because the administrators (whose PII is contained in the system) are charged with reviewing, monitoring and ensuring that new accounts are setup and terminated as necessary. As a result ensuring outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system.

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

Administrators:

Provide system administration and maintenance.

Contractors:

Provide system administration and maintenance.

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

Designated System Administrator access is determined by the staffing of the project and is managed by the contractor project manager. The established policy is that System Administrators have access to each other's email address that are used as stored user names in the system. However, they do not have access to each other's passwords

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.

The policy is that System Administrators use their PII (credentials) solely for the purpose of administrative and maintenance functions of the system.

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.

There is no training and awareness provided since users know that the only purpose of the email address and name stored in the system is to allow administrative users to authenticate to access the system. All HHS employees and contractors are required to complete annual privacy and security training.

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

N/A

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.

The General Records Retention Schedule 4.3, Item 040 applies: Destroy immediately after copying to a record keeping system or otherwise preserving, but longer retention is authorized if required for business use.

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

The user names and credentials for the IaaS are stored using the Amazon AWS Identity and Access Management service (IAM). IAM provides securely controlled access to services and resources and has been covered by the AWS Federal Risk and Authorization Management Program (FEDRAMP) package. has been covered by the AWS Federal Risk and Authorization Management Program (FedRAMP) package.

AWS' infrastructure services can accommodate many types of customer applications, with different security objective categorizations depending on the type of data processed by the application. The AWS infrastructure meets the NIST 800-53 Low control baseline, plus the additional FedRAMP controls.

Examples of controls used to secure PII in the HSMP & SPS IaaS system:
Administrative controls:
System Security Plan
Contingency Plan

Technical Controls:
User Identification
Passwords

Physical controls:
Due to the nature of the AWS environment all HSMP & SPS IaaS servers are hosted by Amazon AWS Datacenters. The security safeguards for the Amazon AWS Datacenters is covered by the pre-existing FedRAMP Agency Authority to Operate (ATO) for the AWS US EastWest System, May 13, 2013.