US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/03/2022

OPDIV:

ACF

Name:

Enterprise Operations System (EOS) - SmartSimple

PIA Unique Identifier:

P-1467687-435386

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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.

In order to modernize operations, ACF is seeking to implement an instance of Smart Simple's Platform3 application, to be utilized as Software as a Service (SaaS), addressing the Budget Execution and Human Capital Management needs as below:

1. The Budget Execution module is where the spending plan is established for each office. The workflows will support and track the execution of Operations against the spending plan. Additionally, the system will support funding requests whereby users can request funds for various activities such as purchase orders, travel, and training for approval.

2. The Human Capital Management module will provide tracking for all positions within ACF. It will track the number of filled and vacant positions and assist with the on/off-boarding of personnel. Each position will be associated with one or more funding sources which will provide the ability for ACF to view the amount of funds available for new personnel actions. It will also assist with succession planning.

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

The system will store data related to the following: Position Descriptions, Funding Sources, Personnel assigned to a position (name, office location, email, phone number, grade and step, salary, mailing address, employment status, employee ID), Accounting Codes, Budget Formulation and Purchase Requests.

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

The system will enable the forecasting, tracking and management of the individual Budget Line items under each funding source within the Enterprise Operations System. It will store records regarding the human capital planning and budget execution for the life of the system. The system maintains and stores the following information: Position Descriptions, Funding Sources, Personnel assigned to a position (name, office location, email, phone number, grade and step, salary, mailing address, employment status, employee ID), Accounting Codes, Budget Formulation and Purchase Requests. However, this system is used for planning and tracking purposes only and is not a system of record.

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

Yes

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

Date entered service (Start Date)

Date started position

Employee ID

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

PII is used to track Employee information, salaries, and its impact on organizational budget. PII is retrieved using Employee ID.

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

Succession Planning

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?

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.

OPM GOVT-1 - General Records

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Paperwork Reduction Act (PRA) does not apply to federal employees acting within scope of their employment. Additionally, if any information entering the system is PRA, it is being collected elsewhere and will have its own PRA number (possibly multiple of them).

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.

This system functions as a secondary system that leverages the data that is collected by other primary systems. No additional data is collected within this system that is not covered by prior notices. Data is currently kept in internal ACF spreadsheets. The data in the spreadsheets will be imported into the EOS. The spreadsheets are populated using data from the HHS Human Resources Employment Processing System (HREPS). and Budget information systems.

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.

Any PII information contained within the system was provided in the host systems from which the data originally came from, in accordance with the existing regulations within the HHS ACF. Specific to users of EOS, they must provide information to create an account on the system in order to do their work. For these reasons, there are no options within EOS to opt-out of the use of PII in this system.

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

No such changes are anticipated. If EOS changes its practices with regard to the collection or handling of PII, the Agency will adopt measures to provide any required notice and obtain consent from individuals regarding the collection and/or use of PII. This may include e-mail to individuals, adding or updating online notices or forms, or other available means to inform the individual.

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.

Any PII information entered into the system is provided in accordance with the existing regulations within the HHS ACF. EOS leverages existing data maintained in other systems (specifically the HREPS and Budget Information systems. As such, there is no process in place for users to correct their PII in 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.

Data Integrity

Data integrity is maintained by disabling access for users no longer associated with the organization or position that requires access. Use of the hypertext transport protocol secure (HTTPS) internet protocol ensures data integrity using encryption when users enter or receive data while using the system. The EOS staff and organizational users review data periodically.

Availability

Data availability is ensured through the underlying infrastructure supported and maintained by AWS. Since EOS is deployed in Amazon Web Services (AWS), the application is deployed on virtual machines that can be created in a short time and can scale quickly. This guarantees high availability since the supporting infrastructure can be provisioned and terminated on-demand with little to no delay while ensuring an immutable infrastructure concept, which guarantees security at the

infrastructure-level.

Accuracy
Data is imported from existing spreadsheets maintained by ACF. The EOS can import those spreadsheets into the system and the system produces an import data report showing the results of the data import process each time. These reports are saved and available for review by EOS staff to ensure accuracy of the imported data when compared to the source spreadsheets.

All organizational user accounts are reviewed on a monthly basis by Account Administrators to ensure that each account remains compliant with previously established account management requirements. Data is verified by the organization. Any changes to the data in the system is updated by authorized users from each organization.

Relevancy
Data is available to EOS organizational users for audit purposes. User login and password data files are covered by National Archives and Records Administration (NARA) General Records Schedule (GRS) Transmittal 31 Section 3.2, Information Systems Security Records, item 0.30; the data will be destroyed when no longer needed for agency/information technology (IT) administrative purposes. The records retention schedule is being determined for the user contact data, and until records are destroyed, they are retained in the system indefinitely.

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.

Role based access controls will be in place to prevent users from accessing the PII that should not be relevant for their daily work activities.

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.

Role based access controls will be in place to prevent users from accessing the PII that should not be relevant for their daily work activities.

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.

All personnel including both direct contractors and government personnel are required to participate in the ACF annual security compliance training and privacy training.

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

System users will be provided basic training on how to use the system and system functionality. This includes a Training manual for system operations.

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 system can be configured to follow the data retention policies of HHS ACF. Specifically the

following records schedules are applicable to this system:
GRS 1.3, item 050, Budget administration records
GRS 2.2, item 010, Employee management administrative records.
All documents created by this system are considered working draft documents and not official records. The information is kept for as long as needed.

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

Administrative
Access to EOS is restricted to authorized users who have been approved by the EOS Administrators to represent their associated Organizations within ACF. Fields can be categorized as PII and be masked via configuration settings if required. The system also supports Data categorization and security and retention policies that can define how long specific data is retained as well as who can access and view data. Access to PII by users is determined through role-based access control (RBAC), where roles are given permissions that define what each user is permitted to view and access. Additionally, all personnel accessing or operating the EOS must read and sign the Rules of Behavior (RoB) prior to gaining access to the system.

Technical
Technical controls as listed below:
All traffic between end users and the authorization boundary is through hypertext transport protocol secure (HTTPS) (TCP, 443).
Authorized users must provide their username and password to gain access to the system.
The system supports multifactor authentication through time-based one-time-passwords (TOTPs).
A maximum of five (5) failed logon attempts are permitted before the system locks the user.
Passwords must be changed once every sixty (60) days.
System and application logs are reviewed regularly to track auditable events.
SmartSimple manages system and communications protections such as boundary protections and antivirus/antimalware solutions.

Physical
Physical controls are inherited from the Cloud Service Provider (CSP).

AWS provides a security control statement for all physical controls in these three control families: Maintenance (MA), Media Protection (MP), and Physical and Environmental (PE).

EOS is completely virtualized via AWS GovCloud. EOS leverages the Provisional Authorization for AWS GovCloud for the physical control families.