US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2022

OPDIV:

ACF

Name:

Smartsheet

PIA Unique Identifier:

P-4889586-783510

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

In order to provide world-class acquisition support to the ACF mission, the Office of Government Contracting Services (GCS) requires a collaborative Business Intelligence system other than basic and common word processing technologies to view and manage the current and future contracting workloads; create, customize, and automate workflows; provide data analytics or dashboard capabilities; and provide a customer-centric interface for new business. This solution is flexible with features for capturing information, project and workload planning, managing work, automating processes, and reporting, which the Government manages through application user roles, business rules, and service level agreements rather than physical control of assets and direct software licensing.

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

Smartsheet.gov will store information used for project and contract tracking such as: Period of Performance PoPs, projected start/end dates, project/contract status, contract numbers, Budget Information, Vendor Names, address, Project/Contract Points of Contact (POC), email addresses,

and phone numbers.

Accounts for Administrators/Users required for login are established using only the individuals first and last names as well as their email address. Once established, administrators/users access the system using multi-factor authentication single sign-on.

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

Smartsheet centers around “sheets” that contain information relating to a particular project or projects. Within each sheet, users can include a variety of details relating to a project(s) and contract (s), such as a description, status, due dates, PoPs, award values, and which users may have been assigned to complete a task. Users can also attach files, add comments, and request updates, among other options.

There are several ways to view sheets, including a spreadsheet-like grid view, Kanban-style cards, Gantt charts, and a calendar view.

Email address, names, and phone numbers are used by Smartsheet assign tasks and send alerts and notifications to the user. This information may also be collected as reference information as it relates to a contract or project.

Budget information is input by a user and can be used in any number of ways. Because Smartsheet is spreadsheet based, users may opt to use the platform in lieu of other standard spreadsheet software for capturing and managing budget information.

Dates, such as Contract PoP start and end dates, are captured and used by Smartsheet as a trigger to notify or alert users when a date has passed, is nearing, or is in the future. Additionally, this information can be used as data filtering criteria.

Contract specific data, such as contract numbers, is used collected and used by the user(s) as reference material.

Smartsheet uses encryption to allow users to safeguard and maintain control over their data. All data is stored with National Institute of Standards and Technology (NIST) approved ciphers, transport layer security (TLS) technology, AES 256-bit at-rest encryption, and Amazon’s S3 service to store and serve uploaded files. Data is stored for three (3) months following account de-activation.

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

Yes

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

Projected start/end dates

Budget Information

Vendor Names

Contract Points of Contact; user credentials

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

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

Assigning roles, tasks, alerts, notifications, and worksheet access.

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

Automated alerts and reminder notifications can be sent to users within the GCS Smartsheet account:

Alerts are reactively triggered by changes to a sheet and notify stakeholders of updates to critical information;

Reminders are proactively triggered by a specific date or time and keep task owners apprised of key deadlines;

Both alerts and reminders can be set up individually or together as part of a larger workflow with multiple conditions.

They can also be sent to multiple recipients on a recurring basis.

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

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Not Applicable – Smartsheet does not require an OMB information collection approval number for the information captured.

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 their personal information will be collected upon initial login to the Smartsheet platfrom, all users, both individuals and system users are directed to review and accept the latest Smartsheet Privacy Notice describing how content may be shared, stored, and accessed through the offerings.

The privacy offerings can be found at https://www.smartsheet.com/legal/privacy-offerings

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.

If an individual wishes to Opt-Out, the Smartsheet's Privacy Page (https://www.smartsheet.com/legal/privacy#rights) provides information on how users can withdraw their consent where processing is based on a consent previously provided using an embedded link found by clicking the help button after logging into the system.

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

Smartsheet may amend, update, or revise their privacy notice from time to time reflecting changes to privacy practices, changing technologies, industry practices, regulatory requirements, or for other reasons. If material changes are made that affect the way data is treated, Smartsheet will notify users by email, through the Sites or Offerings, or by other legally acceptable means. Users are encouraged to periodically review the Smartsheet Privacy notice for the latest information on privacy practices.

Upon initial login to the Smartsheet platfrom, users are directed to review and accept the lastest Smartsheet Privacy Notice describing how content may be shared, stored, and accessed through the offerings. The privacy offerings can be found at https://www.smartsheet.com/legal/privacy-offerings

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.

Details regarding Individual's Rights related to Access, Erasure, Objection, Probability, Rectification, Restriction, and Withdrawal of Consent are all available on Smartsheets privacy information page https://www.smartsheet.com/legal/privacy. All individuals with access to HHS's Federal information and information systems must report a suspected or confirmed breach to the OpDiv or HHS as soon as possible and without unreasonable delay, consistent with OpDiv and HHS incident management policies and procedures.

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 need and requirement for data integrity, availability, accuracy, and relevancy will be identified by system users and can be rectified by contacting the system program manager or system administrator with concerns about the account. Also, should the system user require an update to the PII data in their account (e.g., name or email address), the user can contact the system owner or system administrators with a request.

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.

Smartsheet Owners and Administrators assign User Roles based on the access needed within Smartsheet.

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.

System user accounts are either assigned through the program office system owner/system administrators or requested through the Smartsheet application. The system owner/program manager then reviews, authorizes, and provides approval to the system administrator to create or approve the account. Once an account is established by the system administrator, the application will automatically notify the new user via email with authentication instructions.

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.

The HHS Learning Management System (LMS) provides annual Cyber Security and Privacy Training which covers the handling and management of PII on HHS information systems. Users must satisfactorily pass a test demonstrating knowledge and proficiency in protecting any information being collected and maintained.

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

Smartsheet offers training on their website which includes a section related to the different types of roles and access given related to those roles. A similar training will be provided to ACF GCS.

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.

ACF GCS will remain in continuous communications with the ACF Records Manager to determine the specific National Archives and Records Administration (NARA) retention schedule. All records will be retained until a determination is made as to the final records disposition schedule. Once established, the records will be disposed of consistent with the records disposition schedule. The following Records Schedule Numbers apply: DAA-GRS-2013-0003-0001 and DAA-GRS-2013-0003-0002 Financial transaction records records related to procuring goods and services, paying bills, collecting debts, and accounting; DAA-GRS-2016-0001-0001 Bids and proposals neither solicited nor accepted.

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

Personally Identifiable Information (PII) is secured and protected in the system using a multi-layer approach. Smartsheet uses multi-factor authentication (MFA) to securely log into the platform. ACF users must be connected to the ACF Government network using Government Furnished Equipment and authenticated through Microsoft 365. Then the user may access Smartsheet using single sign-on MFA. Additionally, Smartsheet utilizes NIST approved ciphers, transport layer security (TLS) technology, AES 256 at-rest encryption, Amazon's S3 service to store and serve uploaded files.

Identify the publicly-available URL:

https://app.smartsheetgov.com

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null