US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/19/2025

OPDIV:

ACF

Name:

Smartsheet

PIA Unique Identifier:

P-4889586-783510

The subject of this PIA is which of the following?

Major Application

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Significant System Management Change

Increased in the range of number of Personally Identifiable Information (PII) records in the system

Describe in further detail any changes to the system that have occurred since the last PIA.

Since the last PIA, the Smartsheet system has been reclassified from a smaller, less complex system (Minor Application) to a more significant system (Major Application), which means it now requires more robust management and security. Additionally, the system now collects more Personally Identifiable Information (PII), increasing from less than 100 records to between 100 and 499 PII records. These changes indicate both an expansion in system usage and the volume of data managed.

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 collect and store information related to project and contract tracking, including periods of performance (PoPs), projected start and end dates, contract status, contract numbers, budget details, vendor names, mailing addresses, points of contact (POC) for contracts, as well as email addresses and phone numbers.

The system also creates accounts for administrators and users, which are established using their first and last names and email addresses. Access to the system requires logging in with both a password and a second security step MFA (multi-factor authentication) single sign-on.

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 is a system that organizes information into 'sheets' where users can track project and contract details, such as descriptions, deadlines, contract numbers, mailing addresses and assigned team members. Users can also attach files, add comments, and request updates. These sheets can be viewed in various formats, including a grid, calendar, and timeline view (Gantt chart)

The system collects and stores names, email addresses and phone numbers to assign tasks and send notifications to users. It also collects contract-specific data, such as contract numbers, project periods of performance (PoPs), and budget information, which is used to manage and track projects. Important dates, such as contract start and end dates, are used to trigger alerts and reminders for users.

Smartsheet employs robust security measures to protect all data. All data is encrypted both when it is transmitted (using Transport Layer Security or TLS) and when it is stored (using AES 256-bit encryption). These encryption methods are approved by the National Institute of Standards and Technology (NIST) and ensure that sensitive data is protected against unauthorized access. Files uploaded to Smartsheet are stored securely using Amazon’s S3 service. In the event of account deactivation, data is retained for three months before being permanently deleted.

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
Mailing Address
Phone Numbers

Contract Period of Performance dates; contract numbers
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.

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Personally Identifiable Information (PII) such as names, email addresses, and phone numbers, is primarily used to manage access to the system, assign tasks, and send alerts or notifications to users. This information ensures that users are correctly identified and assigned appropriate roles through role-based access control. Role-based access control means that each user is granted access to only the data and tools they need based on their role in a project or within the organization. For example, administrators might have broader permissions to manage sheets and tasks, while regular users are limited to specific functions. Additionally, PII enables the system to notify users of important updates or tasks related to their projects.

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

In addition to the primary purpose, PII is used to facilitate automated alerts and reminder notifications within the GCS Smartsheet account. These notifications ensure that users stay informed about changes and upcoming deadlines. Alerts are triggered by changes to a sheet, such as an update to key project information, and notify relevant stakeholders. Reminders are set up in advance and triggered by specific dates or times, keeping task owners aware of critical deadlines.

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.

Directly from an individual about whom the information pertains
Email
Online
Identify the OMB information collection approval number and expiration date
Within Application
Identify the SORN(s)
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 of the collection or use of their personal information, they can do so by visiting the Smartsheet's Privacy Page (https://www.smartsheet.com/legal/privacy#rights). This page explains how users can withdraw consent for processing personal data by managing their privacy preferences, which include access, correction, and deletion rights. Users can find these options by clicking the help button after logging into the system. Since submitting PII is voluntary, individuals are not required to provide personal information unless they choose to.

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 Health and Human Services (HHS) Learning Management System (LMS) provides annual Cyber Security and Awareness Training (CSAT) 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 Administration for Children and Families (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 General Records Schedule (GRS) 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.

Administrative Control:

Personally Identifiable Information (PII) is secured and protected in the system using a multi-layer approach. Access to Smartsheet is restricted to authorized ACF users, who must connect to the ACF Government network using Government Furnished Equipment (GFE). Authentication is conducted through Microsoft 365, where users utilize single sign-on (SSO) with multi-factor authentication (MFA) to access the platform securely.

Technical Controls:
Smartsheet employs advanced technical measures to safeguard PII. Multi-factor authentication (MFA) is used to secure logins, ensuring only authorized personnel gain access. Data is encrypted both in transit and at rest using NIST-approved ciphers, with Transport Layer Security (TLS) technology protecting data during transmission. Additionally, Smartsheet implements Advanced Encryption Standard (AES) 256-bit encryption for at-rest data security, ensuring robust protection against unauthorized access.

Physical Control:
PII is securely stored using Amazon's S3 service, a reliable and highly secure storage solution designed to protect uploaded files and ensure data integrity. The physical infrastructure supporting data storage is managed by Amazon Web Services (AWS), which enforces stringent access controls and adheres to industry-leading security standards to protect against physical and environmental threats.

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