

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

07/16/2024

**OPDIV:**

ACF

**Name:**

Enterprise Smartsheet

**PIA Unique Identifier:**

P-8562144-774328

**The subject of this PIA is which of the following?**

Major Application

**Identify the Enterprise Performance Lifecycle Phase of the system.**

Implementation

**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.**

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.**

ACF Tech has acquired a Smartsheet account that can be utilized by the entire agency, primarily for process and project management purposes. Secondary uses include gathering information for reporting and event registration, contingent upon meeting Paperwork Reduction Act requirements. This agency-wide Smartsheet platform enables offices with limited technology and data investment capabilities to utilize a flexible, no-code project/process management system. ACF Tech aims to discuss consolidating Smartsheet accounts with offices holding their own office-specific contracts to reduce overall agency costs.

Smartsheet offers a cloud collaboration platform allowing users to plan, manage, automate, and report on work, leveraging various collaboration features. Its intuitive interface empowers business users to swiftly configure, adapt, and refine their work processes for faster execution. Features include project tracking, smart grids, calendars, dashboards, cards, portals, forms, automations, and control center.

Smartsheet projects equip teams with essential tools for efficient project management, fostering collaborative execution with speed and accountability, ultimately leading to successful outcomes. Users can manage all aspects of complex projects and visualize tasks in Gantt, card, and calendar views. Smart grids offer a unified, customized project view to keep teams on track and on schedule, facilitating easy tracking of multiple components. Smart calendars synchronize teams with an interactive, comprehensive view of activities and critical timelines. Smart dashboards provide project owners and stakeholders with real-time insights into key performance indicators, trends, and summary reports. Smart cards enhance visual communication and collaboration, enabling teams to share and act on projects more effectively. Smart portals facilitate team collaboration and information sharing through easy creation and maintenance of centralized portals. Smart forms empower business users to expedite execution and encourage innovation by simplifying data collection and action. Smart automations streamline work processes with simple yet powerful automation rules, yielding quick implementation.

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

Smartsheet is used for process and project management. It will include operational information such as status of different tasks, assigned task owners, and other work tracking-related data elements. As documented in the System Categorization form, ACF's agency Smartsheet instance is anticipated to be used for use cases including management improvement, program monitoring and evaluation, and budget formulation. Most uses cases may include non-sensitive Personally Identifiable Information (PII) such as names, email, mailing address, and phone number. A minority of use cases for HR and security functions could collect sensitive PII such as date of birth, driver license number, social security number, passport, taxpayer ID, photo ID, education records, and employment status.

All users developing Smartsheet documents must authenticate into Smartsheet using Personal Identity Verification (PIV) credential or Login.gov credentials. If Smartsheet's form functionality is used for purposes such as report submissions or event registration with an audience that is not within ACF (e.g., grant recipients), those external respondents would only be able to submit information into the form but would not be able to see the back end of Smartsheet where the data are stored.

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

Smartsheet offers a cloud-based collaboration platform designed to facilitate planning, capturing, managing, automating, and reporting on work, all while leveraging a range of collaborative features. Its user-friendly interface empowers business users to swiftly configure, adapt, and enhance their work processes for faster execution. Key features of the application encompass project tracking, smart grids, calendars, dashboards, cards, portals, forms, automations, and a control center.

Primarily utilized for process and project management, Smartsheet serves as a repository for operational information such as task statuses, assigned owners, and other pertinent work tracking data. According to the System Categorization form, ACF's agency wide Smartsheet instance is expected to support use cases including management improvement, program monitoring and evaluation, and budget formulation. While some use cases may involve non-sensitive Personally Identifiable Information (PII) like names, email addresses, and phone numbers, a subset may entail sensitive PII, such as the collection of new hire forms containing identification numbers (e.g. Social Security Numbers, driver's license, passport, taxpayer ID), mailing address, education records, date of birth, and employment status for HR or security-related functions. Data stored within Smartsheet will be retained for as long as it remains relevant and in use.

Users may update their profile to include their picture.

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

Yes

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

Social Security Number  
Date of Birth  
Name  
Photographic Identifiers  
Driver's License Number  
E-Mail Address  
Mailing Address  
Phone Numbers  
Education Records  
Employment Status  
Passport Number  
Taxpayer ID

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

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

**How many individuals' PII is in the system?**

500-4,999

**For what primary purpose is the PII used?**

Identifying task owners, approvers, and individuals to be informed throughout project implementation and process tracking.

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

When an ACF program office holds a virtual event, technical assistance (TA) forum, conference, or any other form of meeting/convening they may use Smartsheet as a registration mechanism to include name, address, phone, and email. PII can also be collected and used for HR and security-related functions such as onboarding and clearance tracking.

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

5 USC 301, Departmental Regulation

**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

Online

Government Sources

**Identify the OMB information collection approval number and expiration date**

Other: If the Paperwork Reduction Act (PRA) is applicable, the PIA will be updated to include

State/local/tribal information collection numbers and expiration dates.

Other Federal Entities

**Is the PII shared with other organizations?**

Yes

**Identify with whom the PII is shared or disclosed and for what purpose.**

**Describe any agreements in place that authorizes the information sharing or disclosure.**

N/A

**Describe the procedures for accounting for disclosures.**

Smartsheet includes such documentation as there is an activity log attached to each asset indicating date, time, and person with email address. Documentation of purpose of disclosure is via emails with the involved parties.

**Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.**

When Smartsheet is used for use cases that collect PII like event registration, individuals will know their personal information is being collected because they will be directly asked for it.

Individuals are notified that their personal information will be collected upon initial login to the Smartsheet platform. 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. The consent withdrawal option can be found by clicking the help button after logging into the system.

For use cases such as event registration, personnel onboarding, and collaborating on / viewing information in Smartsheet, if individuals do not want their PII used they are not able to participate in the opportunity as there is no practical way to complete the process without providing PII.

ACF's enterprise Smartsheet is available as a flexible shared service across the agency. Offices that elect to use Smartsheet for project management or other purposes are responsible for establishing clear points of contact, notice, and data management processes for their use cases.

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

Smartsheet reserves the right to amend, update, or revise its privacy notice periodically to reflect changes in privacy practices, evolving technologies, industry standards, regulatory requirements, or other relevant factors. In the event of material changes that impact how data is handled, Smartsheet will notify users via email, through the Sites or Offerings, or by other legally acceptable means. Users are encouraged to review the Smartsheet Privacy notice regularly for the latest information on privacy practices.

Upon their initial login to the Smartsheet platform, users are prompted to review and accept the

latest Smartsheet Privacy Notice, which outlines how content may be shared, stored, and accessed through the offerings. The privacy offerings can be accessed at Privacy Offerings.

ACF's enterprise Smartsheet is available as a flexible shared service across the agency. Offices that elect to use Smartsheet for whatever purposes re responsible for establishing clear points of contact, notice, and data management processes for their use cases.

**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.**

Information concerning Individual's Rights pertaining to Access, Erasure, Objection, Probability, Rectification, Restriction, and Withdrawal of Consent can be found on Smartsheet's privacy information page at <https://www.smartsheet.com/legal/privacy>. It is imperative that all individuals who have access to HHS's Federal information and information systems promptly report any suspected or confirmed breaches to the OpDiv or HHS without delay, in accordance with OpDiv and HHS incident management policies and procedures.

In the event individuals feel ACF has inappropriately obtained, used, or disclosed their information or if their information is inaccurate, they can reach out to the creators of the relevant Smartsheet assets if they are known to the individual. If not, individuals can reach out to ACF's Data Tools team at [datatools@acf.hhs.gov](mailto:datatools@acf.hhs.gov) to investigate and resolve with the creators of the relevent Smartsheet assets.

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

Users of the system will recognize the importance of maintaining data integrity, availability, accuracy, and relevance. Any concerns regarding these aspects can be addressed by reaching out to the system program manager or system administrator for resolution. Additionally, if a user needs to update their Personally Identifiable Information (PII) data within their account (such as their name or email address), they can submit a request to the system owner or system administrators for assistance.

**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's access based on role based access requirements, needed by the organization to conduct required reporting 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.**

User permissions that grant ability to view data are set so that users only have access to the Smartsheet assets they are using or are explicitly granted access to due to need.

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.**

All federal staff complete annual security compliance training and privacy training.

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

ACF Tech has developed a system admin handbook and user Frequently Asked Questions (FAQ), in addition to providing technical support on user questions.

**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.**

Records will be maintained in accordance with their approved records schedule. These schedules are specific to the varied use cases Smartsheet can be used for across ACF and therefore users are responsible for working with their records officers to determine specific retention schedules as needed. The primary categories of General Retention Schedules that apply for ACF's enterprise Smartsheet use cases include the following. These are not an exhaustive list given the flexibility of Smartsheet for all sorts of administrative planning purposes:

Financial management and reporting administrative records DAA-GRS2016-00130001

Property, plant and equipment (PP&E) and other asset accounting. DAA-GRS2013-00030004

Budget administration records. DAA-GRS2015-00060007

Employee management administrative records. DAA-GRS2017-00070001

Recruitment records DAA-GRS2018-00080003

Administrative records maintained in any agency office. DAA-GRS2016-00160001

Technology management administrative records DAA-GRS2016-00130002

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

Administrative

Smartsheet is designed with least privilege by default. Any content (including PII) is only accessible to the author unless they choose to share it with other users. Only licensed users (granted by the system administrator in ACF Tech) can own content in Smartsheet and only owners can share content with others. An owner can share content to others with Admin, Editor or Viewer permissions. Owners of sheets with PII are responsible for taking care that only those who require access to the PII data can view and otherwise access/use it.

Technical

Smartsheet uses encryption to secure data. All data is durably 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.

Smartsheet maintains firewalls to protect data accessible by the Internet. They maintain programs and routines to keep Smartsheet up to date with the latest upgrades, updates, bug fixes, new

versions, and other modifications. They deploy anti-malware software, keeping it up to date.

#### Physical

Smartsheet has multi-site data redundancy and is hosted at Amazon Web Services (AWS) facilities that are SOC 1, SOC 2, ISO 27001, and Federal Information Security Modernization Act (FISMA) examined and certified. Data center monitoring includes biometric scanning protocols, continuous surveillance, and 24x7 production environment management.