SSP ATTACHMENT 4 –
FedRAMP Privacy Impact Assessment (PIA) Template

CSP Name

Information System Name

Version #.#

Version Date

Controlled Unclassified Information

 Prepared by

| Organization Name that prepared this document |
| --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Prepared for

|

| Organization Name for whom this document was prepared |
| --- |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

 |
|  | Street Address | Click here to enter text. |
| Suite/Room/Building | Click here to enter text. |
| City, State, ZIP | Click here to enter text. |

Record of Changes

| Date | Description |
| --- | --- |
| 9/30/2016 | Sec 1.2 clarity rewrites; and added Voice recordings to list of PII examples.Sec 2 clarity rewrites; Sec 3.1-3. Added NIST control identifiers and edits to questions Removed Acronyms and referenced FedRAMP Master Acronyms and Glossary resource document |
| 3/9/2017 | Renamed document from "FedRAMP Privacy Impact Assessment Template" to "SSP ATTACHMENT 4 - FedRAMP Privacy Impact Assessment (PIA) Template"  |
| 6/6/2017 | Updated logo |

Revision History

Detail specific changes in the table below

| Date | Version | Page(s) | Description | Author |
| --- | --- | --- | --- | --- |
| Click here to enter a date. | Click  | Click  | Click here to enter text. | Click  |
| Click here to enter a date. | Click  | Click  | Click here to enter text. | Click  |

How to contact us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *info@fedramp.gov*

For more information about the FedRAMP project, see [www.fedramp.gov](http://www.fedramp.gov)

Table of Contents

[1 PRIVACY OVERVIEW AND Point of Contact (POC) 1](#_Toc476809187)

[1.1 Applicable Laws and Regulations 1](#_Toc476809188)

[1.2 Personally Identifiable Information (PII) 1](#_Toc476809189)

[2 Privacy Designation 2](#_Toc476809190)

[3 Privacy Impact Assessment Talking Points 2](#_Toc476809191)

[3.1 PII Mapping of Components (SE-1, DM-1) 3](#_Toc476809192)

[3.2 Prospective PII Use 3](#_Toc476809193)

[3.3 Sources of PII and Purpose 4](#_Toc476809194)

[3.4 Access to PII and Sharing 4](#_Toc476809195)

[3.5 PII Safeguards and Liabilities 5](#_Toc476809196)

[3.6 Contracts, Agreements, and Ownership 6](#_Toc476809197)

[3.7 Accuracy of the PII and Redress 6](#_Toc476809198)

[3.8 Maintenance and Administrative Controls 7](#_Toc476809199)

[3.9 Business Processes and Technology 7](#_Toc476809200)

[3.10 Privacy Policy 8](#_Toc476809201)

[3.11 SIGNATURES 8](#_Toc476809202)

[4 ACRONYMS 8](#_Toc476809203)

List of Tables

[Table 1‑1 - System Name Privacy POC 1](#_Toc454977011)

[Table 3‑1 PII Mapped to Components 3](#_Toc454977012)

# PRIVACY OVERVIEW AND Point of Contact (POC)

The Table 1‑1 - System Name Privacy POC individual is identified as the System Name Privacy Officer and POC for privacy at CSP Name.

Table 1‑1 - System Name Privacy POC

| Name | Click here to enter text. |
| --- | --- |
| Title | Click here to enter text. |
| CSP / Organization | Click here to enter text. |
| Address | Click here to enter text. |
| Phone Number | Click here to enter text. |
| Email Address | Click here to enter text. |

## Applicable Laws and Regulations

The FedRAMP Laws and Regulations can be found on: www.fedramp.gov

Table 1‑2 Information System Name Laws and Regulations include additional laws and regulations specific to Information System Name. These will include law and regulations from the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), United States Code (USC), and Homeland Security Presidential Directives (HSPD).

Table 1‑2 Information System Name Laws and Regulations

| Identification Number | Title | Date | Link |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

## Personally Identifiable Information (PII)

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Information that could be tied to more than one person (date of birth) is not considered PII unless it is made available with other types of information that together could render both values as PII (for example, date of birth and street address). A non-exhaustive list of examples of types of PII includes:

* Social Security numbers
* Passport numbers
* Driver’s license numbers
* Biometric information
* DNA information
* Bank account numbers
* Voice recordings

PII refers to information that can be traced back to an individual person.

# Privacy Designation

Cloud Service Providers (CSPs) perform an annual analysis to determine if PII is collected by any of the system components. Clouds that do not collect PII and would like to opt-out of hosting privacy information may elect to do so and are not required to fill out the Privacy Impact Assessment Questions. If a CSP is willing to host PII, the Privacy Impact Assessment Questions should be answered given the current knowledge of the CSP. A CSP is not required to solicit customers for the information.

Federal cloud customers (data owner/system owners) are required to perform their own Privacy Impact Assessments, and may share this information with the CSP if they so desire (for informational purposes and/or to work with the CSP to develop processes and procedures for managing their PII).

Threshold Analysis

Check one.

|  |
| --- |
|[ ]  Opt-out. This cloud will not host privacy information.  |
|[ ]  This cloud is willing to host privacy information. Select the cloud layers that are represented by <System Name>. Select all that apply.  |
|[ ]  This cloud includes Software as a Service (SaaS).  |
|[ ]  This cloud includes Platform as a Service (PaaS). |
|[ ]  This cloud includes Infrastructure as a Service (IaaS).  |

# Privacy Impact Assessment Talking Points

According to NIST SP 800-122, Appendix D,

*There must be no personal data record-keeping systems whose very existence is secret.*

Additionally, NIST SP 800-122, Appendix D states,

*There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.*

In light of the NIST guidance, Privacy Impact Assessment talking points have been developed for the purpose of ensuring full disclosure between stakeholders.

Identifiers in parenthesis after a section title indicate NIST SP 800-53, Appendix J privacy controls that are related to the particular talking point. These mappings to Appendix J privacy controls are not considered a replacement for Appendix J controls.

## PII Mapping of Components (SE-1, DM-1)

System Name consists of Enter Number key components. Each component has been analyzed to determine if any elements of that component collect and/or store PII. The type of PII collected and/or stored by System Name and the functions that collect it are recorded in Table 3-1.

Table 3‑1 PII Mapped to Components

| **Components** | **Does this Component Collect or Store PII?****(Yes/No)** | **Type of PII** | **Reason for Collection of PII** | **Safeguards** |
| --- | --- | --- | --- | --- |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |
| Click here to enter text. | Select One | Click here to enter text. | Click here to enter text. | Click here to enter text. |

## Prospective PII Use

Respond to the following questions:

|  |
| --- |
| 1. Are there any data fields in the platform or application that have been targeted for the collection or storage of PII? If yes, please name those fields. (SE-1, DM-1, IP-1)
 |
| *Click here to enter explanation.* |
| 1. If PII fields are used, can individuals “opt-out” of PII fields by declining to provide PII or by consenting only to a particular use (e.g., allowing basic use of their personal information, but not sharing with other government agencies)? (IP-1)
 |
| *Click here to enter explanation.* |
|[ ]  Yes | Explain the circumstances of being able to opt-out of PII fields (either for specific data elements or specific uses of the data). (IP-1)  |
|  |  | *Click here to enter explanation.* |
|[ ]  No | It is not possible to opt-out.  |

## Sources of PII and Purpose

1. Does CSP Name have knowledge of existing federal agencies that provide PII that gets imported into the system? (AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Has any agency that is known to provide PII to the system provided a stated purpose for populating the system with PII? (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Does CSP Name currently populate the system with PII? If yes, where does the PII come from and what is the purpose? (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Will any third party sources be providing PII that will be imported into the system (if known)? Please explain. (AP-1, AP-2)

|  |
| --- |
| *Click here to enter explanation.* |

## Access to PII and Sharing

1. What third-party organizations will have access to the PII (if known)? Who establishes the criteria for what PII can be shared? (AP-1, AP-2, AR-8, IP-1, UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What CSP Name personnel roles will have access to PII fields (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP Name personnel to have access to the PII. (AR-8, UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. For CSP support staff, how is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access to PII require manager approval? (IP-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do other systems that interconnect to the system share, transmit, or access the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing of PII. (UL-2)

|  |
| --- |
| *Click here to enter explanation.* |

## PII Safeguards and Liabilities

1. What controls are in place to prevent the misuse (e.g., browsing) of PII by those having access? (AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? (AR-1, AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Does the CSP Name provide annual security training include privacy training? Does CSP Name require their contractors that have access to the PII to take the training? (AR-5)

|  |
| --- |
| *Click here to enter explanation.* |

1. Who is privacy officer responsible for assuring safeguards for the PII? (AR-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. What is the magnitude of harm to the individuals if privacy related data is disclosed, intentionally or unintentionally? (AR-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the PII owner advised about what federal agencies or other organizations share or have access to the data? (AR-1)

|  |
| --- |
| *Click here to enter explanation.* |

## Contracts, Agreements, and Ownership

1. NIST SP 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this accountability described in contracts with customers? Why or why not? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do contracts with customers establish who has ownership rights over data including PII? (AR-2, AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do contracts with customers require that customers notify CSP Name if the customer intends to populate the service platform with PII? Why or why not? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Do CSP Name contracts with customers establish record retention responsibilities for both the customer and CSP Name? (AR-2, AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the degree to which CSP Name will accept liability for exposure of PII clearly defined in agreements with customers? (AR-3)

|  |
| --- |
| *Click here to enter explanation.* |

## Accuracy of the PII and Redress

1. Is the PII collected verified for accuracy? Why or why not? (DI-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the PII current? How is this determined? (DI-1)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is there a process for individuals to have inaccurate PII that is maintained by the system corrected or amended, as appropriate?

*Click here to enter explanation.*

## Maintenance and Administrative Controls

1. If the system is operated in more than one site, how is consistent use of the PII maintained in all sites? Are the same controls used?

|  |
| --- |
| *Click here to enter explanation.* |

1. What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines? (AR-2, AR-3, DM-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures? (AR-2, DM-2)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the system using new technologies that contain PII in ways that have not previously deployed? (e.g., smart cards, caller-ID, biometrics, PIV cards, etc.)?

|  |
| --- |
| *Click here to enter explanation.* |

1. How does the use of this technology affect privacy? Does the use of this technology introduce compromise that did not exist prior to the deployment of this technology?

|  |
| --- |
| *Click here to enter explanation.* |

1. Is access to the PII being monitored, tracked, or recorded? (AR-4)

|  |
| --- |
| *Click here to enter explanation.* |

1. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision? (TR-2)

|  |
| --- |
| *Click here to enter explanation.* |

## Business Processes and Technology

1. Have the talking points found herein resulted in circumstances that requires changes to business processes?

|  |
| --- |
| *Click here to enter explanation.* |

1. Does the outcome of these talking points require that technology or operational changes be made to the system?

|  |
| --- |
| *Click here to enter explanation.* |

## Privacy Policy

1. Is there a system privacy policy and is it provided to all individuals whose PII you collect, maintain or store? (IP-1, TR-1, TR-3)

|  |
| --- |
| *Click here to enter explanation.* |

1. Is the privacy policy publicly viewable? If yes, provide the URL. (TR-1, TR-3)

|  |
| --- |
| *Click here to enter explanation.* |

## SIGNATURES

The information found herein has been documented by *Name of organization* and has been reviewed by the CSP Name, Chief Privacy Officer for accuracy.

|  |
| --- |
| Assessor Signature |
| Name | Enter Name | Date | Select date. |

|  |
| --- |
| Chief Privacy Officer Signature |
| Name | Enter Name | Date | Select date. |

# ACRONYMS

The master list of FedRAMP acronym and glossary definitions for all FedRAMP templates is available on the FedRAMP website [Documents](https://www.fedramp.gov/resources/documents-2016/) page under Program Overview Documents.

Please send suggestions about corrections, additions, or deletions to info@fedramp.gov.