FedRAMP Privacy Threshold Analysis   
and Privacy Impact Assessment Template



Enter CSP Name

System Name

Enter Version Number #.#

Version Date mm/dd/yyyy

For Authorized Use Only

Prepared by

| <Organization Name that prepared this document> | | |
| --- | --- | --- |
|  | Street Address |  |
| Suite/Room/Building |  |
| City, State, ZIP |  |

Prepared for

| <Organization Name for whom this document was prepared> | | |
| --- | --- | --- |
|  | Street Address |  |
| Suite/Room/Building |  |
| City, State, ZIP |  |

Revision History

| Date | Version | Page(s) | Description | Author |
| --- | --- | --- | --- | --- |
| Month DD, YYYY | 0.X | All or specific | Sample—Describe changes | Last name or Team Name |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1. PRIVACY OVERVIEW AND Point of Contact (POC) 1](#_Toc440543551)

[1.1. PRIVACY LAWS, REGULATIONS, AND GUIDANCE 1](#_Toc440543552)

[1.2. PERSONALLY IDENTIFIABLE INFORMATION (PII) 1](#_Toc440543553)

[2. PRIVACY THRESHOLD ANALYSIS 1](#_Toc440543554)

[2.1. QUALIFYING QUESTIONS 1](#_Toc440543555)

[2.2. DESIGNATION 1](#_Toc440543556)

[3. PRIVACY IMPACT ASSESSMENT 1](#_Toc440543557)

[3.1. PII MAPPING OF COMPONENTS 1](#_Toc440543558)

[3.2. PII IN USE 1](#_Toc440543559)

[3.3. SOURCES OF PII AND PURPOSE 1](#_Toc440543560)

[3.4. ACCESS TO PII AND SHARING 1](#_Toc440543561)

[3.5. PII SAFEGUARDS AND LIABILITIES 1](#_Toc440543562)

[3.6. CONTRACTS, AGREEMENTS, AND OWNERSHIP 1](#_Toc440543563)

[3.7. ATTRIBUTES AND ACCURACY OF THE PII 1](#_Toc440543564)

[3.8. MAINTENANCE AND ADMINISTRATIVE CONTROLS 1](#_Toc440543565)

[3.9. BUSINESS PROCESSES AND TECHNOLOGY 1](#_Toc440543566)

[3.10. PRIVACY POLICY 1](#_Toc440543567)

[3.11. ASSESSOR AND SIGNATURES 1](#_Toc440543568)

[4. ACRONYMS 1](#_Toc440543569)

List of Tables

[Table 1. System Name Privacy POC 1](#_Toc440530364)

[Table 2. PII Mapped to Components 1](#_Toc440530365)

How To Contact Us

For questions about FedRAMP or this document, email to [info@fedramp.gov](mailto:info@fedramp.gov).  
For more information about FedRAMP, visit the website at <http://www.fedramp.gov>.

1. PRIVACY OVERVIEW AND Point of Contact (POC)

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

Table 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. |

* 1. PRIVACY LAWS, REGULATIONS, AND GUIDANCE

A summary of laws, and regulations related to privacy include:

* 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104-231, 110 Stat. 3048
* 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
* Public Law 100-503, Computer Matching and Privacy Act of 1988
* E-Government Act of 2002 § 208
* Federal Trade Commission Act § 5
* 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
* Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
* OMB Circular A-130, Management of Federal Information Resources, 1996
* OMB Memo M-10-23, Guidance for Agency Use of Third-Party Websites
* OMB Memo M-99-18, Privacy Policies on Federal Web Sites
* OMB Memo M-03-22, OMB Guidance for Implementing the Privacy Provisions
* OMB Memo M-07-16, Safeguarding Against and Responding to the Breach of PII
* The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
* State Privacy Laws

Guidance on privacy issues can be found in the following publication:

* NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing  
  http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
* Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress
* https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
* Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)
* http://www.archives.gov/records-mgmt/bulletins/2010/2010-05.html
* Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks  
  https://www.fdic.gov/regulations/examinations/offshore/offshore\_outsourcing\_06-04-04.pdf
  1. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) as defined in OMB Memo 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

PII does not refer to business information or government information that cannot be traced back to an individual person.

1. PRIVACY THRESHOLD ANALYSIS

Enter CSP Name performs a Privacy Threshold Analysis annually to determine if PII is collected by any of the System Name components. If PII is discovered, a Privacy Impact Assessment is performed. The Privacy Impact Assessment template used by Enter CSP Name can be found in Section 3. This section constitutes the Privacy Threshold Analysis and findings.

* 1. QUALIFYING QUESTIONS

|  |  |
| --- | --- |
| Select One | 1. Does the <Information System Name> collect, maintain, or share PII in any identifiable form? |
| Select One | 1. Does the <Information System Name> collect, maintain, or share PII information from or about the public? |
| Select One | 1. Has a Privacy Impact Assessment ever been performed for the <Information System Name>? |
| Select One | 1. Is there a Privacy Act System of Records Notice (SORN) for this system? If Yes; the SORN identifier and name is: Enter SORN ID/Name. |

If answers to questions 1-4 are all “No” then a Privacy Impact Assessment may be omitted. If any of the answers to question 1-4 are “Yes” then complete a Privacy Impact Assessment.

* 1. DESIGNATION

Check one.

|  |  |
| --- | --- |
|  | A Privacy Sensitive System |
|  | Not a Privacy Sensitive System (in its current version) |

1. PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment has been conducted for the System Name on <Enter Date>.

* 1. PII MAPPING OF COMPONENTS

System Name consists of Enter Number key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by System Name and the functions that collect it are recorded in Table 2 - PII Mapped to Components.

Table 2 - PII Mapped to Components

| Components | Does this function 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. |

* 1. PII IN USE

Complete the following questions:

|  |  |  |
| --- | --- | --- |
| 1. What PII (name, social security number, date of birth, address, etc.) is contained in the CSP service offering? | | |
| Click here to enter text. | | |
| 1. Can individuals “opt-out” 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)? | | |
| *Click here to enter explanation.* | | |
|  | Yes | Explain the issues and circumstances of being able to opt-out (either for specific data elements or specific uses of the data): |
|  |  | *Click here to enter explanation.* |
|  | No | *Click here to enter explanation.* |

* 1. SOURCES OF PII AND PURPOSE

1. Does the CSP have knowledge of federal agencies that provide PII to the system?

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

1. Has any agency that is providing PII to the system provided a stated purpose for populating the system with PII?

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

1. Does the CSP populate the system with PII? If yes, what is the purpose?

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

1. What other third party sources will be providing PII to the system? Explain the PII that will be provided and the purpose for it.

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

* 1. ACCESS TO PII AND SHARING

1. What federal agencies have access to the PII, even if they are not the original provider? Who establishes the criteria for what PII can be shared?

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

1. What CSP personnel will have access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, other)? Explain the need for CSP personnel to have access to the PII.

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

1. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval?

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

1. 1Do other systems share, transmit, or have access to the PII in the system? If yes, explain the purpose for system to system transmission, access, or sharing.

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

* 1. PII SAFEGUARDS AND LIABILITIES

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

|  |
| --- |
| *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?

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

1. Does the CSP annual security training include privacy training? Does the CSP require contractors to take the training?

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

1. Who is responsible for assuring safeguards for the PII?

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

1. What is the magnitude of harm to the corporation if privacy related data is disclosed, intentionally or unintentionally?. Would the reputation of the corporation be affected?

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

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

|  |
| --- |
| *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?

|  |
| --- |
| *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?

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

* 1. 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 principle described in contracts with customers? Why or why not?

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

1. Do contracts with customers establish who has ownership rights over data including PII?

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

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

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

1. Do CSP contracts with customers establish record retention responsibilities for both the customer and the CSP?

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

1. Is the degree to which the CSP will accept liability for expose of PII clearly defined in agreements with customers?

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

* 1. ATTRIBUTES AND ACCURACY OF THE PII

1. Is the PII collected verified for accuracy? Why or why not?

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

1. Is the PII current? How is this determined?

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

* 1. MAINTENANCE AND ADMINISTRATIVE CONTROLS

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

|  |
| --- |
| *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?

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

1. Is the system using 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?

|  |
| --- |
| *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?

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

* 1. BUSINESS PROCESSES AND TECHNOLOGY

1. Does the conduct of this PIA result in circumstances that requires changes to business processes?

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

1. Does the completion of this PIA potentially result in technology changes?

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

* 1. PRIVACY POLICY

1. Is there a CSP privacy policy and is it provided to all individuals whose PII you collect, maintain or store?

*Click here to enter explanation.*

1. Is the privacy policy publicly viewable? If yes, provide the URL:

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

* 1. ASSESSOR AND SIGNATURES

This Privacy Impact Assessment has been conducted by <name of organization> and has been reviewed by the Enter 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. |

1. ACRONYMS

| Acronym | Definition |
| --- | --- |
| CSP | Cloud Service Provider |
| HIPAA | Health Insurance Portability and Accountability Act |
| IT | Information Technology |
| NIST | National Institute for Standards and Technology |
| OMB | Office of Management and Budget |
| POC | Point of Contact |
| PII | Personally Identifiable Information |
| PTA | Privacy Threshold Analysis |
| SORN | System of Records Notice |