State of California

California Department of Technology

Office of Information Security

# Privacy Threshold Assessment and Privacy Impact Assessments

SIMM Section 5310-C

November 2019

## REVISION HISTORY

| REVISION | DATE OF RELEASE | OWNER | SUMMARY OF CHANGES |
| --- | --- | --- | --- |
| Initial Release | November 2019 | Office of Information Security (OIS) |  |

Table of Contents

[Privacy Threshold Assessment and Privacy Impact Assessments 1](#_Toc23851126)

[REVISION HISTORY 2](#_Toc23851127)

[I. Introduction 1](#_Toc23851128)

[II. Privacy Coordinator Responsibilities 1](#_Toc23851129)

[III. Responsibilities of Information Owner and Others 1](#_Toc23851130)

[IV. Privacy Threshold Assessment and Privacy Impact Assessment Requirements 1](#_Toc23851131)

[V. Privacy Threshold Assessment and Privacy Impact Assessment Form 2](#_Toc23851132)

[VI. Definitions 2](#_Toc23851133)

[Privacy Threshold Assessment and Privacy Impact Assessment 2](#_Toc23851134)

[Privacy Threshold Assessment and Privacy Impact Assessment Form 2](#_Toc23851135)

[VII. Related Policies and Standards 2](#_Toc23851136)

[VIII. Sources 2](#_Toc23851137)

[IX. Privacy Threshold Assessment and Privacy Impact Assessment Form Template 3](#_Toc23851138)

[1 Project/Process/System/Program and Data/Information 3](#_Toc23851139)

[2 Project Contact Information 5](#_Toc23851140)

[3 Privacy Threshold Assessment 6](#_Toc23851141)

[4 Privacy Impact Assessment 8](#_Toc23851142)

[4.1 Privacy Program Administration 8](#_Toc23851143)

[4.2 Collection 12](#_Toc23851144)

[4.3 Use 15](#_Toc23851145)

[4.4 Maintenance and Storage 17](#_Toc23851146)

[4.5 Disclose/Share 19](#_Toc23851147)

[4.6 Distruction/Disposal 21](#_Toc23851148)

[5 Privacy Threshold / Impact Assessment Authorization and Acceptance 23](#_Toc23851149)

[6 Authority 23](#_Toc23851150)

[7 FIPS and NIST SP 800-53 Reference 24](#_Toc23851151)

[8 Related SIMM References 24](#_Toc23851152)

[9 Related Policies, Procedures and Standards 24](#_Toc23851153)

[10 Revision History 24](#_Toc23851154)

[11 Definitions of Key Terms 24](#_Toc23851155)

# Introduction

A Privacy Threshold Assessment (PTA) and a Privacy Impact Assessment (PIA) are part of the process for assessing the impact on individual privacy of state information assets and record systems that collect or maintain personal information, and for identifying the strategies to mitigate such impact. The purpose of the PTA and PIA process is to assist Information Owners, program managers and system owners with incorporating privacy protections into the development and management of state information assets and records.

# Privacy Coordinator Responsibilities

Agency Privacy Coordinators shall lead Information Owners, project managers and other key stakeholders in conducting and documenting the PIA process, in compliance with this Privacy Threshold Assessment and Privacy Impact Assessment Standard. Privacy Coordinators shall keep a record of PTAs and PIAs conducted to include the name of the system, process, project or program assessed, the date the assessment was completed, the names and contact information of the Privacy Coordinator and the Information Owner or project manager.

# Responsibilities of Information Owner and Others

Information Owners shall collaborate with the Privacy Coordinator in performing the assessment and documenting the PTA and PIA, in compliance with the requirements in this Standard. The Information Owner is responsible for ensuring implementation of the mitigation strategies identified in the process. Others with significant responsibilities for the information asset, such as project managers during the development or implementation stages and information security officers, shall also collaborate in the PTA and PIA process. In addition, legal counsel, information technology staff and others with related responsibilities shall provide information to the Privacy Coordinator as needed to conduct the PIA.

# Privacy Threshold Assessment and Privacy Impact Assessment Requirements

The requirements below apply to entities, as mandated in the State Administrative Manual (SAM) 5310.8 on PTA and PIA. Entities must conduct PTAs for all proposed and modified information systems (paper or electronic) and PIAs on information assets and records systems that collect or maintain personal information on individuals. The PIA process has two goals: 1) determine the privacy risks and effects of collecting, maintaining, using, and disclosing personal information; and 2) evaluate protections and alternative processes for handling personal information to eliminate or mitigate potential privacy risks.

A PTA is the first step to determine if any personal information is being collected, used, maintained or shared within the system, process, project or programs being developed. If all answers to the PTA questions are “NO”, a PIA is not required. If any answers are “YES”, a PIA is required to be completed. A PIA should be reviewed and, if appropriate, updated whenever a system, process, project or program undergoes a major change in technology or in business practices. The PIA analysis is organized to align with the Fair Information Practice.

Principles, which form the basis of most privacy laws, including the Information Practices Act. These Principles express the rights of individuals to control their personal information and the obligation of organizations to respect those rights. The Principles are Transparency, Purpose Specification, Collection Limitation, Use Limitation, Individual Participation, Data Quality, Security, and Accountability.

# Privacy Threshold Assessment and Privacy Impact Assessment Form

The PTA and PIA Form is one document that contains both the PTA and PIA. This form is to be used to report the comprehensive assessment of privacy risks and the identification of related mitigations. As part of the California Department of Technology Project Approval Lifecycle process, a PTA and PIA form should be completed for any new system, process, project, program, or technology that collects, uses, maintains or shares personally identifiable information and for major changes to such systems, processes, programs, or technologies.

A template for the Privacy Threshold Assessment and Privacy Impact Assessment form is provided with this SIMM.

# Definitions

Privacy Threshold Assessment and Privacy Impact Assessment – The process of assessing the impact on individual privacy of state information assets and record systems that collect or maintain personal information, and for identifying strategies for eliminating or mitigating the risks. Such an assessment shall comply with the Privacy Threshold Assessment and Privacy Impact Assessment Standard.

Privacy Threshold Assessment and Privacy Impact Assessment Form – A tool for use by agency Privacy Coordinators to conduct a comprehensive privacy threshold assessment and privacy impact assessment.

# Related Policies and Standards

* SAM 5310 Privacy
* SAM 5310.8 Privacy Threshold and Privacy Impact Assessments
* SAM 5315.1 System and Services Acquisition
* SAM 5315.2 System Development Lifecycle

# Sources

Source lists can be found in SAM 5310 Privacy Policy and in the Department of Homeland Security, Guidance on Privacy Impact Assessments, dated March 2017.

# Privacy Threshold Assessment and Privacy Impact Assessment Form Template

In accordance with state and federal policy, regulations and mandates, the [State Entity] conducts Privacy Impact Assessments (PIAs) on systems, business processes, projects and programs that involve the collection, creation, maintenance, distribution or disposal of personal information as defined in [Civil Code section 1798.3](http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=2.). The objective of a PIA is to identify privacy risks and protections throughout the life cycle of personal information collected to support business processes. PIAs are also conducted to ensure that programs or information systems that contain or use personal information comply with legal, regulatory, and policy requirements regarding privacy.

To fulfill the commitment to protect personal data, the following requirements must be met:

* The collection and use of the information must be both relevant and necessary for the stated purpose.
* The collection of only the minimum necessary for the state purposed.
* Information collected for a particular purpose must not be used for another purpose without the data subject’s consent unless such other uses are specifically authorized or mandated by law.
* Information collected must be sufficiently accurate, relevant, timely, and complete to ensure the individual’s privacy rights. Processes must be in place for the rectification of inaccurate or incorrect personal information.

The purpose of this PIA is to document the privacy risks and controls in place to protect the personally identifiable information being collected, used, maintained, stored and disposed within [State Entity] [Name of business process, system development projects, Name of program/programs, or other activity].

The PIA is typically completed by the information asset owner, assisted by and in collaboration the [State Entity] Privacy Coordinator and/or Information Security Officer, as well as information asset custodians.

Please send an electronic copy of the completed assessment to <Security@state.ca.gov>.

Questions or guidance about completing this document should be directed to the <Information Security Officer (ISO) or Privacy Coordinator> at <Security@state.ca.gov> or call <(916) 445-5239>.

# Project/Process/System/Program and Data/Information

| **Questions** | **Answers** |
| --- | --- |
| **New Project Name:** | <insert new project name here> |
| **Brief description of the project/process/system/program (if a project include the system and business process(es) being developed within the scope of the project).** | <insert brief description here> |
| **Data Classification:**  **(per SIMM 5305-A)**  **\*please check all that apply** | Confidential  Sensitive  Public |
| **Security Categorization (NIST 800-53)**  **(per FIPS 199)**  **\*select only one** | High  Medium  Low |
| **Has a system security plan been completed for the project?** | Yes  No  N/A  If N/A is selected, please provide an explanation  <Insert explanation here> |

# Project Contact Information

| **Privacy Officer/Privacy Coordinator** | **Fillable Information** |
| --- | --- |
| **Name** | **<Insert Privacy Officer / Privacy Coordinator Name>** |
| **Title** | **<Insert Privacy Officer / Privacy Coordinator Title>** |
| **Contact Number** | **<Insert Privacy Officer / Privacy Coordinator Contact Number>** |
| **E-mail Address** | **<Insert Privacy Officer / Privacy Coordinator E-mail Address>** |
| **Organization Unit/Office** | **<Insert Privacy Officer / Privacy Coordinator Organization Unit / Office>** |

| **Data Owner** | **Fillable Information** |
| --- | --- |
| **Name** | **<Data Owner Name>** |
| **Contact Number** | **<Data Owner Contact Number>** |
| **E-mail Address** | **<Data Owner E-mail Address>** |
| **Organization Unit/Office** | **<Data Owner Organization Unit / Office>** |

**ata On**

| **Business Process Owner** | **Fillable Information** |
| --- | --- |
| **Name** | **<Business Process Owner Name>** |
| **Contact Number** | **<Business Process Owner Contact Number>** |
| **E-mail Address** | **<Business Process Owner E-mail Address>** |
| **Organization Unit/Office** | **<Business Process Owner Organization Unit / Office>** |

| **IT Manager/Data Custodian** | **Fillable Information** |
| --- | --- |
| **Name** | **<IT Manager / Data Custodian Name>** |
| **Contact Number** | **<IT Manager / Data Custodian Contact Number>** |
| **E-mail Address** | **<IT Manager / Data Custodian E-mail Address>** |
| **Organization Unit/Office** | **<IT Manager / Data Custodian Organization Unit / Office>** |

| **Project Manager** | **Fillable Information** |
| --- | --- |
| **Name** | **<Project Manager Name>** |
| **Contact Number** | **<Project Manager Contact Number>** |
| **E-mail Address** | **<Project Manager E-mail Address>** |
| **Project Name** | **<Project Manager Project Name>** |

# Privacy Threshold Assessment

The Privacy Threshold Assessment (PTA) enables the respondent to assess at a very high level what personal identifiable information (PII) may be collected, used, maintained or shared within the process or system being developed. This may also be referred to as a PII data inventory.

It also assists System Owners and respondents in determining whether a full Privacy Impact Assessment needs to be completed.

| **Will the system collect, use, maintained or shared any of the following types of personally identifiable information as it relates to an individual?** | **Yes** | **No** |
| --- | --- | --- |
| Name, Former Name, or Alias |  |  |
| Date of Birth |  |  |
| Social Security Number (SSN) |  |  |
| Truncated SSN |  |  |
| Driver’s License Number or State Identification Card Number |  |  |
| Financial Data (e.g. account number or credit/debit card numbers, etc.) |  |  |
| Health Insurance Information (e.g. including policy number, subscriber identifier, medical ID, or any information in an individual’s application or claims history, including appeals records, etc.) |  |  |
| Medical Information (e.g. medical history, mental and physical condition, or medical treatment or diagnosis, etc.) |  |  |
| User Name/ID, email address, password or security question and answer |  |  |
| Physical Description (including height, weight, etc. please specify) |  |  |
| Biometric Data (e.g. fingerprints, iris scans, DNA, photographic facial images etc.) |  |  |
| Education History |  |  |
| Employment History |  |  |
| Criminal History |  |  |
| Information or data collected through the use or operation of the automated license plate recognition system |  |  |
| Other personal information (e.g. home address, email address, mother’s maiden name, home phone number, personal cell phone number, place of birth, etc.). Specify: <specify here> |  |  |

*STOP 
If ALL of the answers above are “NO”, proceed to the signature authorization page at the end of this document, and sign the document. You are done!

If ANY of the answers above are “YES”, proceed to the next page and complete the Privacy Impact Assessment.
*

**If ALL of the answers above are “NO”, proceed to the signature authorization page at the end of this document, and sign the document. You are done!**

**If ANY of the answers above are “YES”, proceed to the next page and complete the Privacy Impact Assessment.**

# Privacy Impact Assessment

The Privacy Impact Assessment will consist of questions in six sections that include: Privacy Program Administration, Collection, Use, Maintenance and Storage, Disclose/share and Destruction/Disposal. Each section will include questions to be completed. At the end of each section will be an analysis that is related to each section that will identify and address privacy risks, mitigations and if needed a correction plan.

There may be multiple privacy risks identified in each section; each of these risks must be identified and documented.

## Privacy Program Administration

| Number | Questions | NIST Reference |
| --- | --- | --- |
| 4.1.1 | Does the organization document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, use, maintenance, sharing, storing, transmitting, and disposal of personally identifiable information (PII)?  Yes No | AR-2 |
| 4.1.2 | Will contractors or service providers have access to PII?  Yes  No – ***If “NO”, skip to question #4.1.5*** | AR-3 |
| 4.1.3 | Describe the privacy roles, responsibilities, and access requirements for contractors and service providers.  <insert response here> | AR-3 |
| 4.1.4 | Are the privacy requirements included in contracts and other acquisition-related documents?  Yes  No  **🛈*Tip:*** *Refer to SAM 5305.8 for guidance.* | AR-3 |
| 4.1.5 | Describe how individuals who have access to PII are trained to appropriately handle the PII.  <insert response here> | AR-5 |
| 4.1.6 | Each project or program may offer training specific to the project or program, which touches on information handling procedures and sensitivity of information. Please describe what controls are in place to ensure that users of the system have completed training relevant to the project or program.  <insert response here> | AR-5 |
| 4.1.7 | Does your organization issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information?  Yes  No  If “YES”, please describe: <insert response here> | DI-1 |
| 4.1.8 | Does the organization provide a means for individuals to authorize collection, use, maintenance, and sharing of PII prior to its collection?  Collection:  Yes  No  Use:  Yes  No  Maintenance:  Yes  No  Sharing:  Yes  No  If “YES”, please describe all applicable means:  <insert response here> | IP-1 |
| 4.1.9 | Describe any procedures your organization has in place that allow an individual access to information collected by the project/process/system/program and/or to an accounting of disclosures of that information.  These procedures should include the entity’s privacy practices. If the Information Practices Act, Civil Code Section 1798 et seq. does not apply, state why this is the case and what procedures and/or regulations are in place that cover an individual gaining access to his/her own information. If additional mechanisms exist, include those in this section.  For example, if your organization has a customer satisfaction unit, list the unit name, phone and email contact information in this section in addition to the entity’s procedures.  <insert response here> | IP-2 |
| 4.1.10 | Describe the procedures for individuals to address possibly inaccurate or erroneous information. If the correction procedures are the same as those given in question above, state as much. If the system has been exempted from the provisions of the IPA, explain why individuals may not access their records.  <insert response here> | IP-3 |
| 4.1.11 | Does your agency require notice to affected individuals when their personal information is requested, sold, or released to third parties?  Yes  No  If no, explain  <insert response here> | TR-1 |
| 4.1.12 | Are the agency privacy practices publicly available through the organizational website?  Yes  No  If no, explain <insert response here> | TR-3 |
| 4.1.13 | Is the privacy incident response plan incorporated into your agency Incident Response Plan?  Yes  No  If no, explain why not and describe where it is located  <insert response here> | SE-2 |
| 4.1.14 | Does your organization’s online privacy notice or statement to the public and individuals include:   * its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII);  Yes  No * authority for collecting PII;  Yes  No * the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices;  Yes  No * the ability to access and have PII amended or corrected if necessary. Yes  No | TR-1 |
| 4.1.15 | Does the organization evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized?  Yes  No  If “YES”, provide a brief description  <insert brief description here> | UL-2 |
| 4.1.16 | Does the privacy notice provide appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII?  Yes  No  Provide copies of the applicable privacy notices. | IP-1 |
| 4.1.17 | This portion of the PIA is for details about information provided in this Privacy Program Administration section. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  **Privacy Risk**:  <insert response here>  **Mitigation:**  <insert response here>  **Correction Action Plan, if necessary**:  <insert response here> | N/A |

## Collection

The following section pertains to the collection of personally identifiable information by the [State Entity].

| Number | Questions | NIST Reference |
| --- | --- | --- |
| 4.2.1 | List all statutory and regulatory authority to collect the personally identifiable information (PII) listed in the Privacy Threshold Assessment.  ***🛈Tip:*** *Explain how the statutory and regulatory authority permits collection, use, maintenance and sharing of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of this Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the collection of the subject information.*  <insert response here> | AP-1 |
| 4.2.2 | If the system collects Social Security Numbers, identify the specific authority allowing such collection. If you are relying on another federal or state agency, please list their legal authorities.  ***🛈Tip:*** *Reference for items # 5.2.2, 5.2.3 and 5.2.5 IPA refers to Information Practices Act-Civil Code Section 1798.*   * *#5.2.2 SAM: 5310, 5305.8 NIST 800-53: AP-1, UL-2 Civil Code Section 1798.85, 1798.86, 1798.89* * *#5.2.3 - NIST 800-53 UL-2* * *#5.2.5 - SAM 5310.1, SIMM 5310-A, SAM 5305.8, NIST 800-53 AP-2, TR-1, TR-2; Civil Code Section 1798.17*   <insert response here> | AP-1 |
| 4.2.3 | If PII is received from another governmental agency/entity pursuant to an agreement, cite the agreement and where it can be found.  <insert response here> | UL-2 |
| 4.2.4 | What is the purpose(s) for which PII is collected, used, maintained?  <insert response here> | AP-2 |
| 4.2.5 | Is the purpose stated above also stated in your ‘notice on collection’?  Yes  No  ***🛈Tip:*** *‘notice on collection’ means clearly communicating to individuals the purpose of collecting their personal information. See SIMM 5310-A.* | TR-1 |
| 4.2.6 | Is the reason information is being collected displayed in clear, simple language that can be easily understood by the data subject?  Yes  No | AP-2 |
| 4.2.7 | Does this project/process/system/program collect PII directly from the individual to the greatest extent possible?  Yes  No  Please identify the sources from which the information may be collected?  Individuals  Another Entity  Business Partner/Vendors  Internally – please describe: <describe here>  Other – please specify: <specify here> | DI-1 |
| 4.2.8 | How will PII be collected? (Format collected – please check all applicable items)  Paper  Electronically  Verbally  Other – please specify: <specify here> | DI-1 |
| 4.2.9 | Are Social Security Numbers extracted from any other source (e.g. an SSN match is made and extracted via other information provided by the claimant, employer, or provider, or verified with SSA, etc.)?  Yes  No  If yes, describe the source:  <insert response here>  ***🛈Tip:*** *References for items 5.2.9 – 5.2.11 SAM 5305.8, NIST 800-53: #5.2.9, #5.2.10 and #5.2.11, Civil Code Section 1798.15 and 1798.16* | UL-2 |
| 4.2.10 | Does the system use information from commercial sources or publicly available data?  Yes  No  If yes, explain why and how this information is used? Also indicate whether the commercial or public source data is marked within the system.  **🛈*Tip:*** *Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, the commercial data is used to verify information already provided by or about the individual.*  <insert explanation here> | UL-2 |
| 4.2.11 | If the system receives information from another system, such as a response to a background check, describe the system from which the information originates, including what information is returned and how it is used.  **System Name:** <insert response here>  **Data elements:** <insert response here>  **How the information is used:** <insert response here>  **Name of the entity:** <insert response here>  **Original source or data owner of the date:** <insert response here> | DI-1  UL-2 |
| 4.2.12 | Does the organization identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose of collection?  Yes  No | DM-1 |

| Number | **Analysis: Collection** |
| --- | --- |
| 4.2.13 | **Analysis: Related to Collection**  This portion of the PIA is to provide details about information related to PII collection. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  **Privacy Risk**:  <insert response here>  **Mitigation:**  <insert response here>  **Correction Action Plan, if necessary**:  <insert response here> |

## Use

The following information relates to how the use of personally identifiable information is controlled and managed within the state entity.

| Number | Questions | NIST Reference |
| --- | --- | --- |
| 4.3.1 | Who is authorized to receive and have access to the PII within the project/system?  **🛈*Tip:*** *Describe the different roles in general terms that have been created to provide access to the information. For example, certain users may have “read-only” access while others may be permitted to make certain amendments or changes to the information.*  <insert response here> | DI-1 |
| 4.3.2 | Is the use of the PII collected limited to the stated purpose for which the individual has provided consent?  Yes  No  If “NO”, please provide further information  <insert response here> | DM-1 |
| 4.3.3 | Will PII be used in testing, training, and or research? Yes  No  If yes, please describe:  <insert response here> | DM-3 |
| 4.3.4 | Are there policies and/or procedures to minimize the use of PII in testing, training, and/or research?  Yes  No  If “YES”, please describe:  <insert response here> | DM-3 |
| 4.3.5 | If PII is used in testing, training and research, what controls will be implemented to protect PII?  <insert response here> | DM-3 |
| 4.3.6 | Is use of PII internally only for the authorized purpose(s) identified in privacy policy or notice on collection?  Yes  No | UL-1 |
| 4.3.7 | What other entities can access the data in this system? What law or statutes authorize the access?  <insert response here> | UL-2  AP-1 |
| 4.3.8 | Describe how the organization will monitor and audit privacy controls for this project/process/system.  Do the audit measures discussed above include the ability to identify specific records each user can access?  Describe the different roles in general terms that have been created to provide access to the project information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.  Example: If certain celebrity records are accessed, a supervisor is notified and reviews to ensure that the records were properly used.  <insert response here> | AR-4 |
| 4.3.9 | Explain whether the project conducts self-audits, or third party independent audits, or reviews by other entities.  <insert response here> | AR-4 |

| Number | **Analysis: Use** |
| --- | --- |
| 4.3.10 | **Analysis: Related to Use**  This portion of the PIA is to provide details about information related to PII use. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  **Privacy Risk:**  <insert response here>  **Mitigation:**  <insert response here>  **Correction Action Plan, if necessary:**  <insert response here> |

## Maintenance and Storage

Please describe below how the state entity controls the maintenance and storage of personally identifiable information.

| Number | Questions and fillable Answers | NIST Reference |
| --- | --- | --- |
| 4.4.1 | Where will PII be stored? Check all applicable items below:  Cloud  Local Drive  Shared Drive  System/Database  Physical paper filed – please specify location:  <If physical paper filed was selected above- please specify location here> | SE-1 |
| 4.4.2 | Explain how the project checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems? How often?  The project or program does not utilize the inaccurate or outdate PII. It merely identifies to the state entity that it is visible when it should not be visible since it should be encrypted. <insert response here>  <insert response here> | DI-1 |
| 4.4.3 | Describe the process used for checking accuracy. If a commercial data aggregator is involved, describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in Research & Development, inaccurate information may not have an impact on the individual or the system. If the system or program does not check for accuracy, please explain why.  <insert response here> | DI-1 |
| 4.4.4 | Describe any technical solutions, policies, or procedures focused on improving personally identifiable information accuracy and integrity within the system/project/process or program.  **🛈*Tip:*** *Example: The system may check the information provided by the individual against any other source of information (within or outside your organization) before the project uses the information to make a decision about an individual.*  <insert response here> | DI-2 |
| 4.4.5 | How long will the information be stored?  ***🛈Tip:*** *Example: The project manager, in consultation with the legal counsel and the component records management officer, must develop a records retention schedule, early in the development process, for the records contained in the system that considers the minimum amount of time necessary to retain information while meeting the needs of the program. Consult with your records management office for assistance with this question if necessary.*  <insert response here> | DM-2  SAM 5310.6 and Civil Code Section:1798.18 |
| 4.4.6 | Is all the information the project/process/system/program collects retained? Is there a specific sub set of information retained?  ***🛈Tip:*** *Example: A project may collect extensive PII initially for the purpose of verifying the identity of an individual for a background check. Upon completion of the background check, the project will maintain the new information, the results of the background check (approved/not approved) and delete all application information.*  *In some cases, the entity may choose to retain files in active status and archive them after a certain period of time. Provide active file retention periods as well as archived records, in number of years. Discuss when the time periods begin for inputs, outputs, and master files.*  *Note: all projects may not require the creation of a new retention schedule. Refer to California Government Code, Title 2, Division 3, part 5/5, Chapter 5, State Records (14740-14769) for requirements.*  <insert response here> | DM-2  SAM 5310.6 and Civil Code Section: 1798.18 |

| Number | Analysis: Maintenance and Storage |
| --- | --- |
| 4.4.7 | Analysis: Related to Maintenance and Storage  This portion of the PIA is to provide details about information related to PII maintenance and storage. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  🛈*Tip: Discuss the risks associated with the length of time personally identifiable information is maintained and stored. How were those risks mitigated?*  *Although establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of California Government Code, Title 2, Division 3, Part 5.5, Chapter 5, State Records (14740 – 14769) to keep the minimum amount of PII for the minimum amount of time. The schedule should align with the stated purpose and mission of the system.*  *Consider the following to assist in providing a response:*   * *Does the project retain only the PII necessary for its purposed and only for as long as necessary and relevant to fulfill the specified purposes?* * *Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*   Privacy Risk:  <insert response here>  Mitigation:  <insert response here>  Correction Action Plan, if necessary:  <insert response here> |

## Disclose/Share

In the following section, describe whether the state entity discloses or shares the personally identifiable information under its purview with other entities.

| Number | Questions and Fillable Answers | NIST Reference |
| --- | --- | --- |
| 4.5.1 | Does the project maintain an accurate accounting/record of disclosure of information held in the system?  Yes  No  Who is responsible for these the ***accounting of disclosures***?  **Title:** [Insert title her - Mandatory]  **Name:** [Insert Name - Optional] | AR-8 |
| 4.5.2 | What is the retention period for the record of disclosure of PII mentioned above?  <insert response here> | AR-8 |
| 4.5.3 | Is the disclosure of the PII collected limited to the stated purpose and for which the individual has provided consent?  <insert response here> | DM-1 |
| 4.5.4 | Discuss the sharing of state information between agencies and departments. Identify and list the State entities with which the information is shared.  **🛈*Tip:*** *Example: Certain systems regularly share information because of the crossover of the different parts of the State*.  <insert response here> | NIST 800-53 UL-2 and Civil Code Section: 1798.24 and 1798.25 |
| 4.5.5 | The following questions are intended to describe the scope of the project/system/process/program information sharing external to the entity. External sharing encompasses sharing with other federal, state and local government and private sector entities.  Is information shared outside of the State as part of normal agency operations? If so, identify the federal, local agencies or privacy sector entities and how the information is accessed and how it is to be used.  <insert response here> | NIST 800-53 UL-2 and Civil Code Section: 1798.24 and 1798.25 |
| 4.5.6 | Does the project share PII with parties external to the state entity only for the authorized purposes identified in the privacy policy or notice on collection?  Yes  No  If response is “NO”, please explain  <insert response here> | UL-2 |
| 4.5.7 | If the organization shares PII collected within this project/system/process/program with external entities please describe how that sharing occurs:   * Are Memoranda of Understanding, Inter-Agency Agreement, Letters of Intent, or similar agreements executed? * Is the PII specifically identified? * Are the purposes for which it will be used detailed? * Does the agreement (in whatever form) detail the responsibilities of the third parties to protect and secure the PII? * Does the agreement require formal acknowledgement (i.e., signature of authority, etc.)?   Yes  No  If response is “YES” to any of the above, please describe:  <insert response here> | UL-2  AR-3 |

| Number | **Analysis: Disclose/Share** |
| --- | --- |
| 4.5.8 | Analysis: Related to Information Disclosure and Sharing  This portion of the PIA is to provide details about information related to PII disclosure and sharing. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  **Privacy Risk:**  <insert privacy risks here>  **Mitigation:**  <insert mitigation here>  **Correction Action Plan, if necessary:**  <insert correction action plan, if necessary here> |

## Distruction/Disposal

Describe below how the state entity manages the destruction and/or disposal of personally identifiable information.

| Number | Questions and Fillable Answers | NIST Reference |
| --- | --- | --- |
| 4.6.1 | How will information be disposed of (e.g. place in confidential bin or done by contractor, or electronically wiped/erased)?  <insert response here> | DM-2 |
| 4.6.2 | What method does the organization use for secure deletion / destruction of PII?  <insert response here> | DM-2 |
| 4.6.3 | Does entity formally validate secure destruction /disposal of PII?  Yes No | DM-2 |

| Number | **Analysis: Destruction/Disposal** |
| --- | --- |
| 4.6.4 | Analysis: Related to Destruction/Disposal  This portion of the PIA is to provide details about information related to PII destruction and/or disposal. Identify privacy risks, remediation strategies and if necessary provide a corrective action plan.  **Privacy Risk:**  <identify privacy risks here>  **Mitigation:**  <insert mitigation here>  **Correction Action Plan, if necessary:**  <insert correction action plan, if necessary here> |

# Privacy Threshold / Impact Assessment Authorization and Acceptance

I have authorized, reviewed and understand the results of the Privacy Threshold / Privacy Impact Assessment for the <(Project Name/System Name/Business Process Name/Program Name)>.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Deputy Director / Data Owner> Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Business Process Owner> Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Chief Information Officer/ IT Manager> Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Privacy Officer /Privacy Coordinator> Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

<Information Security Officer> Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Print Name

# Authority

This PTA/PIA template supports compliance with the State of California Government Code Section [11549.3](http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=GOV&sectionNum=11549.3.) , SAM Sections 5310 through 5310.8, and SIMM Sections 5310-A through SIMM Section 5310-C

.

# FIPS and NIST SP 800-53 Reference

| Family | Control |
| --- | --- |
| Planning (PL) | PL-04 |
| Awareness and Training (AT) | AT-01, AT-02, AT-03, AT-04 |
| Media Protection (MP) | MP-01 |
| Personnel Security (PS) | PS-01, PS-02, PS-06, PS-08 |
| Access Control (AC) | AC-20 |
| Appendix J: Privacy Control Catalog | AP-1, AP-2, AR-2, AR-3, AR-4, AR-5, AR-8, DI-1, DI-2, DM-1, DM-2, DM-3, IP-1, IP-2, IP-3, SE-1, SE-2, TR-1, TR-3, UL-1, UL-2 |
| FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems | [NIST Computer Security Resource Center](https://csrc.nist.gov/Publications/Search?requestSeriesList=3&requestStatusList=1,3&requestDisplayOption=brief&requestSortOrder=5&itemsPerPage=All) |

# Related SIMM References

| Reference | Article |
| --- | --- |
| 5310-A | Privacy Policy Statement and Notice on Collection |
| 5310-B | Individual Access |

# Related Policies, Procedures and Standards

| Reference | Article |
| --- | --- |
|  | Incident Response Policy |
|  | Risk Management Policy |
|  | Security Variance Policy |
|  | Security Variance Process |

# Revision History

| **Date** | **Description of Change** | **Reviewer** |
| --- | --- | --- |
| <Insert Date> | <Insert Description> | <Insert Reviewer> |

# Definitions of Key Terms

[State Entity] uses the information security and privacy definitions issued by the California Department of Technology Office of Information Security in implementing information security and privacy policy. Terms and definitions are defined here and are also on the California Department of Technology website at <https://cdt.ca.gov/security/technical-definitions/>.

| **Key Term** | **Definition** |
| --- | --- |
| Commercial data | Commercial data includes information from data aggregators where the information was originally collected by the private organization for non-governmental purposes, such as marketing or credit reporting. |
| Publicly available data | Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator. |