| **Title** | 5310-C Privacy Threshold Assessments and Privacy Impact Assessments |
| --- | --- |
| **Owner** | Office of Information Security – Privacy Program |
| **Publish Date** | September 2019 |
| **Last Review Date** | July 2024  |

# Purpose

A Privacy Threshold Assessment (PTA) and a Privacy Impact Assessment (PIA) are part of assessing the impact on individual privacy of state information assets and record systems that collect or maintain personal information and 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 in incorporating privacy protections into developing and managing state information assets and records. The PIA analysis is organized to align with the Fair Information Practices. [Click here to move to the form.](#_dnvy7k7u7xjw)

The Information Practices Act is based on principles that express individuals' rights to control their personal information and organizations' obligations to respect those rights. The principles are Transparency, Purpose Specification, Collection Limitation, Use Limitation, Individual Participation, Data Quality, Security, and Accountability.

# Scope

The requirements herein apply to all entities as mandated in the State Administrative Manual (SAM) 5310.8 Privacy Threshold and Privacy Impact Assessments.

# Compliance

Government Code (GC) Section 11549.3 empowers the Office of Information Security (OIS) to create, issue, and maintain policies, standards, and procedures; oversee information security risk management for agencies and state entities; provide information security and privacy guidance; and ensure compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

Entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, and standards governing their agency or entity. Full compliance is expected.

# Responsibilities

## Privacy Coordinator Responsibilities

Agency and entity privacy coordinators shall lead information owners, project managers, and other key stakeholders in conducting and documenting the PIA process in compliance with this standard.

Privacy Coordinators shall keep a record of PTAs and PIAs conducted.

Records should include:

* Name of the system, process, project, or program assessed
* Date the assessment was completed
* Name and contact information of the privacy coordinator
* Name and contact information for the information owner or project manager

## Information Owner Responsibilities

Information owners shall collaborate with the privacy coordinator to perform the assessment and document the PTA and PIA in compliance with this standard's requirements.

The information owner is responsible for ensuring the implementation of the mitigation strategies identified in the process.

## Additional Stakeholder Responsibilities

Key stakeholders, such as project managers and information security officers, may also collaborate in the PTA and PIA process. Legal counsel, IT staff, and others with related responsibilities should provide information as needed for the PIA.

# PTA and PIA Requirements

Entities must conduct PTAs for all proposed and modified information systems, paper or electronic. PIAs are required for information assets and records systems that collect or maintain personal information on individuals.

## PTAs

 A PTA is the first step in determining whether personal information is being collected, used, maintained, or shared within the system, process, project, or program under development. If all answers to the PTA questions are “NO,” a PIA is not required.

If any answers are “YES,” a PIA must be completed.

## PIAs

A PIA should be reviewed and updated whenever a system, process, project, or program undergoes a major change in technology or business practices. The PIA process has two goals:

1. Determine the privacy risks and effects of collecting, maintaining, using, and disclosing personal information.
2. Evaluate protections and alternative processes for handling personal information to eliminate or mitigate potential privacy risks.

# PTA and PIA Form

The PTA and PIA Form is one document that contains both the PTA and PIA. This form will 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.

The Privacy Threshold Assessment and Privacy Impact Assessment Form is provided with this standard.

# Definitions

* **Privacy** - The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.
* **Privacy Threshold Assessment (PTA)** – A preliminary assessment to determine whether a system, project, or data collection initiative involves PII. The assessment identifies if further analysis, such as a Privacy Impact Assessment, is necessary.
* **Privacy Impact Assessment (PIA)** - An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

# References

* [SAM 5310](https://www.dgs.ca.gov/en/Resources/SAM/TOC/5300/5310) - Privacy
* [SAM 5310.8](https://www.dgs.ca.gov/Resources/SAM/TOC/5300/5310-8) - Privacy Threshold and Privacy Impact Assessments
* [SAM 5315.1](https://www.dgs.ca.gov/Resources/SAM/TOC/5300/5315-1) - System and Services Acquisition
* [SAM 5315.2](https://www.dgs.ca.gov/Resources/SAM/TOC/5300/5315-2) - System Development Lifecycle
* [SIMM 5300](https://cdt.ca.gov/policy/simm/#5300)
* <https://www.dhs.gov/privacy-impact-assessments> - Department of Homeland Security, guidance on Privacy Impact Assessments

# Questions

Questions regarding this requirement may be sent to:

California Department of Technology
Office of Information Security
Security@state.ca.gov

# Revision History

| **Version** | **Date** | **Owner** | **Change Summary** |
| --- | --- | --- | --- |
| v.1 | September 2019 | Office of Information Security (OIS) | Initial Release |
| v.2 | June 2022 | OIS | Minor update to include NIST 800-53 |
| v.3 | September 2022 | OIS | Minor update to correct 4.2 Tip Information |
| v.4 | June 2024 | OIS | Update to layout, addition of GenAI and CSF 2.0 alignment |

Privacy Threshold Assessment and Privacy Impact Assessment Form

# Purpose

In accordance with state and federal policy, regulations, and mandates, state entities must conduct Privacy Threshold Assessments (PTA) and Privacy Impact Assessments (PIA) 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.

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

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 data for the stated purpose.
* 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 accurate, relevant, timely, and complete to ensure the individual’s privacy rights. Processes must be in place to rectify inaccurate or incorrect personal information.

# Completion

This form is typically completed by the information asset owner in collaboration with the state entity privacy coordinator and/or information security officer and information asset custodians. A PTA and, when applicable, a PIA must be completed for all new programs and projects and whenever a change to an existing program, project, or system occurs. For projects, this usually occurs during the Project Approval Lifecycle (PAL) Stage 2.

Once completed, submit this form to the project information security officer (ISO) or privacy coordinator.

## Instructions

1. Answer all questions in the form.
2. Text surrounded by brackets must be deleted and replaced with the appropriate text.
	1. Ex: [insert response here]
	2. The form is restricted, so text can only be entered where appropriate.
3. A stop sign indicates the end of the PTA. If all the answers to the previous questions are “no,” proceed to the signature authorization page and complete the document.
4. If any answer is yes, a PIA is required. Complete the rest of the form.

If you have questions or need guidance about completing this document, please contact the Information Security Officer (ISO) or Privacy Coordinator.

# Form Questions

1. **Project/Process/System/Program and Data/Information**

| **Questions**  | **Answers**  |
| --- | --- |
| **New Project Name:**  | {Q1\_1} |
| **Brief description of the project/process/system/program (if a project includes the system and business process(es) being developed within the scope of the project).**  | {Q1\_2} |
| **Data Classification:** **(Per SIMM 5305-A)** **\* Check all that apply**  | {#Q1\_3\_Confidential}☒{/}{^Q1\_3\_Confidential}☐{/} Confidential{#Q1\_3\_Sensitive}☒{/}{^Q1\_3\_Sensitive}☐{/} Sensitive{#Q1\_3\_Public}☒{/}{^Q1\_3\_Public}☐{/} Public |
| **Security Categorization (NIST 800-53)** **(Per FIPS 199)** **\*Select only one**  | {#Q1\_4\_High}☒{/}{^Q1\_4\_High}☐{/} High{#Q1\_4\_Moderate}☒{/}{^Q1\_4\_Moderate}☐{/} Moderate{#Q1\_4\_Low}☒{/}{^Q1\_4\_Low}☐{/} Low |
| **Has a system security plan been completed for the project?**  | {#Q1\_5\_Yes}☒{/}{^Q1\_5\_Yes}☐{/} Yes{#Q1\_5\_No}☒{/}{^Q1\_5\_No}☐{/} No{#Q1\_5\_NA}☒{/}{^Q1\_5\_NA}☐{/} N/AIf No or N/A is selected, please explain why it is not completed and when it will be completed (e.g., before procurement).{Q1\_5\_explanation} |
| **Is there a Generative Artificial Intelligence (GenAI) component or byproduct to this project, regardless of whether it is intentional or incidental?**  | {#Q1\_6\_Yes}☒{/}{^Q1\_6\_Yes}☐{/} Yes{#Q1\_6\_No}☒{/}{^Q1\_6\_No}☐{/} NoIf “YES,” attach the completed mandatory GenAI Risk Assessment (SIMM 5305-F) and outcome of CDT consultation (for details, refer to Technology Letter 24-01 and 24-03).    |

1. **Project Contact Information**

| **Privacy Officer/Privacy Coordinator**  | **Fillable Information**  |
| --- | --- |
| **Name**  | {Q2\_1\_1} |
| **Title**  | {Q2\_1\_2} |
| **Contact Number**  | {Q2\_1\_3} |
| **E-mail Address**  | {Q2\_1\_4} |
| **Organization Unit/Office**  | {Q2\_1\_5} |

| **Data Owner**  | **Fillable Information**  |
| --- | --- |
| **Name**  | {Q2\_2\_1} |
| **Contact Number**  | {Q2\_2\_3} |
| **E-mail Address**  | {Q2\_2\_4} |
| **Organization Unit/Office**  | {Q2\_2\_5} |

| **Business Process Owner**  | **Fillable Information**  |
| --- | --- |
| **Name**  | {Q2\_3\_1} |
| **Contact Number**  | {Q2\_3\_3} |
| **E-mail Address**  | {Q2\_3\_4} |
| **Organization Unit/Office**  | {Q2\_3\_5} |

| **IT Manager/Data Custodian**  | **Fillable Information**  |
| --- | --- |
| **Name**  | {Q2\_4\_1} |
| **Contact Number**  | {Q2\_4\_3} |
| **E-mail Address**  | {Q2\_4\_4} |
| **Organization Unit/Office**  | {Q2\_4\_5} |

| **Project Manager**  | **Fillable Information**  |
| --- | --- |
| **Name**  | {Q2\_5\_1} |
| **Contact Number**  | {Q2\_5\_3} |
| **E-mail Address**  | {Q2\_5\_4} |
| **Project Name**  | {Q2\_5\_5} |

1. **Privacy** **Threshold Assessment**

The Privacy Threshold Assessment (PTA) enables the respondent to assess at a very high level what personally identifiable information (PII) may be collected, used, maintained, or shared within the developed process or system.  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, maintain, or share any of the following types of personally identifiable information as it relates to an individual?**  | **Yes** | **No** |
| --- | --- | --- |
| Name, Former Name, or Alias  | {#Q3\_1\_Yes}☒{/}{^Q3\_1\_Yes}☐{/} | {#Q3\_1\_No}☒{/}{^Q3\_1\_No}☐{/} |
| Date of Birth  | {#Q3\_2\_Yes}☒{/}{^Q3\_2\_Yes}☐{/} | {#Q3\_2\_No}☒{/}{^Q3\_2\_No}☐{/} |
| Social Security Number (SSN)  | {#Q3\_3\_Yes}☒{/}{^Q3\_3\_Yes}☐{/} | {#Q3\_3\_No}☒{/}{^Q3\_3\_No}☐{/} |
| Truncated SSN  | {#Q3\_4\_Yes}☒{/}{^Q3\_4\_Yes}☐{/} | {#Q3\_4\_No}☒{/}{^Q3\_4\_No}☐{/} |
| Driver’s License Number or State Identification Card Number  | {#Q3\_5\_Yes}☒{/}{^Q3\_5\_Yes}☐{/} | {#Q3\_5\_No}☒{/}{^Q3\_5\_No}☐{/} |
| Financial Data (e.g., account number, credit/debit card numbers, etc.)  | {#Q3\_6\_Yes}☒{/}{^Q3\_6\_Yes}☐{/} | {#Q3\_6\_No}☒{/}{^Q3\_6\_No}☐{/} |
| 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.)  | {#Q3\_7\_Yes}☒{/}{^Q3\_7\_Yes}☐{/} | {#Q3\_7\_No}☒{/}{^Q3\_7\_No}☐{/} |
| Medical Information (e.g., medical history, mental and physical condition, or medical treatment or diagnosis, etc.)  | {#Q3\_8\_Yes}☒{/}{^Q3\_8\_Yes}☐{/} | {#Q3\_8\_No}☒{/}{^Q3\_8\_No}☐{/} |
| Username/ID, email address, password, or security question and answer  | {#Q3\_9\_Yes}☒{/}{^Q3\_9\_Yes}☐{/} | {#Q3\_9\_No}☒{/}{^Q3\_9\_No}☐{/} |
| Physical Description (including height, weight, etc., please specify) {Q3\_10\_explanation} | {#Q3\_10\_Yes}☒{/}{^Q3\_10\_Yes}☐{/} | {#Q3\_10\_No}☒{/}{^Q3\_10\_No}☐{/} |
| Biometric Data (e.g., fingerprints, iris scans, DNA, photographic facial images, etc.)  | {#Q3\_11\_Yes}☒{/}{^Q3\_11\_Yes}☐{/} | {#Q3\_11\_No}☒{/}{^Q3\_11\_No}☐{/} |
| Education History  | {#Q3\_12\_Yes}☒{/}{^Q3\_12\_Yes}☐{/} | {#Q3\_12\_No}☒{/}{^Q3\_12\_No}☐{/} |
| Employment History  | {#Q3\_13\_Yes}☒{/}{^Q3\_13\_Yes}☐{/} | {#Q3\_13\_No}☒{/}{^Q3\_13\_No}☐{/} |
| Criminal History  | {#Q3\_14\_Yes}☒{/}{^Q3\_14\_Yes}☐{/} | {#Q3\_14\_No}☒{/}{^Q3\_14\_No}☐{/} |
| Information or data collected through the use or operation of the automated license plate recognition system  | {#Q3\_15\_Yes}☒{/}{^Q3\_15\_Yes}☐{/} | {#Q3\_15\_No}☒{/}{^Q3\_15\_No}☐{/} |
| Genetic Data  | {#Q3\_16\_Yes}☒{/}{^Q3\_16\_Yes}☐{/} | {#Q3\_16\_No}☒{/}{^Q3\_16\_No}☐{/} |
| Other personal information (e.g., home address, email address, mother’s maiden name, home phone number, personal cell phone number, place of birth, etc.).  {Q3\_17\_explanation} | {#Q3\_17\_Yes}☒{/}{^Q3\_17\_Yes}☐{/} | {#Q3\_17\_No}☒{/}{^Q3\_17\_No}☐{/} |



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

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

1. **Privacy Impact Assessment**

The Privacy Impact Assessment will consist of questions in six sections: Privacy Program Administration, Collection, Use, Maintenance and Storage, Disclose/Share, and Destruction/Disposal.

Each section includes questions to be completed. At the end of each section, an analysis related to that section will identify and address privacy risks, mitigations, and, if necessary, a correction plan.

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

* 1. **Privacy Program Administration**

| **No.** | **Questions** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 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)?** {#Q4\_1\_1\_Yes}☒{/}{^Q4\_1\_1\_Yes}☐{/} Yes{#Q4\_1\_1\_No}☒{/}{^Q4\_1\_1\_No}☐{/} No | RA-3, RA-8 | GV.PO-01 |
| 4.1.2 | **Will contractors or service providers have access to PII?** {#Q4\_1\_2\_Yes}☒{/}{^Q4\_1\_2\_Yes}☐{/} Yes{#Q4\_1\_2\_No}☒{/}{^Q4\_1\_2\_No}☐{/} No***If “NO,” skip to question #4.1.5***  | SA-1, SA-4, SA-9 | PR.AA-05 |
| 4.1.3 | **Describe the privacy roles, responsibilities, and access requirements for contractors and service providers.**{Q4\_1\_3} | SA-1, SA-4, SA-9, | GV.RR-02PR.AA-05 |
| 4.1.4 | **Are the privacy and GenAI disclosure notification requirements included in contracts and other acquisition-related documents?**{#Q4\_1\_4\_Yes}☒{/}{^Q4\_1\_4\_Yes}☐{/} Yes{#Q4\_1\_4\_No}☒{/}{^Q4\_1\_4\_No}☐{/} No***Tip****:  Refer to SAM 5305.8 and GenAI Guidance.*  | SA-1, SA-4, SA-9 | GV.SC-05 |
| 4.1.5 | **Describe how individuals who have access to PII are trained to handle the PII appropriately.**{Q4\_1\_5} | AT-1,AT-2,AT-3,PL-4 | PR.AT-02 |
| 4.1.6 | **Describe what controls are in place to ensure system users have completed training relevant to the project or program.*****Tip****: Each project or program may offer training specific to the project or program, including GenAI, which touches on information handling procedures and the sensitivity of information*.{Q4\_1\_6} | AT-1,AT-2,AT-3,PL-4 | PR.AT-02 |
| 4.1.7 | **Does your organization issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information?**{#Q4\_1\_7\_Yes}☒{/}{^Q4\_1\_7\_Yes}☐{/} Yes{#Q4\_1\_7\_No}☒{/}{^Q4\_1\_7\_No}☐{/} No**If “YES,” describe**:{Q4\_1\_7\_ex} | PM-22 SI-18 | GV.OC-03 |
| 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:** {#Q4\_1\_8\_collection\_Yes}☒{/}{^Q4\_1\_8\_collection\_Yes}☐{/} Yes{#Q4\_1\_8\_collection\_No}☒{/}{^Q4\_1\_8\_collection\_No}☐{/} No **Use**: {#Q4\_1\_8\_use\_Yes}☒{/}{^Q4\_1\_8\_use\_Yes}☐{/} Yes{#Q4\_1\_8\_use\_No}☒{/}{^Q4\_1\_8\_use\_No}☐{/} No **Maintenance:** {#Q4\_1\_8\_maintenance\_Yes}☒{/}{^Q4\_1\_8\_maintenance\_Yes}☐{/} Yes{#Q4\_1\_8\_maintenance\_No}☒{/}{^Q4\_1\_8\_maintenance\_No}☐{/} No **Sharing**: {#Q4\_1\_8\_sharing\_Yes}☒{/}{^Q4\_1\_8\_sharing\_Yes}☐{/} Yes{#Q4\_1\_8\_sharing\_No}☒{/}{^Q4\_1\_8\_sharing\_No}☐{/} No **If “YES,” describe all applicable means:**{Q4\_1\_8\_ex} | PT-4 | GV.OC-03 |
| 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.****Tip**: 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’s name, phone and email contact information in this section in addition to the entity’s procedures. {Q4\_1\_9} | AC-1 AC-3(14), PM-20, PT-5,PT-6 | PR.AA-01 |
| 4.1.10 | **Describe the procedures for individuals to address possibly inaccurate or erroneous information.****Tip**: 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.{Q4\_1\_10} | PM-22,SI-18,SI-18(4), SI-18(5) | GV.OC-03 |
| 4.1.11 | **Does your agency require notice to affected individuals when their personal information is requested, sold, or released to third parties?**{#Q4\_1\_11\_Yes}☒{/}{^Q4\_1\_11\_Yes}☐{/} Yes{#Q4\_1\_11\_No}☒{/}{^Q4\_1\_11\_No}☐{/} No**If “NO,” explain:**{Q4\_1\_11\_explanation} | PT-5,PT-5(1) | PR.DS-02 |
| 4.1.12 | **Are the agency privacy practices publicly available through the organizational website?**{#Q4\_1\_12\_Yes}☒{/}{^Q4\_1\_12\_Yes}☐{/} Yes{#Q4\_1\_12\_No}☒{/}{^Q4\_1\_12\_No}☐{/} No**If “NO”, explain:**{Q4\_1\_12\_explanation} | PM-20 | GV.PO-01 |
| 4.1.13 | **Is the privacy incident response plan incorporated into your entity’s Incident Response Plan?**{#Q4\_1\_13\_Yes}☒{/}{^Q4\_1\_13\_Yes}☐{/} Yes{#Q4\_1\_13\_No}☒{/}{^Q4\_1\_13\_No}☐{/} No**If “NO,” explain why not; if “YES,” describe where it is located.**{Q4\_1\_13\_explanation} | IR-8,IR-8(1) | ID.IM-04 |
| 4.1.14 | **Does your organization’s online privacy notice or statement to the public and individuals include the following:*** Its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII)

 {#Q4\_1\_14\_a\_Yes}☒{/}{^Q4\_1\_14\_a\_Yes}☐{/} Yes {#Q4\_1\_14\_a\_No}☒{/}{^Q4\_1\_14\_a\_No}☐{/} No* Authority for collecting PII

 {#Q4\_1\_14\_b\_Yes}☒{/}{^Q4\_1\_14\_b\_Yes}☐{/} Yes {#Q4\_1\_14\_b\_No}☒{/}{^Q4\_1\_14\_b\_No}☐{/} No * The choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices

 {#Q4\_1\_14\_c\_Yes}☒{/}{^Q4\_1\_14\_c\_Yes}☐{/} Yes{#Q4\_1\_14\_c\_No}☒{/}{^Q4\_1\_14\_c\_No}☐{/} No * The ability to access and have PII amended or corrected if necessary

 {#Q4\_1\_14\_d\_Yes}☒{/}{^Q4\_1\_14\_d\_Yes}☐{/} Yes {#Q4\_1\_14\_d\_No}☒{/}{^Q4\_1\_14\_d\_No}☐{/} No | PT-5,PT-5(1) | GV.OC-03 |
| 4.1.15 | **Does the organization evaluate any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized?**{#Q4\_1\_15\_Yes}☒{/}{^Q4\_1\_15\_Yes}☐{/} Yes{#Q4\_1\_15\_No}☒{/}{^Q4\_1\_15\_No}☐{/} No**If “YES,” provide a brief description:**{Q4\_1\_15\_explanation} | AC-21, AC-3(5), , PT-2, PT-3 | GV.OV-03 |
| 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?**{#Q4\_1\_16\_Yes}☒{/}{^Q4\_1\_16\_Yes}☐{/} Yes{#Q4\_1\_16\_No}☒{/}{^Q4\_1\_16\_No}☐{/} NoProvide copies of the applicable privacy notices.  | PT-4 | GV.OC-03 |

| **No.** | **Analysis: Privacy Program Administration** |
| --- | --- |
| 4.1.17 | **Analysis: Related to Privacy Program Administration**This portion of the PIA is for details about information provided in this Privacy Program Administration section. Identify privacy risks, mitigation strategies and, if necessary, provide a corrective action plan. **Privacy Risk**: {Q4\_1\_17\_risk} **Mitigation:** {Q4\_1\_17\_mitigation}**Corrective Action Plan**: {Q4\_1\_17\_action} |

* 1. **Collection**

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

| **No.** | **Questions** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 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 the collection, use, maintenance, and sharing of the information.  A simple citation without more information will not be sufficient for the purposes of this document and will result in the rejection of this Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the collection of the subject information.{Q4\_2\_1} | PT-2 | GV.OC-03 |
| 4.2.2 | **Does the system collect Social Security Numbers?**{#Q4\_2\_2\_Yes}☒{/}{^Q4\_2\_2\_Yes}☐{/} Yes{#Q4\_2\_2\_No}☒{/}{^Q4\_2\_2\_No}☐{/} No**If “YES,” identify the specific authority allowing such collection. If you are relying on another federal or state agency, list their legal authorities**.**Tip:**  Reference for items # 4.2.2, 4.2.3 and 4.2.5 IPA refers to Information Practices Act-Civil Code Section 1798. #4.2.2 SAM: 5310, 5305.8 NIST 800-53: PT-2, AC-21, AT-3(5), AU-2, PT-2, PT-3 Civil Code Section 1798.85, 1798.86, 1798.89 #4.2.3 - NIST 800-53 AC-21, AT-3(5), AU-2, PT-2, PT-3 #4.2.5 - SAM 5310.1, SIMM 5310-A, SAM 5305.8, NIST 800-53 PT-3, PT-5, PT-5(1) PT-5(2), PT-6; Civil Code Section 1798.17 {Q4\_2\_2\_explanation} | PT-2 | GV.OC-03 |
| 4.2.3 | **Is PII received from another governmental agency or entity under an agreement?**{#Q4\_2\_3\_Yes}☒{/}{^Q4\_2\_3\_Yes}☐{/} Yes{#Q4\_2\_3\_No}☒{/}{^Q4\_2\_3\_No}☐{/} No**If “YES,” cite the agreement and where it can be found.**{Q4\_2\_3\_explanation} | AC-21, AT-3(5), AU-2, PT-2, PT-3 | RC.CO-03 |
| 4.2.4 | **Describe the purpose(s) for which PII is collected, used, and maintained.**{Q4\_2\_4} | PT-3 | GV.PO-01 |
| 4.2.5 | **Is the above purpose also stated in your ‘notice on collection’?**{#Q4\_2\_5\_Yes}☒{/}{^Q4\_2\_5\_Yes}☐{/} Yes{#Q4\_2\_5\_No}☒{/}{^Q4\_2\_5\_No}☐{/} No**Tip:** ‘Notice on collection’ means clearly communicating to individuals the purpose of collecting their personal information. See SIMM 5310-A.  | PT-5, PT-5(1) | GV.PO-01 |
| 4.2.6 | **Is the reason information is being collected displayed in clear, simple language that can be easily understood by the data subject?**{#Q4\_2\_6\_Yes}☒{/}{^Q4\_2\_6\_Yes}☐{/} Yes{#Q4\_2\_6\_No}☒{/}{^Q4\_2\_6\_No}☐{/} No | PT-3 | GV-OC-03 |
| 4.2.7 | **Does this project/process/system/program collect PII directly from the individual to the greatest extent possible?**{#Q4\_2\_7\_Yes}☒{/}{^Q4\_2\_7\_Yes}☐{/} Yes{#Q4\_2\_7\_No}☒{/}{^Q4\_2\_7\_No}☐{/} No**Identify the sources from which the information may be collected**.{#individuals}☒{/}{^individuals}☐{/} Individuals{#another\_entity}☒{/}{^another\_entity}☐{/} Another Entity{#business\_partner}☒{/}{^business\_partner}☐{/} Business Partner/Vendors{#internally}☒{/}{^internally}☐{/} Internally – please describe: {Q4\_2\_7\_internally\_text}{#genai\_training}☒{/}{^genai\_training}☐{/} GenAI Training Model (if this option is selected, complete 4.2.8; otherwise, go to 4.2.9){#other}☒{/}{^other}☐{/} Other – please specify: {Q4\_2\_7\_explanation} | PM-22, SI-18 | GV-OC-03 |
| 4.2.8 | **Will the system ingest or output information, such as images, videos, audio clips, or text that has been significantly altered or generated by algorithms, including by AI, known as “synthetic data”?**{#Q4\_2\_8\_Yes}☒{/}{^Q4\_2\_8\_Yes}☐{/} Yes{#Q4\_2\_8\_No}☒{/}{^Q4\_2\_8\_No}☐{/} No | NIST AI 100-4 |  |
| 4.2.9 | **Is there a probability that the synthetic data will impact information integrity, increase fraud, or cause intellectual property and/or copyright issues?**{#Q4\_2\_9\_Yes}☒{/}{^Q4\_2\_9\_Yes}☐{/} Yes{#Q4\_2\_9\_No}☒{/}{^Q4\_2\_9\_No}☐{/} No If “YES, please describe how:{Q4\_2\_9\_explanation} | NIST AI 100-4 |  |
| 4.2.10 | **Will the data output be reviewed/audited by an individual/team to mitigate against hallucinations and bias to ensure that data outputs are accurate and factual?**{#Q4\_2\_10\_Yes}☒{/}{^Q4\_2\_10\_Yes}☐{/} Yes{#Q4\_2\_10\_No}☒{/}{^Q4\_2\_10\_No}☐{/} No**If “NO,” describe here and document it as a risk. Provide a mitigation plan in the Analysis: Collection section.**{Q4\_2\_10\_explanation} | GenAI guidelinesand toolkit | GenAI guidelinesand toolkit |
| 4.2.11 | **How will PII be collected? Select all applicable items:**{#paper}☒{/}{^paper}☐{/} Paper{#electronically}☒{/}{^electronically}☐{/} Electronically{#verbally}☒{/}{^verbally}☐{/} Verbally{#other2}☒{/}{^other2}☐{/} Other – please specify: {Q4\_2\_11} | PM-22, SI-18 | GV.OC-03 |
| 4.2.12 | **Are Social Security Numbers extracted from any other source?****Tip**: For example, is an SSN match made and extracted via other information provided by the claimant, employer, or provider, or verified with SSA, etc.?{#Q4\_2\_12\_Yes}☒{/}{^Q4\_2\_12\_Yes}☐{/} Yes{#Q4\_2\_12\_No}☒{/}{^Q4\_2\_12\_No}☐{/} No**If “YES”, describe the source:**{Q4\_2\_12\_explanation} | AC-21, AT-3(5), AU-2, PT-2, PT-3 | GV.OC-03 |
| 4.2.13 | **Does the system or manual process use information from commercial sources, including GenAI or publicly available data?**{#Q4\_2\_13\_Yes}☒{/}{^Q4\_2\_13\_Yes}☐{/} Yes{#Q4\_2\_13\_No}☒{/}{^Q4\_2\_13\_No}☐{/} No **If “YES,” explain why and how this information is used. Indicate whether the commercial or public source data is marked within the system.**{Q4\_2\_13\_explanation}***If GenAI data is used, answer the following questions:*****What data sets are being pulled, and where are they pulled from?** {Q4\_2\_13\_datasets}**Why is the data set being pulled, and what is it used for?**{Q4\_2\_13\_purpose} **How will you ensure that publicly available data, in combination with other data, does not create/output PII data?** **Tip**:  Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, commercial data is used to verify information already provided by or about the individual.{Q4\_2\_13\_protection}  | AC-21, AT-3(5), AU-2, PT-2, PT-3 | GV.OC-05 and GenAI toolkit |
| 4.2.14 | **Does the system receive or send data to another system or third party outside of the organization?****Tip**: For example, is data received through an application programming interface (API) or other data transfer protocols, e.g., a response to a background check? {#Q4\_2\_14\_Yes}☒{/}{^Q4\_2\_14\_Yes}☐{/} Yes{#Q4\_2\_14\_No}☒{/}{^Q4\_2\_14\_No}☐{/} No**If “YES,” describe the system, entity, and data sharing agreement, including what information is used and how it is used**.  **System Name:** {Q4\_2\_14\_system\_name}  **Data elements:** {Q4\_2\_14\_data\_elements}  **How the information is used:** {Q4\_2\_14\_how\_used}  **Name of the entity:** {Q4\_2\_14\_entity\_name} **Original source or data owner of the date:** {Q4\_2\_14\_data\_owner}  | PM-22, SI-18,AC-21, AT-3(5), AU-2, PT-2, PT-3 |  |
| 4.2.15 | **Does the organization identify the minimum PII elements required by the information system or activity to accomplish the legally authorized purpose of collection?**{#Q4\_2\_15\_Yes}☒{/}{^Q4\_2\_15\_Yes}☐{/} Yes{#Q4\_2\_15\_No}☒{/}{^Q4\_2\_15\_No}☐{/} No | SA-8(33), PM-5(1), SI-12(1) |   |

| No. | **Analysis: Collection** |
| --- | --- |
| 4.2.16 | **Analysis: Related to Collection** This portion of the PIA is to provide details about information related to PII collection. Identify privacy risks, including GenAI risks, mitigation, and, if necessary, provide a corrective action plan. **Privacy Risk**: {Q4\_2\_16\_risk} **Mitigation:** {Q4\_2\_16\_mitigation} **Corrective Action Plan**:  {Q4\_2\_16\_action}  |

* 1. **Use**

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

| **No.** | **Questions** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 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. {Q4\_3\_1} | PM-22, SI-1 | PR.AA-01 |
| 4.3.2 | **Is the use of the PII collected limited to the stated purpose for which the individual has provided consent?**{#Q4\_3\_2\_Yes}☒{/}{^Q4\_3\_2\_Yes}☐{/} Yes{#Q4\_3\_2\_No}☒{/}{^Q4\_3\_2\_No}☐{/} No**If “NO,” please provide further information.**{Q4\_3\_2\_explanation}  | SA-8(33), PM-5(1), SI-12(1) | GV OC-03 |
| 4.3.3 | **Will PII be used in testing, training, and or research?** {#Q4\_3\_3\_Yes}☒{/}{^Q4\_3\_3\_Yes}☐{/} Yes{#Q4\_3\_3\_No}☒{/}{^Q4\_3\_3\_No}☐{/} No   **If “Yes,” please describe:**{Q4\_3\_3\_explanation} **If “NO,” go to 4.3.6**.  | PM-25, SI-12(2) | GV OC-03 |
| 4.3.4 | **Are there policies and/or procedures to minimize the use of PII in testing, training, GenAI training models and/or research?**{#Q4\_3\_4\_Yes}☒{/}{^Q4\_3\_4\_Yes}☐{/} Yes{#Q4\_3\_4\_No}☒{/}{^Q4\_3\_4\_No}☐{/} No  **If “YES,” describe and provide the name and location of the policies/procedures:**{Q4\_3\_4\_explanation} | PM-25, SI-12(2) | GV.OC-03 |
| 4.3.5 | **If PII is used in testing, training, GenAI training models, or research, what controls will be implemented to protect PII from unauthorized use and disclosure?**{Q4\_3\_5}  | PM-25, SI-12(2) | PR.DS-01,02,10 |
| 4.3.6 | **Is the use of PII internally only for the authorized purpose(s) identified in the privacy policy or notice on the collection?**{#Q4\_3\_6\_Yes}☒{/}{^Q4\_3\_6\_Yes}☐{/} Yes{#Q4\_3\_6\_No}☒{/}{^Q4\_3\_6\_No}☐{/} No | PT-3 | GV.OC-03 |
| 4.3.7 | **Can other entities (including contractors or service providers) access the data in this system?**{#Q4\_3\_7\_Yes}☒{/}{^Q4\_3\_7\_Yes}☐{/} Yes{#Q4\_3\_7\_No}☒{/}{^Q4\_3\_7\_No}☐{/} No**If “YES,” What laws or regulations authorize access?**{Q4\_3\_7\_explanation}  | AC-21, AT-3(5), AU-2, PT-2, PT-3PT-2 | PR.AA-02 |
| 4.3.8 | **Describe how you ensure that only the employees authorized to access the PII data have access to it.**{Q4\_3\_8\_a} **Describe how the organization will monitor and audit privacy controls for this project/process/system**. {Q4\_3\_8\_b} **Do the audit measures discussed above include the ability to identify specific records each user can access?**{#Q4\_3\_8\_c\_Yes}☒{/}{^Q4\_3\_8\_c\_Yes}☐{/} Yes{#Q4\_3\_8\_c\_No}☒{/}{^Q4\_3\_8\_c\_No}☐{/} No**If “NO,” explain why**{Q4\_3\_8\_c} **Describe the different roles that have been created to provide access to the project information**. **Use general terms.****Tip**: 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. {Q4\_3\_8\_d}  | CA-2 | PR.AA-01 |
| 4.3.9 | **Does the project have human verification on GenAI outputs and perform self-audits or third-party audits and/or reviews by other entities?**{#Q4\_3\_9\_Yes}☒{/}{^Q4\_3\_9\_Yes}☐{/} Yes{#Q4\_3\_9\_No}☒{/}{^Q4\_3\_9\_No}☐{/} No{#Q4\_3\_9\_NA}☒{/}{^Q4\_3\_9\_NA}☐{/} N/A**If “NO,” explain why**{Q4\_3\_9\_explanation}  | CA-2 | ID.IM-01 |

| No. | **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 including GenAI risks, mitigation strategies and, if necessary, provide a corrective action plan. **Privacy Risk:** {Q4\_3\_10\_a} **Mitigation:** {Q4\_3\_10\_b} **Corrective Action Plan:**{Q4\_3\_10\_c}  |

* 1. **Maintenance and Storage**

Please describe below how [State Entity] controls the maintenance and storage of personally identifiable information.

| **No.** | **Questions and Fillable Answers** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 4.4.1 | **Where will PII be stored? Select all applicable items:**{#cloud}☒{/}{^cloud}☐{/} Cloud{#local\_drive}☒{/}{^local\_drive}☐{/} Local Drive{#shared\_drive}☒{/}{^shared\_drive}☐{/} Shared Drive{#system\_db}☒{/}{^system\_db}☐{/} System/Database (including GenAI Training model){#third\_party}☒{/}{^third\_party}☐{/} Third-Party storage: {Q4\_4\_1\_vendor}{#physical\_paper}☒{/}{^physical\_paper}☐{/} Physical paper filed: {Q4\_4\_1\_location} | PM-5(1) | ID.AM-08 |
| 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?****Tip**: For example, the project or program does not utilize the inaccurate or outdated PII. It merely identifies to the state entity that it is visible when it should not be visible since it should be encrypted.  {Q4\_4\_2} | PM-22, SI-18 | ID.AM-08 |
| 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.****Tip**: Sometimes, information is assumed to be accurate, or in Research & Development, inaccurate information may not impact the individual or the system. If the system or program does not check for accuracy, including reviewing/auditing GenAI outputs, please explain why. {Q4\_4\_3} | PM-22, SI-18 | GV.OC-03 |
| 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*. {Q4\_4\_4} | PM-24, SI-1 | GV.OC-03 |
| 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 program's needs. Consult with your records management office for assistance with this question if necessary. {Q4\_4\_5} | MP-6, SI-12, SI-12(3)SAM 5310.6 and Civil Code Section:1798.18 | ID.AM-08 |
| 4.4.6 | **Is all the information the project/process/system/program collects retained?**{#Q4\_4\_6\_Yes}☒{/}{^Q4\_4\_6\_Yes}☐{/} Yes{#Q4\_4\_6\_No}☒{/}{^Q4\_4\_6\_No}☐{/} No **If “YES,” Is there a specific subset of information retained?**{#Q4\_4\_6\_subset\_Yes}☒{/}{^Q4\_4\_6\_subset\_Yes}☐{/} Yes{#Q4\_4\_6\_subset\_No}☒{/}{^Q4\_4\_6\_subset\_No}☐{/} No If “YES,” describe:**Tip:**  Example: A project may collect extensive PII initially to verify an individual's identity for a background check.  Upon completion of the background check, the project will maintain the new information and 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. {Q4\_4\_6\_subset\_explanation} | MP-6, SI-12, SI-12(3)SAM 5310.6 and Civil Code Section: 1798.18 | ID.AM-08 |
| 4.4.7 | **Is there an automated purge process built into this system/program for all data housed within the system/program?**{#Q4\_4\_7\_Yes}☒{/}{^Q4\_4\_7\_Yes}☐{/} Yes{#Q4\_4\_7\_No}☒{/}{^Q4\_4\_7\_No}☐{/} NoProvide the Business Use Case, which outlines the purge criteria. {Q4\_4\_7\_explanation}  |   | ID.AM-08 |
| 4.4.8 | **Are there any data elements within this system/program that do not adhere to an automated purge process?**{#Q4\_4\_8\_Yes}☒{/}{^Q4\_4\_8\_Yes}☐{/} Yes{#Q4\_4\_8\_No}☒{/}{^Q4\_4\_8\_No}☐{/} No**If “YES,” is there an active data retention variance for this data?**{#Q4\_4\_8\_variance\_Yes}☒{/}{^Q4\_4\_8\_variance\_Yes}☐{/} Yes{#Q4\_4\_8\_variance\_No}☒{/}{^Q4\_4\_8\_variance\_No}☐{/} No **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 the 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 purpose and only for as long as necessary and relevant to fulfill the specified purposes? • Has the PIA described policies and procedures for purging PII that is no longer relevant and necessary? {Q4\_4\_8\_variance\_explanation} |   | ID.AM-08 |
| 4.4.9 | **Can the synthetic data be tracked and audited for integrity and non-reputability?**{#Q4\_4\_9\_Yes}☒{/}{^Q4\_4\_9\_Yes}☐{/} Yes{#Q4\_4\_9\_No}☒{/}{^Q4\_4\_9\_No}☐{/} No **If “YES,” please describe how:** {Q4\_4\_9\_explanation} | NIST AI 100-4 |  |
| 4.4.10 | **Is there a mechanism to ensure consumers are notified when speaking to Artificial Intelligence and can opt out if they choose to do so?**{#Q4\_4\_10\_Yes}☒{/}{^Q4\_4\_10\_Yes}☐{/} Yes{#Q4\_4\_10\_No}☒{/}{^Q4\_4\_10\_No}☐{/} No  | NIST AI 100-4  |  |

| **No.** | **Analysis: Maintenance and Storage** |
| --- | --- |
| 4.4.11 | **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, mitigation 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 the 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 purpose and only for as long as necessary and relevant to fulfill the specified purposes? Has the PIA described policies and procedures for purging PII that is no longer relevant and necessary? **Privacy Risk:**{Q4\_4\_11\_risk} **Mitigation:**{Q4\_4\_11\_mitigation}**Corrective Action Plan**: {Q4\_4\_11\_action} |

* 1. **Disclose/Share**

In the following section, describe whether [State Entity] discloses or shares the personally identifiable information under its purview with other entities.

| **No.** | **Questions and Fillable Answers** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 4.5.1 | **Does the project maintain an accurate accounting/record of disclosure of information held in the system?**{#Q4\_5\_1\_Yes}☒{/}{^Q4\_5\_1\_Yes}☐{/} Yes{#Q4\_5\_1\_No}☒{/}{^Q4\_5\_1\_No}☐{/} No Who is responsible for the accounting of disclosures? **Title:** {Q4\_5\_1\_title} **Name:** {Q4\_5\_1\_name}  | PM-21 | PR.PS-04 |
| 4.5.2 | **What is the retention period for the accounting/record of disclosure of PII mentioned above?**{Q4\_5\_2} | PM-21 | ID.AM-08 |
| 4.5.3 | **Is the disclosure of the PII collected limited to the stated purpose and for which the individual has provided consent?**{#Q4\_5\_3\_Yes}☒{/}{^Q4\_5\_3\_Yes}☐{/} Yes{#Q4\_5\_3\_No}☒{/}{^Q4\_5\_3\_No}☐{/} NoIf “NO,” describe:{Q4\_5\_3\_explanation}  | SA-8(33), PM-5(1), SI-12(1) | GV.OC-03 |
| 4.5.4 | **Discuss state information sharing between agencies and departments and/or public and private sector entities**. * Identify and list the State entities with which the information is shared.
* What laws or statutes authorize disclosure?

**Tip**: For example, certain systems regularly share information because of the crossover of the different parts of the state. {Q4\_5\_4} | AC-21, AT-3(5), AU-2, PT-2, PT-3 Civil Code Section: 1798.24 1798.25 | ID.RA-08 |
| 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?**{#Q4\_5\_5\_Yes}☒{/}{^Q4\_5\_5\_Yes}☐{/} Yes{#Q4\_5\_5\_No}☒{/}{^Q4\_5\_5\_No}☐{/} No **If “YES,” identify the federal, state, and local agencies or privacy sector entities, how the information is accessed, and how it is to be used.**{Q4\_5\_5\_yes}  | AC-21, AT-3(5), AU-2, PT-2, PT-3 and Civil Code Section: 1798.24 and 1798.25 | RS.CO-03 |
| 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?**{#Q4\_5\_6\_Yes}☒{/}{^Q4\_5\_6\_Yes}☐{/} Yes{#Q4\_5\_6\_No}☒{/}{^Q4\_5\_6\_No}☐{/} No **If “NO”, explain.**{Q4\_5\_6\_explanation} | AC-21, AT-3(5), AU-2, PT-2, PT-3 | RS.CO-03 |
| 4.5.7 | **If the organization shares PII collected within this project/system/process/program with external entities, describe how that sharing occurs:**{Q4\_5\_7}**Are Memoranda of Understanding, Inter-Agency Agreement, Letters of Intent, or similar agreements executed?**{#Q4\_5\_7\_mou\_Yes}☒{/}{^Q4\_5\_7\_mou\_Yes}☐{/} Yes{#Q4\_5\_7\_mou\_No}☒{/}{^Q4\_5\_7\_mou\_No}☐{/} NoIf “YES,” provide a copy. **Is the PII specifically identified?**{#Q4\_5\_7\_identified\_Yes}☒{/}{^Q4\_5\_7\_identified\_Yes}☐{/} Yes{#Q4\_5\_7\_identified\_No}☒{/}{^Q4\_5\_7\_identified\_No}☐{/} No**Are the purposes for which it will be used detailed?**{#Q4\_5\_7\_purposes\_Yes}☒{/}{^Q4\_5\_7\_purposes\_Yes}☐{/} Yes{#Q4\_5\_7\_purposes\_No}☒{/}{^Q4\_5\_7\_purposes\_No}☐{/} No **Does the agreement (in whatever form) detail the responsibilities of the third parties to protect and secure the PII?**{#Q4\_5\_7\_protect\_Yes}☒{/}{^Q4\_5\_7\_protect\_Yes}☐{/} Yes{#Q4\_5\_7\_protect\_No}☒{/}{^Q4\_5\_7\_protect\_No}☐{/} No **Does the agreement require formal acknowledgment (i.e., the signature of authority, etc.)?**{#Q4\_5\_7\_signature\_Yes}☒{/}{^Q4\_5\_7\_signature\_Yes}☐{/} Yes{#Q4\_5\_7\_signature\_No}☒{/}{^Q4\_5\_7\_signature\_No}☐{/} No**Is the data captured for this system or the output of this system being used to train another AI model?** {#Q4\_5\_7\_ai\_Yes}☒{/}{^Q4\_5\_7\_ai\_Yes}☐{/} Yes{#Q4\_5\_7\_ai\_No}☒{/}{^Q4\_5\_7\_ai\_No}☐{/} No**If the response is “YES” to any of the above, describe:**{Q4\_5\_7\_ai} **If the response is “No” to any of the above and data is being shared/exchanged, explain how this risk is mitigated in the analysis section**. | AC-21, AT-3(5), AU-2, PT-2, PT-3, SA-1, SA-4, SA-9 | RS.CO-03 |
| 4.5.8 | **What is the process for the discovery of data subject to PII disclosure?**{Q4\_5\_8}  | AC-1, AC-3(14), PM-20, PT-5, PT-6 | Gv.OC-03 |
| 4.5.9 | **Will any of the following techniques be implemented to *directly* disclose how AI was used in the content creation?**Select all applicable items:{#content\_labels}☒{/}{^content\_labels}☐{/} Content labels{#visible\_watermarks}☒{/}{^visible\_watermarks}☐{/} Visible watermarks{#disclosures\_fields}☒{/}{^disclosures\_fields}☐{/} Disclosures fields{#other}☒{/}{^other}☐{/} Other – please specify: {Q4\_5\_9\_other} | NIST AI 100-4 |  |
| 4.5.10 | **Will any of the following techniques be implemented to *indirectly* disclose how AI was used in the content creation?**Select all applicable items: {#covert\_watermarks}☒{/}{^covert\_watermarks}☐{/} Covert watermarks{#digital\_fingerprints}☒{/}{^digital\_fingerprints}☐{/} Digital fingerprints{#embedded\_metadata}☒{/}{^embedded\_metadata}☐{/} Embedded metadata**Will the system host metadata information?**{#Q4\_5\_10\_metadata\_Yes}☒{/}{^Q4\_5\_10\_metadata\_Yes}☐{/} Yes{#Q4\_5\_10\_metadata\_No}☒{/}{^Q4\_5\_10\_metadata\_No}☐{/} No **If “YES,” will there be security controls to prevent privacy leakage through the visibility of sensitive metadata across the network?**{#Q4\_5\_10\_security\_Yes}☒{/}{^Q4\_5\_10\_security\_Yes}☐{/} Yes{#Q4\_5\_10\_security\_No}☒{/}{^Q4\_5\_10\_security\_No}☐{/} No{#Q4\_5\_10\_security\_Other}☒{/}{^Q4\_5\_10\_security\_Other}☐{/} Other – please specify: {Q4\_5\_10\_other}  |  |  |

| No. | **Analysis: Disclose/Share** |
| --- | --- |
| 4.5.11 | **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, mitigation strategies and, if necessary, provide a corrective action plan.  **Privacy Risk:** {Q4\_5\_11\_risk}**Mitigation:** {Q4\_5\_11\_mitigation}**Corrective Action Plan:** {Q4\_5\_11\_action}  |

* 1. **Destruction/Disposal**

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

| **No.** | **Questions and Fillable Answers** | **References** |
| --- | --- | --- |
| **NIST** | **CSF 2.0** |
| 4.6.1 | **How will information be disposed of (e.g., placed in a confidential bin, disposed of by a contractor, or electronically wiped/erased)?**{Q4\_6\_1}**If done by a contractor, provide the name of the contractor and a copy of the agreement.**{Q4\_6\_1\_contractor} | MP-6, SI-12, SI-12(3) | GV.SC-10 |
| 4.6.2 | **What method does the organization use for secure deletion/destruction of PII?**{Q4\_6\_2} | MP-6, SI-12, SI-12(3) | GV.SC-10 |
| 4.6.3 | **Does the entity formally validate the secure destruction /disposal of PII?**{#Q4\_6\_3\_Yes}☒{/}{^Q4\_6\_3\_Yes}☐{/} Yes{#Q4\_6\_3\_No}☒{/}{^Q4\_6\_3\_No}☐{/} No  | MP-6, SI-12, SI-12(3) | GV.SC-10 |

| No. | **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, mitigation strategies and, if necessary, provide a corrective action plan. **Privacy Risk:** {Q4\_6\_4\_risk}**Mitigation:** {Q4\_6\_4\_mitigation}**Corrective Action Plan:**{Q4\_6\_4\_action}  |

# Privacy Threshold / Impact Assessment Authorization and Acceptance

I have authorized, reviewed, and understand the ☐ Privacy Threshold ☐ Privacy Impact Assessment results for the {Q1\_1}.

 {Q5\_1\_date}

<Deputy Director / Data Owner> Signature Date

{Q5\_1\_title}

Print Name

Click or tap here to enter text.  {Q5\_2\_date}

<Business Process Owner> Signature Date

{Q5\_2\_title}

Print Name

Click or tap here to enter text.  {Q5\_3\_date}

<Chief Information Officer/ IT Manager> Signature Date

{Q5\_3\_title}

Print Name

Click or tap here to enter text.  {Q5\_4\_date}

<Privacy Officer /Privacy Coordinator> Signature Date

{Q5\_4\_title}

Print Name

Click or tap here to enter text. {Q5\_5\_date}

<Information Security Officer> Signature Date 

{Q5\_5\_title}

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 and SIMM Section 5310-C.

# NIST SP 800-53 and FIPS Reference

| **Family** | **Control** |
| --- | --- |
| Access Control (AC)  | AC-20  |
| Assessment, Authorization, and Monitoring  | CA-2  |
| Audit and Accountability  | AU-2  |
| Awareness and Training (AT)  | AT-1, AT-2, AT-3, AT 3(5), AT-6  |
| Incident Response (IR)  | IR-8, IR-8(1)  |
| Media Protection (MP)  | MP-6  |
| Personally Identifiable Information Processing and Transparency (PT)  | PT-2, PT-3, PT-4, PT-5, PT-5(1), PT-5(2), PT-6,   |
| Personnel Security (PS)  | PS-1, PS-2, PS-6, PS-8  |
| Planning (PL)  | PL-4  |
| Program Management (PM)  | PM-3, PM-5(1), PM-18, PM-19, PM-20, PM-21, PM-22, PM-24, PM-25, PM-26, PM-27  |
| Risk Assessment (RA)   | RA-3, RA-8  |
| System and Services Acquisition  | SA-1, SA-4, SA-8(33), SA-9  |
| System and Information Integrity  | SI-1, SI-12, SI-12(1), SI-12(2), SI-12(3), SI-18, SI-18(4), SI-14(5)  |
|   |   |
| 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)  |
| NIST AI RMF Policy & Technical Documents | [NIST 100-4](https://airc.nist.gov/AI_RMF_Knowledge_Base/Technical_And_Policy_Documents) |

# Related SIMM and Guideline References

| **Reference** | **Article** |
| --- | --- |
| 5310-A  | Privacy Statement and Notices Standard  |
| 5310-B  | Privacy Individual Access Standard  |

[GenAI Guidelines](https://cdt.ca.gov/wp-content/uploads/2024/03/3a-GenAI-Guidelines.pdf)

# Related Policies, Procedures and Standards

**Tip*:*** *Refer to the Policy, Procedures Templates located on OIS AgencyNet for examples of articles below.*

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

# Revision History

| **Date** | **Description of Change** | **Reviewer** |
| --- | --- | --- |
| {Q5\_6\_date\_1} | {Q5\_6\_description\_1} | {Q5\_6\_reviewer\_1} |

# 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.    |