State of California

Department of Technology

Designation Letter

Statewide Information Management Manual – 5330-A

May 2025

Table of Contents

Document History

Revision	Date of Release	Owner	Summary of Changes
Initial Release	August 2012	California Office of Information Security	
Minor Update	September 2013	California Information Security Office	SIMM number change, change "agency" to "state entity," and change references to other related SIMM documents
Minor Update	January 2018	Office of Information Security (OIS)	Office name change; Designation Letter: item #1, clarification on SIMM signing authority; item #2, addition of the AIO and AISO, correction of the functions supported titles; parent/child entity relationship definition; addition of contact information of the Secretary/Director Attachment A: correction of SIMM forms that designees are authorized to sign. Attachment B: correction of page title; removal of pager number Attachment C: clarification on organizational chart submission instructions and attachment of sample org chart; Attachment D: revised instructions; inclusion of parent/child entity relationship; corrections to SIMM reference
Minor Update	March 2019	OIS	Attachment A: updated to include required submission to AIO/AISO; Attachment B: revised to include space for additional email address fields; moved detailed instructions into the Designation Letter Instructions (SIMM 5330-D); added confidential statement
Minor Update	January 2020	OIS	Update format; remove Parent/Child sections, creating new Parent/Child SIMM 5330-E; add AIO/AISO back-up option
Minor Update	March 2023	OIS	Update format; Added separate compliance forms requirement for all state entities; added field for phone extensions

Revision	Date of Release	Owner	Summary of Changes
Minor Update	December 2023	OIS	Attachment D- Entity Partnership Types are clearly defined and Supported by Program Agreement SIMM 5330-G was created.
Minor Update	June 2024	OIS	Template and format update, verbiage clarifications made.
Major Update	May 2025	OIS	Clarification of responsibilities of Host/Hosted provided, format updated, addendums incorporated.

Introduction

Purpose

All state entities must submit the Designation Letter annually to the Office of Information Security (OIS) on the last business day of the state entity's scheduled reporting month, as outlined in the Information Security Compliance Reporting Schedule (SIMM 5330-C) or within (10) business days of any designation changes.

Within the Designation Letter, the state entity head shall designate staff to be designated signers and points of contact to fulfill the state entity's security and privacy requirements. In addition to the designee assignments, the state entity head must attach the organizational chart and identify if the entity receives support from another entity.

Scope

The Information Security Compliance Reporting Schedule and Designation Letter applies to all California state entities, including departments, divisions, bureaus, boards, and commissions, as defined in Government Code Section 11546.1.

Compliance

As outlined in Government Code (GC) Section 11549.3, OIS is entrusted with creating, issuing, and maintaining policies, standards, and procedures, overseeing information security risk management for agencies and state entities, providing information security and privacy guidance, and ensuring compliance with State Administrative Manual (SAM) Chapter 5300 and Statewide Information Management Manual (SIMM) section 5300.

State entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their agency or state entity. Full compliance is expected. State entities must adhere to OIS-issued information security and privacy policies and all relevant laws, regulations, rules, and standards governing their state entity. Compliance may be reflected in audit findings and maturity scores. For any known non-compliance, the state entity must log the non-compliance or risk entry in their Risk Register & Plan of Action and Milestones (RRPOAM).

To: Office of Information Security
California Department of
Technology Attn: Security
Compliance Reporting
P.O. Box 1810, Mail Stop Y- 01
Rancho Cordova, CA 95741

ENTITY NAME: ____ **ORG CODE:** _________

GOV CODE: Choose an item. **COMPLIANCE REPORT DUE DATE:**

Please be advised that it is mandatory for each individual state entity or agency to complete and submit the SIMM 5330-A, irrespective of the state entity partnership type delineated in Section D.

SUBJECT: **Designation Letter**

I, the undersigned, hereby certify that I am the Secretary/Director (*or equivalent state entity head*) for the above-referenced state entity. In compliance with the requirements set forth in State Policy (State Administrative Manual Chapter 5300), I have made the following designations to ensure the fulfillment of information security and privacy requirements for this state entity:

1. **Secretary/Director's Signature Authority Designee(s)** as authorized by me in **Section A**. These executive-level individual(s) are authorized to sign specified information security and privacy compliance-related documents on my behalf.

2. **Secretary/Director's Designee(s)** are identified by me in **Section B** and include the Agency Information Officer (AIO) or Agency Chief Information Officer (ACIO), Agency Information Security Officer (AISO), CIO, ISO, Technology Recovery Coordinator, Privacy Officer/Coordinator, and their back-ups.

I certify that the organizational chart for this state entity is included with this form, reflecting our organization's alignment with Government Code Section 11546.1(d) or 11000.

I certify that this state entity is fully supported, partially supported, or self-supported for services as declared in **Section C**.

For additional information about this submission, please contact:

______________________ ______________________ ______________________
Name Telephone Number Email

Signature and contact information of the Secretary/Director (or equivalent state entity head):

______________________ ______________________ ______________________
Name Signature Date

______________________ ______________________ ______________________
Business Mailing Address Telephone Number Email

SECTION A: SECRETARY/DIRECTOR’S SIGNATURE AUTHORITY DESIGNEE(S)

ONE OF THE BELOW OPTIONS MUST BE SELECTED:

☐ I **have not** authorized any designees to sign on my behalf.

☐ I **have** authorized the following executive-level individual(s) to sign information security-related documents on my behalf, as specified below:

Designee Name:		**I authorize this designee to sign the following form(s) on my behalf:** ☐ Designation Letter (SIMM 5330-A) ***Note:* Designee may only sign 5330-A updates within this reporting period.** ☐ Technology Recovery Program Compliance Certification (SIMM 5325-B) ☐ Risk Register and Plan of Action and Milestones (RRPOAM) (5305-C)
Working Title:		
Classification:		
Telephone Number:		
Extension:		
Email Address:		
Designee Signature:		

Designee Name:		**I authorize this designee to sign the following form(s) on my behalf:** ☐ Designation Letter (SIMM 5330-A) ***Note:* Designee may only sign 5330-A updates within this reporting period.** ☐ Technology Recovery Program Compliance Certification (SIMM 5325-B) ☐ Risk Register and Plan of Action and Milestones (RRPOAM) (5305-C)
Working Title:		
Classification:		
Telephone Number:		
Extension:		
Email Address:		
Designee Signature:		

Designee Name:		**I authorize this designee to sign the following form(s) on my behalf:** ☐ Designation Letter (SIMM 5330-A) ***Note:* Designee may only sign 5330-A updates within this reporting period.** ☐ Technology Recovery Program Compliance Certification (SIMM 5325-B) ☐ Risk Register and Plan of Action and Milestones (RRPOAM) (5305-C)
Working Title:		
Classification:		
Telephone Number:		
Extension:		
Email Address:		
Designee Signature:		

SECTION B (Part 1): STATE ENTITY LEVEL DESIGNEES *and* BACK-UP DESIGNEES

Primary Designations	Chief Information Officer	Information Security Officer	Technology Recovery Coordinator	Privacy Program Coordinator
Name *				
Classification *				
Business Mailing Address *				
IMS Code				
Office Phone *				
Extension				
Mobile Phone				
Fax Number				
Direct Email Address *				
Group Email Address				
SOC Email Address *				

Back-up Designations	Chief Information Officer (backup)	Information Security Officer (backup)	Technology Recovery Coordinator (backup)	Privacy Program Coordinator (backup)
Name *				
Classification *				
Business Mailing Address *				
IMS Code				
Office Phone *				
Extension				
Mobile Phone				
Fax Number				
Direct Email Address *				

***Required Field** SOC Email address is required and must follow the standardized naming convention as outlined in the Email Threat Protection Standard (SIMM 5315-A)**

SECTION B (Part 2): AGENCY LEVEL DESIGNEES *and* BACK-UP DESIGNEES

IMPORTANT: Complete this section with the Agency CIO and ISO as outlined in GC 11546.1. If this state entity is or reports to a Cabinet-level Agency within the Executive Branch, the following section must be completed:

Primary Designations	**AGENCY** **Chief Information Officer**	**AGENCY** **Information Security Officer**
Name *		
Classification *		
Business Mailing Address *		
IMS Code		
Office Phone *		
Extension		
Mobile Phone		
Fax Number		
Direct Email Address *		
Group Email Address		
****SOC Email Address ***		

Back-up Designations **(optional)**	**AGENCY** **Chief Information Officer** **(back-up)**	**AGENCY** **Information Security Officer** **(back-up)**
Name		
Classification		
Business Mailing Address		
IMS Code		
Extension		
Office Phone		
Mobile Phone		
Fax Number		
Direct Email Address		

*** Required Field ** SOC Email address is required and must follow the standardized naming convention as outlined in the Email Threat Protection Standard (SIMM 5315-A)**

SECTION C: STATE ENTITY SERVICES & PARTNERSHIPS

List the state entities responsible for **providing** your organization with the services outlined below**.**

Refer to **Appendix A** for the criteria that must be met for a state entity to claim responsibility for a service. **All** listed criteria must be satisfied for a state entity to be recognized as providing that service.

If your state entity is self-supporting any services listed below and does not require assistance from another state entity, please specify your state entity's name; otherwise, please list the state entity responsible for providing that service.

Note: *Only one state entity can claim responsibility for a particular service; however, different entities may support different services. This will help OIS determine who is responsible for the organization's Information Security Program Audit (ISPA) and Independent Security Assessment (ISA).*

Services	State entity Name	Secretary/Director (or equivalent state entity head) Signature of State entity Providing the Service
Active Directory Environment		
Security Boundary		
Policy Boundary		

IMPORTANT:

- The state entity providing the Policy Boundary service will be audited for an ISPA. Entities that receive Policy Boundary support from another state entity will inherit that state entity's California Maturity Metric (CMM) score after an OIS validation.
- If a state entity receives both the Active Directory Environment and Security Boundary services from the same state entity, the ISA responsibility will be assigned to that supporting state entity, and the supported state entity will inherit its CMM and ISA scores.
- OIS will utilize **Appendix B** to categorize each state entity and identify ownership of Roles and Responsibilities for ISAs, ISPAs, and Risk and Compliance activities.

SECTION D: ORGANIZATIONAL CHART

Attach the entity's official organizational chart, which displays the **CIO/ISO** reporting structure**,** as signed by the Director and approved by CalHR. OIS uses this information to, among other things, validate compliance with Government Code Section 11546.1(c).

Appendix A: Service Definitions

If you receive support for any services listed below from another state entity, **all** listed criteria must be met simultaneously and by that single state entity for the service to be considered supported. If the supporting state entity does not meet a criterion at any time, your state entity must document that it is self-supporting the service in **Section D: State entity Services & Partnerships** of this document.

Active Directory Environment:

1. Another state entity hosts and administers the organization's Active Directory.

Security Boundary:

1. Can demonstrate partial or full IT support and patch management for systems within the organization, per SAM 5345.
2. Can demonstrate asset management of all information assets within the organization, per SAM 5305.5 and SAM 5315.3.
3. Can demonstrate and provide full remediation of technical information security gaps and deficiencies within the organization, per SIMM 5305-C and SAM 5305.6-7.
4. Can demonstrate partial or full administration of network infrastructure.
5. Can demonstrate the implementation of all cyber security safeguards.

Policy Boundary:

1. All information security incidents encountered are addressed, remediated, and reported through the proper channels as outlined in SIMM 5340-A, per SIMM 5340 and SAM 5340.3 – 5340.4.
2. All information security policies are developed, maintained, and enforced for the state entity in compliance with SIMM and SAM 5300, including, but not limited to, Privacy Policy Statements (SAM 5310-5310.5), Security Awareness and Privacy Training (SIMM 5320-A, SAM 5320), and an Acceptable Use Policy (SAM 5320.4).
3. The Technology Recovery Plan (TRP) and required supporting materials, including Business Impact Analysis (BIA) and System Security Plans (SSP), are developed, managed, and submitted to OIS for review. The TRP must outline all information technology and business processes for the state entity and establish communication flow and recovery priorities based on impacts, risks, and requirements outlined in SIMM 5325-A and the SAM 5325 series.
4. Information security safeguard gaps are documented and prioritized as part of a Risk Register Plan of Action and Milestones (RRPOAM), per SIMM 5305-C and SAM 5305.6-7.
5. Have the resources and be capable of being assessed for an ISPA.
6. Possess the expertise, resources, and knowledge to accurately and timely represent the state entity's Information Technology capacity. This includes but is not limited to the information security program,

network architecture, systems and critical systems, data houses and processing, and business functions when meeting with CDT directorates.

7. SIMM 5300 compliance documentation is submitted. The following documentation is required when there is an established policy boundary: (Please refer to SIMM 5330-C for reporting schedules):
    - Information Technology Cost Report (SIMM 55-B)
    - Information Technology Cost Report Transmittal (SIMM 55-C)
    - Information Security and Privacy Program Compliance Certification (SIMM 5330-B)
    - Information Security and Privacy Program Compliance Certification (SIMM 5330-F)

Appendix B Legend:

OIS utilizes the table on the next page to categorize each state entity and determine the ownership of roles and responsibilities related to ISAs, ISPAs, and risk and compliance activities. This information is provided to promote transparency.

The state entity is not required to take action on this table when completing this form.

Steward = State entity providing services or support
Client = State entity receiving services or support
Yes/No = You are or are not inheriting a score

🟧	Assessment Responsibilities
🟩	Governance Responsibilities

Appendix B: For OIS Categorization

Classification	Description	ISA	Audit	Policy	Roles	TRP	RRPOAM	Cal-CSIRS
Self-supporting	No services or support from/to any other state entity	Yes	Yes	Self	Self	Self	Self	Self
Self-supporting with Sub-entity	Provides support to the sub-entity in its entirety. The sub-entity is wholly within the host and may have a separate Org Code.	Yes Sub inherits	Yes Sub inherits	Self Sub inherits	Yes Sub inherits	Yes Sub inherits	Yes Sub inherits	Yes Sub inherits
Limited Technical	Provides (steward) or receives (client) support from/to another state entity. • Active Directory Environment • Security Boundary	Steward: receives the ISA. Client: does not receive an ISA and will inherit a score from Steward.	Steward: receives an Audit. Client: receives their own separate Audit.	Self -or- inherits from: Steward -or- Agency	The Steward & Client have their own assigned roles and designees.	Steward & Client have separate TRPs and reporting.	Steward & Client have separate RRPOAMs and reporting.	Steward & Client report separately under their own state entity.
Limited Program	Provides (steward) or receives (client) programmatic support from/to another state entity. • Policy Boundary	Steward: receives an ISA. Client: receives their own separate ISA.	Steward: receives an Audit Client: does not receive an Audit and will inherit a score from the Steward.	Policy inherits from: Steward -or- Agency	Steward is responsible for all client assigned roles.	Steward includes client systems, prioritization, and business functions in their own TRP.	Steward includes all security gaps for client in their RRPOAM	Steward reports for the client but as a separate state entity.
Host/Hosted	All functions provided from/to another state entity, including: • Active Directory Environment • Security Boundary • Policy Boundary	Host: Yes The hosted entity inherits the host's score. The hosted may impact the host's score.	Host: Yes The hosted entity inherits host's score. The hosted may impact the host's score.	Policy inherits from: Host -or- Agency	Host is responsible for all client roles.	Host maintains the hosted entity's TRP.	Host includes all security gaps for the hosted entity in their RRPOAM.	Host reports for the hosted entity under themselves.