State of California

Department of Technology

Designation Letter

Statewide Information Management Manual – 5330-A

April 2026

Table of Contents

Revision History 2
Introduction 3
Purpose 3
Scope 3
Compliance 3
Definitions 4
Designation Letter 4
SECTION A: SECRETARY/DIRECTOR'S SIGNATURE AUTHORITY DESIGNEE(S) 6
SECTION B (Part 1): STATE ENTITY LEVEL DESIGNEES *and* BACK-UP DESIGNEES 7
SECTION B (Part 2): AGENCY LEVEL DESIGNEES *and* BACK-UP DESIGNEES 8
SECTION C: STATE ENTITY SERVICES & PARTNERSHIPS 9
SECTION D: ORGANIZATIONAL CHART 9
Questions 9

Revision 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
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.
Major Update	April 2026	OIS	Simplified Section C: State Entity Services & Partnerships. Removed Appendices.

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 as defined in State Administrative Manual (SAM) 5300.4.

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. Compliance may be reflected in audit findings and maturity scores. Non-compliance will be addressed according to the Office of Information Security Policy Compliance and Enforcement Standard (SIMM 5330-H).

As described in GC Section 11549.3.(f) (2), a state agency as defined in GC Section 11000 that is not under the direct authority of the Governor may adopt and implement this policy voluntarily.

Definitions

OIS utilizes SAM 5300 definitions as well as approved authoritative sources for terms not defined in SAM 5300. For the purposes of SIMM Section 5330-A, the following definitions apply:

Self-supporting - No services or support from/to any other state entity.

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.

Host/Hosted - Functions provided from/to another state entity.

Designation Letter

See following page.

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:** Click or tap to enter a 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 determined in the process described in Section C.

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.

For additional information about this submission, please contact:

Name	ext. Telephone Number	Email

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

Name	Signature	Date

Business Mailing Address	ext. 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

OIS will confer with entities to determine supported roles and services between entities (e.g. host/hosted relationships). If your organization receives support for any services from another state entity, OIS will work with your organization to determine and document support relationships and implications for oversight functions. Based on that determination, OIS will inform your organization of its specific reporting, Information Security Program Audit (ISPA), and Independent Security Assessment (ISA) requirements.

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).

Questions

Questions regarding the completion of this Designation Letter may be sent to:

California Department of Technology

Office of Information Security

security@state.ca.gov