State of California

Department of Technology

Office of Information Security

Designation Letter

SIMM 5330-A

July 2024

REVISION HISTORY

REVISION	DATE OF	OWNER	SUMMARY OF CHANGES
Minor Update	June 2024	OIS	Template and format update, verbiage clarifications made.

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 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 shall certify that the Information Security Officer (ISO) reports to the Chief Information Officer (CIO) through the inclusion of the California Department of Human Resources (CalHR) approved organizational chart, and if the entity gives and/or 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, commissions, and independent and constitutional entities.

Compliance

Government Code Section 11549.3 authorizes 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.

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.

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

DATE: _____

ENTITY NAME: _____

ORG CODE: _____

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 entity relationship type delineated in Attachment D.

SUBJECT: Designation Letter

I, the undersigned, hereby certify that I am the Secretary/Director (*or equivalent head of the state entity*) 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 **Attachment A**. These are executive-level individual(s) authorized to sign specified information security and privacy compliance-related documents on my behalf.

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

I certify that the organizational chart for this state entity is included herein as **Attachment C** and reflects our organization's alignment with Government Code Section 11546.1(c) (e.g.,

ISO reports to the CIO within our organization).

I hereby further certify if this state entity provides and/or receives partial or full support for the CIO Designation, ISO Designation, Technology Recovery Management, Incident Management, Privacy Program Management, and/or Information Security & Risk Management functions or if this state entity is fully self-sufficient (as defined in **Attachments D**).

IMPORTANT: If this entity reports to a Cabinet-level Agency within the Executive Branch, a copy of this Designation Letter must be provided to the AIO and/or AISO.

For additional information about this submission, please contact:

Name	Telephone Number	Email

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

Name	Signature	Date

Business Mailing Address	Telephone Number	Email

For detailed instructions on how to complete this form, refer to the Designation Letter Instructions (SIMM 5330-D)

ATTACHMENT 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)
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.**
Working Title:		
Classification:		
Telephone Number:		
Extension:		
Email Address:		

Designee Signature:		☐ Technology Recovery Program Compliance Certification (SIMM 5325-B) ☐ Risk Register and Plan of Action and Milestones (RRPOAM)

Designee Name:		**I authorize this designee to sign the following form(s) on my behalf:** ☐ Designation Letter (SIMM 5330-A) ***<u>Note</u>: 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)
Working Title:		
Classification:		
Telephone Number:		
Extension:		
Email Address:		
Designee Signature:		

ATTACHMENT 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)**

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

IMPORTANT: If this 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)**

ATTACHMENT C: 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).

ATTACHMENT D: ENTITY PARTNERSHIP TYPES

Please select the relevant option and submit the corresponding compliance form(s) according to your entity-partner relationship(s). Within the same entity partnership, a single entity can fall under multiple categories, such as Options 2, 3, or 4.

☐ **OPTION 1 - Self-Supported:** The entity does not receive support from or provide support to any other state entity or agency.

- Required Additional Actions: No further action is necessary.

☐ **OPTION 2 - Limited IT Support:** An entity relationship where limited IT support is agreed upon between two entities. This can include but is not limited to individual or multiple system support, personnel hardware agreements, service desk/help desk support, data center services, Security Operations Center as a Service, etc.

- Required Additional Actions: The Technology Recovery Coordinator (TRP) must complete the SIMM 5325-A—Technology Recovery Plan Instructions Section 7 for the Data Center Services requirements.

☐ **OPTION 3 - Host/Hosted:** This entity is part of a host/hosted partnership with another state entity.

- Required Additional Actions: Complete and submit the SIMM 5330-E – Host/Hosted Self-Certification form.

☐ **OPTION 4 - Supported Roles and Functions:** This entity provides/receives support to/from another entity for compliance-based roles and functions.

- Required Additional Actions: Complete and submit the SIMM 5330-G - Supported Program Agreement form.

☐ **OPTION 5 - Fully Supported Entity:** This entity is fully supported (including all non-IT business

units) by another state entity. Submitting your supporting entities' compliance documents is acceptable if the supporting state entity has documented the inclusion of the supported entity in its strategy, communications, and system risk requirement considerations in their Business Continuity Plan, Technology Recovery Plan, Privacy Documentation, POAM, and other required compliance documentation.

- Required Additional Actions: Complete **BOTH** SIMM 5330-E- Host/Hosted Self-Certification and SIMM 5330-G Supported Program Agreement forms.

IMPORTANT:

A lack of submitted signed documentation will result in non-compliance.

If your entity provides support to and/or receives support from multiple entities, please submit a separate SIMM 5330-E and SIMM 5330-G for each entity that provides support to your entity or receives support from your entity.

REVISION HISTORY

REVISION	DATE OF	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.