State of California

Department of Technology

Designation Letter Instructions

Statewide Information Management Manual – 5330-D

May 2025

Table of Contents

Document History 2

Introduction 3

Purpose 3

Scope 3

Compliance 3

Form Completion 4

Digital Signature Guidelines 4

Director/Secretary Certification Page 5

Section A: Secretary/Director's Signature Authority Designee(s) 6

Section B (Part 1 &2): State Entity Level Primary Designees and Backup Designees. 7

Section C: State Entity Services & Partnerships 8

Appendix A: Service Definitions 8

Appendix B: OIS Categorization 9

Form Submission 9

References 9

Document History

Revision	Date of Release	Owner	Summary of Changes
Initial Release	March 2019	Office of Information Security (OIS)	
Update	January 2020	OIS	Updated format. Removed Parent/Child sections, creating new Host/Hosted Self-Certification (SIMM 5330-E). Added AIO/AISO back-up option. Added Digital Signature guidelines.
Minor update	May 2025	OIS	Aligning with major update to SIMM 5330-A, Designation Letter.

Introduction

Purpose

Each state entity shall validate compliance with statewide information security policy, standards, and procedures as set forth in the State Administrative Manual (SAM) chapter 5330.

Per SAM 5330.2, all state entities must submit the Designation Letter (Statewide Information Management Manual (SIMM) 5330-A) 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 SIMM 5330-A, the state entity head shall designate staff as designated signers and the point 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) by including the organizational chart and stating whether the state entity provides and/or receives support from another entity.

The state entity head must sign the annual SIMM 5330-A submission; however, updated SIMM 5330-A documents submitted within the same reporting period may be signed by the SIMM 5330-A Signature Authority Designee.

Scope

This standard applies to all California state entities, including agencies, 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 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 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).

Form Completion

Digital Signature Guidelines

If a state entity elects to use a digital signature on the compliance submissions, the entity must meet the following security guidelines.

Must be compliant with:

- SAM 4983, 5100 & 5300
- NIST Special Publication 800-53 control framework
- California Government Code §16.5 & California Code of Regulations, Digital Signatures, Title 2. Administration, Division 7. Secretary of State, Chapter 10 Digital Signatures §22000 – §22005
- Federal Information Processing Standard (FIPS) 186-4 “Specifications for the DIGITAL SIGNATURE STANDARD (DSS)”
- The California Uniform Electronic Transactions Act, California Civil Code §1633.1 et seq
- Section 508
- Requires “electronic” signature solution methodologies to incorporate, at a minimum, level 2 or higher identity assurance technical requirements for individual signers, as specified in NIST SP 800-63 -2 “Electronic Authentication Guideline.”

- Requires signature (electronic and digital) solutions to have security procedures for the secure storage, retrieval, and retention (based on subscriber retention timeframe requirements) of signed instruments, documents, transactions, or processes. Hashing of signed instruments, documents, transactions, or processes shall comply with the specifications and guidance contained in FIPS 180-4 Secure Hash Standard (SHS), FIPS 140-3 “Security Requirements for Cryptographic Modules;” and NIST SP 800-107 (Rev.1) “Recommendation for Applications Using Approved Hash Algorithms.”
- Digital signatures and all associated data must be saved within the continental US in a NIST-compliant solution.

Director/Secretary Certification Page

This section provides Director/Secretary certification for the following items:

- They are the Secretary/Director (or equivalent head of the state entity) for the state entity they submit on behalf of.
- The state entity is compliant with the requirements set forth in State Policy (SAM Chapter 5300).
- They approve and authorize signature authority to specific executive-level designees and approve and authorize selected designees to fulfill security and privacy requirements for the state entity.
- The organizational chart for this state entity is included in the submission and reflects the organization’s required alignment of the reporting structure between the CIO and ISO.
- The state entity is self-sufficient *or* if the entity receives partial or full support for the CIO Designation, ISO Designation, Technology Recovery Management, Incident Management, Privacy Program Management, and/or Security & Risk Management functions.
- Provides direct contact information for the Secretary/Director of the state entity.

Step-by-Step Instructions:

1. Enter the date of the submission.
2. Enter the full name of the state entity.
3. Enter the official organizational code, as identified in the Department of Finance Uniform Code Manual.
4. Select the appropriate GOV code for compliance reporting, 11546.1 or 11000.
5. Enter the appropriate compliance report due date as defined by SIMM 5330-C, Information Security Compliance Reporting Schedule.
6. Enter contact information of who to contact if there are questions about SIMM 5330-A, this typically is the designated Information Security Officer.
7. Provide the name, mailing address, telephone number, and email address for the current Secretary/Director (or equivalent to the head of the state entity).

On the mandatory annual submission, **the state entity head must sign the bottom of page one**. This certifies that the entity head agrees to the information submitted within SIMM 5330-A, however updated SIMM 5330-A documents submitted within the same reporting period may be signed by the SIMM 5330-A Signature Authority Designee.

Section A: Secretary/Director's Signature Authority Designee(s)

This section provides Director/Secretary authorization for the following items:

- Appointment of designees authorized to sign specified compliance-related documents on behalf of the state entity's director or secretary.
- Requires that the selected designees sign the form to certify awareness of the responsibilities assigned to them by the entity head.

NOTE: The Director/Secretary must sign the annual submission of SIMM 5330-A. The selected designees must be executive-level individuals (s) and will only be authorized to sign updated SIMM 5330-A documents submitted within the same reporting period.

Step-by-Step Instructions:

1. The entity head must select one of the options at the top of the page to acknowledge if they are designating individuals to sign specified compliance documents on their behalf.
2. In the appropriate boxes, enter the designee's name, working title, classification, telephone number, and email address.
3. Select the forms each specific designee is authorized to sign on behalf of the entity head.
4. The designee must sign this page.

Additional copies of Section A may be submitted if needed.

Section B (Part 1 &2): State Entity Level Primary Designees and Backup Designees

This section provides Director/Secretary authorization for the following items:

- Appointment of designees that are authorized to fulfill the security and privacy requirements for the state entity.

Step-by-Step Instructions:

1. Complete ALL required fields (*) for the following designee appointments on Attachment B (Part 1 &2):
    - 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
    - Designated back-ups for all roles

2. Submit a group email address if you would like additional Information Security staff to receive communications from OIS (not required).
3. The Security Operations Center (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

This section provides Director/Secretary certification for the following items:

- Certifies if the state entity is self-supporting or receives support from another state entity.

Step-by-Step Instructions:

1. List the state entity or entities responsible for **providing** your organization with the services identified below. Enter the name of your state entity If the entity is self-supported for the identified services and does not receive assistance from another state entity.
    - Active Directory Environment
    - Security Boundary
    - Policy Boundary

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), Independent Security Assessment (ISA), and Risk and Compliance activities.

Appendix A: Service Definitions

Appendix A is a resource that outlines the criteria a single state entity must meet **simultaneously** for the service to be considered supported. Please note that this resource does not include fillable fields and does not need to be submitted to OIS.

Appendix B: OIS Categorization

OIS uses the table in Appendix B to categorize each state entity and clarify the ownership of roles and responsibilities associated with ISAs, ISPAs, and risk and compliance activities. This information aims to enhance transparency. Please note that Appendix B does not include fillable fields and does not need to be submitted to OIS.

Form Submission

Step-by-Step Instructions:

Upon completing SIMM 5330-A, submit the form to OIS through the Secure Automated File Exchange (SAFE). If your entity needs assistance with SAFE access, contact OIS at security@state.ca.gov.

References

- State Administrative Manual (SAM)
- Statewide Information Management Manual (SIMM)
- Department of Finance Uniform Code Manual