State of California

California Department of Technology

Office of Information Security

Designation Letter Instructions

SIMM 5330-D

January 2020

REVISION HISTORY

REVISION	DATE OF	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.

TABLE OF CONTENTS

INTRODUCTION

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 (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 the SIMM 5330-A, the state entity head shall designate staff to be designated signers and the point of contacts to fulfill the security and privacy requirements for the state entity (this is outlined in the SIMM 5330-A, attachments A and B).

In addition to the designee assignments, within the SIMM 5330-A the state entity head shall certify that the ISO reports to the 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.

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

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.

For details on the California Department of Technology (CDT) eSignature/Digital Signature policy, please refer to the CDT policy: https://cdt.ca.gov/services/vhss-esignature/.

DIRECTOR/SECRETARY CERTIFICATION PAGE

Purpose:

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

- That they are the Secretary/Director (or equivalent head of the state entity) for the state entity they are submitting on behalf of.
- That their entity is in compliance with the requirements set forth in State Policy (SAM Chapter 5300).
- That 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.
- Certifies that 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.
- Certifies if the state entity is self-sufficient *or* if the 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 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. Enter the contact information of who to contact if there are questions about the SIMM 5330-A, this typically is the designated Information Security Officer.
5. Provide the name, mailing address, telephone number, and email address for the current Secretary/Director (or equivalent to the head of the state entity).
6. 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 the 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.

ATTACHMENT A – SECRETARY/DIRECTOR'S SIGNATURE AUTHORITY DESIGNEE(S)

Purpose:

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

- Appointment of designees that are authorized to sign specified compliance related documents on behalf of the Director/Secretary of the state entity.
- 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 the SIMM 5330-A.The selected designees must be executive level individual(s) and will only be authorized to sign updated SIMM 5330-A documents that are 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. Enter designee name, working title, classification, telephone number, and email address in the appropriate boxes.
3. Select the forms that each specific designee is authorized to sign on behalf of the entity head.
4. Designee must sign this page.
5. Additional copies of Attachment A may be submitted if needed.

ATTACHMENT B (Part 1 &2) – SECRETARY/DIRECTOR'S PRIMARY and BACK-UP DESIGNEES

Purpose:

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:

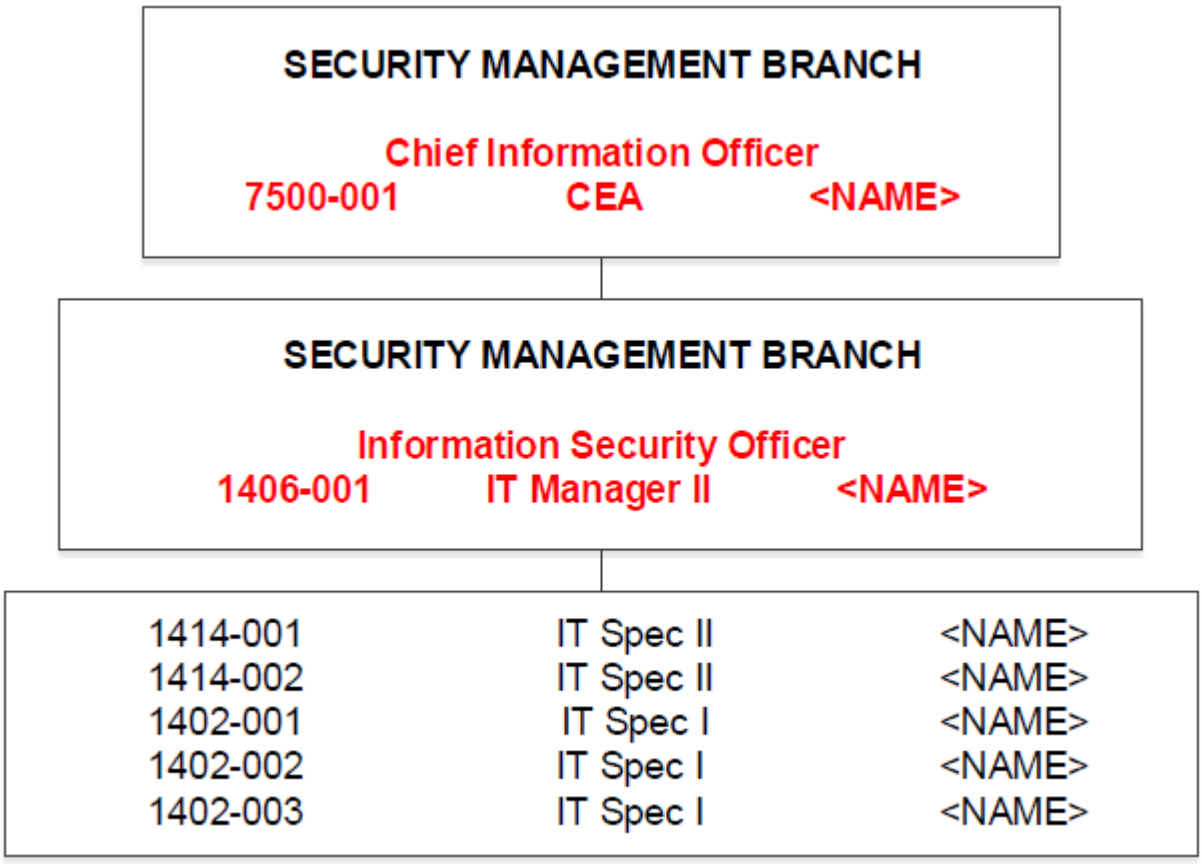
1. Complete ALL required fields (*) for the following designee appointments on Attachment B (Part 1 &2):
    - Agency Chief Information Officer (AIO/ACIO)
    - Agency Information Security Officer (AISO)
    - Chief Information Officer (CIO)
    - Information Security Officer (ISO)
    - Technology Recovery 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 Email Threat Protection Standard (SIMM 5315-A).

ATTACHMENT C – ORGANIZATIONAL CHART

Step-by-Step Instructions:

1. Submit the organizational chart for the state entity which displays the CIO/ISO reporting structure and is the official organizational chart 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) (see example below).

   NOTE: If you are a supported entity and your CIO or ISO report to another entity, you may need to include a functional organizational chart along with the official CalHR organizational chart for your entity.



ATTACHMENT D (Part 1) - SUPPORTED ROLES AND FUNCTIONS

Purpose:

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

- Certifies **IF** the state entity receives support from *and/or* provides support to another state entity.

Step-by-Step Instructions:

1. Select the appropriate options contained within this section:
    - This state entity **DOES NOT RECEIVE or PROVIDE SUPPORT** to any other state entities.
    - This state entity **PROVIDES SUPPORT**, and agrees to fully or partially support roles and functions for another state entity. In conjunction with the roles and functions that are being supported, the state entity providing support agrees to be responsible for specified compliance and certification for another state entity. **If this option is selected, follow instructions and complete Attachment D (Part 2).**
    - This state entity **RECEIVES SUPPORT**, full or partial, within the area of supported roles and functions, from another state entity. In conjunction with the roles and functions that are being supported, this state entity also receives support in the area of compliance and certification from another state entity. **If this option is selected, follow instructions and complete Attachment D (Part 3).**

IMPORTANT:

- All state entities, whether or not they are a supported entity, must comply with all mandatory compliance reporting requirements. Separate compliance forms are required for **ALL** state entities, multiple entities cannot combine compliance documents onto one form.
- If an entity provides support to another entity, they may also provide assistance with the supported compliance reporting related tasks.
- If a department provides support to or receives support from another entity, both entities will need to complete "Attachment D (Part 2 and/or 3)" on their individual SIMM 5330-A. If the department receives support, the Director/Secretary will need to sign "Attachment D (Part 3)".

ATTACHMENT D (Part 2) - PARTIAL *OR* FULLY SUPPORTED ROLES AND FUNCTIONS PROVIDED TO ANOTHER ENTITY

Purpose:

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

- Certifies that your state entity **PROVIDES SUPPORT** to another state entity and agrees to fully or partially support functions consisting of one or more of the areas selected in the "Functions Supported" section. If partially supported, clearly define functions supported.

- In conjunction with the functions that are being supported, this section certifies that your state entity **PROVIDES SUPPORT** and agrees to be responsible for the selected areas within the "Compliance and Certification Supported" section.

Step-by-Step Instructions:

1. List the name and organizational code of the state entity(s) that your state entity provides support to.

2. Check all boxes that apply within the "Roles & Functions Supported" section, identifying if the support given is partial or full support.

3. Check all boxes that apply within the "Compliance and Certification Supported" section.

4. If partial support is provided, describe in detail the function(s) that your state entity supports.

5. Additional copies of Attachment D may be submitted if needed.

ATTACHMENT D (Part 3) - PARTIAL *OR* FULLY SUPPORTED ROLES AND FUNCTIONS RECEIVED FROM ANOTHER ENTITY

Purpose:

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

- Certifies that your state entity **RECEIVES SUPPORT** from another state entity for functions consisting of one or more of the following areas selected in the "Functions Supported" section. If partially supported, clearly define functions supported.

- In conjunction with the functions that are being supported, this section certifies that your state entity **RECEIVES SUPPORT** and acknowledges that the state entity providing support will be responsible for the selected areas within the "Compliance and Certification Supported" section.

- If your department receives support from another entity, your Director/Secretary will need to sign the bottom of "Attachment D (Part 3)".

  This is required to state that they certify that they are the Secretary/Director (or equivalent head of the state entity) of the entity which is receiving support and that they acknowledge that they agree to the listed functions, compliance, and certification to be supported by the listed state entity.

  Additionally, they understand that they must communicate with the state entity providing support to ensure that they continue to have a full understanding of the current status of the security and risk management strategy in place to protect their information and information systems, and to allow them to make informed judgments and decisions about the risk for their state entity.

Step-by-Step Instructions:

1. List the name and organizational code of the state entity that your state entity receives support from.

2. Check all boxes that apply within the "Roles & Functions Supported" section, identifying if the support given is partial or full support.

3. Check all boxes that apply within the "Compliance and Certification Supported" section.

4. If partial support is provided, describe in detail the function(s) that your state entity receives support with.

5. The entity head of the entity receiving support must sign and date the bottom of this form.

6. Additional copies of Attachment D may be submitted if needed.

SUBMISSION

Step-by-Step Instructions:

Upon completion of the SIMM 5330-A, submit form to OIS through one of the following methods:

- Mail to: Office of Information Security
  Attention: Compliance Reporting
  PO Box 1810, MS Y-01
  Rancho Cordova, CA 95741
- Deliver to: 10860 Gold Center Drive
  Rancho Cordova, CA 95670
  (2nd Floor Security Desk)
- Email to: security@state.ca.gov
- Electronic submission: Submit through SAFE (contact our office if your entity needs assistance with SAFE access)

IMPORTANT: If this agency 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 further assistance please contact our office at security@state.ca.gov.