# State of California California Department of Technology

**Office of Information Security**

**Technology Recovery Program Certification**

# SIMM 5325-B

**March 2023**

**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **REVISION** | **DATE OF**  **RELEASE** | **OWNER** | **SUMMARY OF CHANGES** |
| **Initial Release** | **November 2009** | **Office of Information**  **Security and Privacy Protection** |  |
| **Minor Update** | **September 2013** | **California Information Security Office (CISO)** | **SIMM number change, change “agency” to “state entity”, change “disaster recovery” to “technology recovery”, and change references to other related SIMM documents. Update links to CalOES and the Executive Order.** |
| **Minor Update** | **August 2015** | **California Information Security Office (CISO)** | **Changed reference to “remediation plan” to Plan of**  **Action and Milestone (POAM).** |
| **Minor Update** | **January 2018** | **Office of Information Security (OIS)** | **Office name/address change; Removal of biennial submission option.** |
| **Minor Update** | **June 2018** | **OIS** | **Incorporate AB1841: Inclusion of critical infrastructure controls and critical infrastructure information.** |
| **Minor Update** | **March 2019** | **OIS** | **Clarify Technology System(s) Inventory Category instructions; Added Confidential Statement** |
| **Minor Update** | **March 2023** | **OIS** | **Formatting changes. Section alignment with 5325-A and TRP Review Report document. Cross reference language added.** |

Office of Information Security

Technology Recovery Program Certification [ SIMM 5325-B]

**Confidential and Exempt - Government Code Section 6254.19**

March 2023

**TO:** Office of Information Security, **DATE:** {submission\_date}

California Department of Technology Attn: Security Compliance Reporting

P.O. Box 1810, Mail Stop Y-01 Rancho Cordova, CA 95741

## ENTITY NAME: {entity\_name}

**ORG CODE:**  {org\_code}(As identified in the [Uniform Codes Manual)](https://dof.ca.gov/accounting/accounting-policies-and-procedures/accounting-policies-and-procedures-uniform-codes-manual/)

Separate compliance forms are required for ALL state entities regardless if they meet the criteria for a Host/Hosted relationship submission. The SIMM 5325-B should be submitted as a standalone artifact from the Technology Recovery Plan.

## SUBJECT: Technology Recovery Program Certification

I, the undersigned, hereby certify that I am the Secretary/Director (*or equivalent head of the state entit*y) or the Secretary/Director’s designee for the above referenced state entity. I certify as follows (*select one option below*):

{compliance\_full\_checkbox} My state entity is in full compliance with the Technology Recovery Management Program requirements set forth in State Policy, [State Administrative Manual (SAM) Section 5325](http://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5325.pdf). As required in [SAM 5330.2](http://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5330.2.pdf), I submit the attached Technology Recovery Plan (TRP) which (*select one):*

{trp\_follows\_simm\_checkbox} Follows the State Information Management Manual (SIMM 5325-A) format.

{trp\_does\_not\_follow\_checkbox} Does NOT follow the SIMM 5325-A format, but we have included the required cross reference sheet (attached).

{compliance\_not\_checkbox} My state entity is NOT in full compliance with the Technology Recovery Management Program requirements, but has a comprehensive plan to achieve full compliance by {compliance\_target\_date}. I understand and accept the risk associated with the gaps in our current program, and have attached a Plan of Action and Milestones (SIMM 5305-C) that identifies the non-compliant components along with timelines indicating when our state entity will meet these requirements.

## NOTE: The TRP typically contains confidential information which must be protected. As such, delivery must be performed in a secure manner.

I, hereby further certify my entity’s IT system inventory is as follows:

|  |  |
| --- | --- |
| **Technology System(s) Inventory Category** | **Enter Number(s)** |
| Mission Critical Information Technology (IT) Systems | {mission\_critical\_systems} |
| State Critical IT Systems | {state\_critical\_systems} |
| Other IT Systems | {other\_systems} |
| Public Facing Web Applications | {web\_applications} |
| Critical Infrastructure Systems | {critical\_infrastructure} |
| Total Number of IT Systems For Your State Entity  The total on this line should reflect your actual count not just a summation of the above table. | {total\_systems} |

Attached is additional explanation or comments as needed. For additional information about this submission please contact:

{contact\_name} {contact\_phone} {contact\_email}

Name Telephone Number E-mail

{entity\_head\_name} {signature\_date}

Printed Name of Entity Head or Designee

Signature of Entity Head or Designee

Date

Technology Recovery Plan Cross Reference Tool

The intent of this portion of the document is to serve as a cross-reference mapping checklist, when the plan is not arranged in the same order that is outlined in SIMM 5325-A.

Most plans submitted to the OIS are not organized in the same order outlined in the instructions, as they are designed for entity staff usability in a crisis versus OIS compliance; thus, the cross-reference mapping tool facilitates both an entity’s compliance check prior to submission, as well as our ability to locate required items during our compliance review.

Note: This cross-reference mapping checklist uses abbreviated descriptions not the complete detail provided in the instructional pages of SIMM 5325-A and has a place for the page number so that an entity can indicate which section and page of the TRP the required items can be located in. Some entities opt to create their own cover sheets, and others have detailed Table of Contents that provide a mapping for purposes of our review.

|  |  |  |  |
| --- | --- | --- | --- |
| **Required elements to be included in an State Entity Technology Recovery Plan** | | **Page Number** | **Issues/Comments** |
| **1** | **Minimum TRP Requirements** | | |
| 1.0 | State Entity Administrative Information | | |
|  | 1.1 Executive summary for structure of  plan | {page\_1\_1} | {comment\_1\_1} |
|  | 1.2 State entity mission, include organization charts, managerial and  technical environment | {page\_1\_2} | {comment\_1\_2} |
|  | 1.3 List state entities that are included in  the recovery plan | {page\_1\_3} | {comment\_1\_3} |
|  | 1.4 Communication Strategy | {page\_1\_4} | {comment\_1\_4} |
|  | 1.5 List state entities that provide services required in the recovery  plan (i.e., SCO, DGS, CDT) | {page\_1\_5} | {comment\_1\_5} |
| 2.0 | Critical Business Functions/Applications | | |
|  | 2.1 List and include description of Critical Business Functions, description of functions, maximum accepted outage and system supporting each function identified as critical. | {page\_2\_1} | {comment\_2\_1} |
|  | 2.2 Approach used to determine  recovery priorities | {page\_2\_2} | {comment\_2\_2} |

|  |  |  |  |
| --- | --- | --- | --- |
| **Required elements to be included in an State Entity Technology Recovery Plan** | | **Page Number** | **Issues/Comments** |
| 3.0 | Critical Infrastructure, systems,  information and controls |  |  |
|  | 3.1 List and include description  of critical infrastructure, | {page\_3\_1} | {comment\_3\_1} |
|  | 3.2 Approach used to determine  recovery priorities | {page\_3\_2} | {comment\_3\_2} |
| 4.0 | Recovery Strategy | | |
|  | 4.1 Description of plan to be  implemented based on severity | {page\_4\_1} | {comment\_4\_1} |
|  | 4.2 Description of recovery strategies | {page\_4\_2} | {comment\_4\_2} |
|  | 4.3 Incident Response and Disaster Recovery strategy interaction | {page\_4\_3} | {comment\_4\_3} |
|  | 4.4 Alternate recovery site details | {page\_4\_4} | {comment\_4\_4} |
| 5.0 | Backup and Offsite Storage | | |
|  | 5.1 Backup and retention schedules and  procedures | {page\_5\_1} | {comment\_5\_1} |
|  | 5.2 Detailed procedures (hardware, software, backup and retention schedules, off-site storage, contacts,  authorized personnel for retrieval) | {page\_5\_2} | {comment\_5\_2} |
| 6.0 | Technology Recovery Procedures | | |
|  | 6.1 Documented procedures for an  orderly restoration | {page\_6\_1} | {comment\_6\_1} |
|  | 6.2 Documented procedures for timely restoration (to meet maximum  outage period) | {page\_6\_2} | {comment\_6\_2} |
|  | 6.3 Step-by-step instructions for  recovery teams | {page\_6\_3} | {comment\_6\_3} |
|  | 6.4 Enough detail for new team members or an emergency response team | {page\_6\_4} | {comment\_6\_4} |
| 7.0 | Data Center Services | | |
|  | 7.1 Data center used and expected services | {page\_7\_1} | {comment\_7\_1} |
|  | 7.2 Interagency agreements, MOUs,  contracts | {page\_7\_2} | {comment\_7\_2} |
|  | 7.3 Procedures for special coordination | {page\_7\_3} | {comment\_7\_3} |

|  |  |  |  |
| --- | --- | --- | --- |
| **Required elements to be included in an State Entity Technology Recovery Plan** | | **Page Number** | **Issues/Comments** |
| 8.0 | Resource Requirements | | |
|  | 8.1 Comprehensive list (equipment, space, telecommunications, data software); hard-copy references (forms/procedures); personnel  required for recovery | {page\_8\_1} | {comment\_8\_1} |
|  | 8.2 Identification of resources to be  available for alternate site | {page\_8\_2} | {comment\_8\_2} |
| 9.0 | Assignment of Responsibility | | |
|  | 9.1 Management and personnel  assignments | {page\_9\_1} | {comment\_9\_1} |
| 10.0 | Contact Information | | |
|  | 10.1 Personnel contact lists | {page\_10\_1} | {comment\_10\_1} |
|  | 10.2 Vendor, other entities, and  outside resources list | {page\_10\_2} | {comment\_10\_2} |
| 11.0 | Testing |  |  |
|  | 11.1 Description of annual test(s) performed, including how the test(s) were conducted and yearly exercise calendar. Examples of testing may include tabletop exercises, data recovery testing, unplanned outage, and/or full plan testing | {page\_11\_1} | {comment\_11\_1} |
| **2** | **Supplemental TRP Requirements**  Required for state entities that do not have a [Continuity Plan](https://www.caloes.ca.gov/office-of-the-director/operations/planning-preparedness-prevention/planning-preparedness/continuity-planning/) as required by [Executive Order S-04-06](https://www.caloes.ca.gov/wp-content/uploads/Preparedness/Documents/S-04-06-Executive-Order.pdf). | | |
| 1.0 | Damage Recognition and Assessment | | |
|  | 1.1 Emergency response | {page\_supp\_1\_1} | {comment\_supp\_1\_1} |
|  | 1.2 Damage assessment | {page\_supp\_1\_2} | {comment\_supp\_1\_2} |
| 2.0 | Mobilization of Personnel | | |
|  | 2.1 Detailed responsibilities of personnel  and management | {page\_supp\_2\_1} | {comment\_supp\_2\_1} |
| 3.0 | Primary Site Restoration and Relocation | | |
|  | 3.1 Detailed procedures after recovery  process is complete | {page\_supp\_3\_1} | {comment\_supp\_3\_1} |
| **3** | **Appendices** | | |
|  |  | {page\_appendices} | {comment\_appendices} |