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.

TO: Office of Information Security,   **DATE:** _____
            California Department of Technology
            Attn: Security Compliance Reporting
            P.O. Box 1810, Mail Stop Y-01
            Rancho Cordova, CA 95741

ENTITY NAME: _____

ORG CODE: _____ (As identified in the 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 entity*) or the Secretary/Director's designee for the above referenced state entity. I certify as follows (*select one option below*):

☐ 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. As required in SAM 5330.2, I submit the attached Technology Recovery Plan (TRP) which (*select one):*

      ☐ Follows the State Information Management Manual (SIMM 5325-A) format.

      ☐ Does NOT follow the SIMM 5325-A format, but we have included the required cross reference sheet (attached).

☐ 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 _____ . 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	
State Critical IT Systems	
Other IT Systems	
Public Facing Web Applications	
Critical Infrastructure Systems	
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.	

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

_____

Name   Telephone Number   E-mail

_____

Printed Name of Entity Head or   Signature of Entity Head or   Date
Designee   Designee

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		
1.2 State entity mission, include organization charts, managerial and technical environment		
1.3 List state entities that are included in the recovery plan		
1.4 Communication Strategy		
1.5 List state entities that provide services required in the recovery plan (i.e., SCO, DGS, CDT)		
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.		
2.2 Approach used to determine recovery priorities		

Office of Information Security
Technology Recovery Program Certification
[SIMM 5325-B]
Confidential and Exempt - Government Code Section 6254.19

3

March 2023

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,		
3.2 Approach used to determine recovery priorities		
4.0 Recovery Strategy		
4.1 Description of plan to be implemented based on severity		
4.2 Description of recovery strategies		
4.3 Incident Response and Disaster Recovery strategy interaction		
4.4 Alternate recovery site details		
5.0 Backup and Offsite Storage		
5.1 Backup and retention schedules and procedures		
5.2 Detailed procedures (hardware, software, backup and retention schedules, off-site storage, contacts, authorized personnel for retrieval)		
6.0 Technology Recovery Procedures		
6.1 Documented procedures for an orderly restoration		
6.2 Documented procedures for timely restoration (to meet maximum outage period)		
6.3 Step-by-step instructions for recovery teams		
6.4 Enough detail for new team members or an emergency response team		
7.0 Data Center Services		
7.1 Data center used and expected services		
7.2 Interagency agreements, MOUs, contracts		
7.3 Procedures for special coordination		

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		
	8.2 Identification of resources to be available for alternate site		
9.0	Assignment of Responsibility		
	9.1 Management and personnel assignments		
10.0	Contact Information		
	10.1 Personnel contact lists		
	10.2 Vendor, other entities, and outside resources list		
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		
2	**Supplemental TRP Requirements** Required for state entities that do not have a Continuity Plan as required by Executive Order S-04-06.		
1.0	Damage Recognition and Assessment		
	1.1 Emergency response		
	1.2 Damage assessment		
2.0	Mobilization of Personnel		
	2.1 Detailed responsibilities of personnel and management		
3.0	Primary Site Restoration and Relocation		
	3.1 Detailed procedures after recovery process is complete		
3	**Appendices**		

Office of Information Security
Technology Recovery Program Certification
[SIMM 5325-B]
Confidential and Exempt - Government Code Section 6254.19

5

March 2023