CALIFORNIA TECHNOLOGY AGENCY # TECHNOLOGY LETTER	NUMBER: **TL 12-10**	DATE ISSUED: **AUGUST 8, 2012**
SUBJECT: **STREAMLINE SECURITY COMPLIANCE FORMS** Incorporate SIMM 70D requirement into SIMM 70B, and SIMM 70E into SIMM 70C	REFERENCES: Government Code 11549.3 State Administrative Manual Section 5360.1 Statewide Information Management Manual (SIMM) Section 70 IT Policy Letter 10-03	

BACKGROUND

The California Office of Information Security initiated several reporting forms as a way for agencies and departments to certify compliance with various privacy and security requirements. Compliance reporting forms include SIMM 70A, 70B, 70C, 70D, and 70E. Some of these forms are similar in nature and can be combined to reduce redundancy.

PURPOSE AND DESCRIPTION

The purpose of this Technology Letter (TL) is to communicate the rescission of two compliance forms (SIMM 70D and SIMM 70E) and the incorporation of content from these forms into two other compliance forms (SIMM 70B and SIMM 70C, respectively). This streamlined reporting process is part of an ongoing review to improve the state's IT program and security processes to ensure they meet their intended purpose in the most efficient manner.

PROCESS

Agencies and departments will be required to complete the two updated forms as described below. Although two SIMM compliance forms are being eliminated, the purpose of each is incorporated in the declaration of compliance into two other forms. The updated forms are as follows:

- Updated Form SIMM 70 B combines SIMM 70 D Disaster Recovery Plan (Complete) and SIMM 70 B Disaster Recovery Plan Certification (No-Change).
- Updated Form SIMM 70 C combines SIMM 70 E Agency Telework and Remote Access Security Compliance Certification and SIMM 70 C Agency Risk Management and Privacy Program Compliance Certification.

All other compliance reporting requirements remain unchanged. Agencies and departments should refer to the Schedule of Required Security Reporting Activities for applicable forms and procedures.

QUESTIONS

Questions should be directed to Michele Robinson, Chief Deputy Director, Office of Information Security, at (916)445-5239 or Michele.Robinson@state.ca.gov.

SIGNATURE

/s/

Carlos Ramos, Secretary
California Technology Agency

STATE ADMINISTRATIVE MANUAL EXCERPTS

[Note: Text to be deleted is shown in strikethrough; text to be added is underlined.]

5340 ACCESS CONTROL
(Revised ~~06/10~~ XX/12)

Agency management is responsible for ensuring the appropriate physical, technical, and administrative controls are in place to support proper access to agency information assets. These controls must be based on both business and security requirements to prevent and detect unauthorized access, and must, at a minimum, include the following controls

1. Mobile, telework, and remote access controls include, but are not limited to the following:

    a. Compliance with the Telework and Remote Access Security Standard (SIMM 66A).

    ~~b. Certifying compliance with the Telework and Remote Access Security Standard (SIMM 66A) by submission of the Agency Telework and Remote Access Security Compliance Certification (SIMM 70E).~~

    ~~c.~~ b. Identifying computing systems that allow dial-up communication or Internet access to sensitive or confidential information, and information necessary for the support of agency critical applications.

    ~~d.~~ c. Periodically changing dial-up access telephone numbers.

    ~~e.~~ d. Auditing usage of dial-up communications and Internet access for security violations.

5355.2 AGENCY DISASTER RECOVERY PLAN
(Revised ~~10/09~~ XX/12)

Each state agency (including each state data center) must maintain a Disaster Recovery Plan (DRP) identifying the computer applications that are critical to agency operations, the information assets that are necessary for those applications, and the agency's plans for resuming operations following an unplanned disruption of those applications.

Each agency that employs the services of a state data center must develop an understanding of the existing service level agreement for recovery services, and its recovery plan must document the data center services that will be required during recovery.

Each agency must keep its DRP up-to-date and provide annual documentation for those updates to the Office. The annual requirements are:

1. Each agency must file a copy of its DRP and the Agency Disaster Recovery ~~Plan Transmittal Letter~~ Program Certification (SIMM Section 70~~D~~B) with the Office, in accordance with the Agency Disaster Recovery Plan Submission Schedule.

2. If the agency employs the services of a state data center, it must also provide the data center with either a full copy or a subset of its plan, containing enough information for the data center to recover the agency's systems and/or data.

~~3. An Agency Disaster Recovery Plan Certification (SIMM Section 70B) may be filed in place of a full DRP if both of the following conditions exist:~~

~~a. A full plan was submitted the previous year and is on file with the Office.~~

~~b. No changes are needed to the current plan.~~

3. Each agency DRP must cover, at a minimum, ten topic areas which are listed and described in the Disaster Recovery Plan Documentation for Agencies Preparation Instructions (SIMM Section 65A). If the agency has not developed a full business continuity plan, three supplemental DRP requirements must be included as directed in SIMM Section 65A. In addition, if the DRP does not follow the format in SIMM Section 65A, a cross reference sheet (see SIMM Section ~~70D~~70B) must be included with the update to indicate where information on each topic area can be found in the DRP.

It is important to adapt the detailed content of each plan section to suit the needs of the individual agency, with the understanding that DRPs are based upon available information so they can be adjusted to changing circumstances.

5360.1 COMPLIANCE SUMMARY
(Revised ~~10/09~~ XX/12)

Designation of Information Security Officer, Disaster Recovery Coordinator and Privacy Coordinator - Due by January 31 of each year, or as designee changes occur. Upon the designation of a new ISO, Disaster Recovery Coordinator, and/or Privacy Program Coordinator, the agency must submit an updated Agency Designation Letter to the Office within ten (10) business days using the Agency Designation Letter (SIMM Section 70A). See SAM Section 5315.1

1. **Agency Risk Management and Privacy Program Compliance Certification** - Due by January 31 of each year. The director of each agency must certify that the agency is in compliance with state policy governing information technology risk management and privacy program compliance by submitting the Agency Risk Management and Privacy Program Compliance Certification (SIMM Section 70C). See SAM Section 5315.1. Per Government Code Section 11019.9, agencies are required to maintain a permanent privacy policy, in adherence with the Information Practices Act of 1977 (Civil Code Section 1798 et seq.) that includes, but is not limited to, assigning a designated individual to oversee the program.

2. **Disaster Recovery Plan** - ~~Due by the date outlined in the Agency Disaster Recovery Plan Submission Schedule, found on the Office's Web site at~~ : https://cdt.ca.gov/security/

   ~~a. Disaster Recovery Plan~~ - Each agency must file a copy of its Disaster Recovery Plan (DRP) with the Agency Disaster Recovery ~~Plan Transmittal Letter~~ Program Certification (SIMM Section 70~~D~~B) with the Office by the due date outlined in the Agency Disaster Recovery Plan Submission Schedule. If the agency employs the services of a state data center, it must also provide the data center with a copy of its plan or subset of the relevant recovery information from the agency's DRP. See SAM Section 5355.1.

~~**b. Agency Disaster Recovery Plan Certification -** An Agency Disaster Recovery Plan Certification (SIMM Section 70B) may be filed in place of a full DRP by the due date outlined in the Agency Disaster Recovery Plan Submission Schedule, if specific conditions exist. See SAM Section 5355.1.~~

3. **Incident Follow-up Report** - Each agency having ownership responsibility for the asset (SAM Section 5320.1) must complete an Agency Information Security Incident Report (SIMM Section 65C) for each incident. The report must be submitted to the Office within ten (10) business days from the date of notification.

The Office may require that the agency provide additional information in conjunction with its assessment of the incident.

STATE INFORMATION MANAGEMENT MANUAL EXCERPTS

[Note: Text to be deleted is shown in strikethrough; text to be added is underlined.]

SIMM Section 70 IT Security Certifications

- A Agency Designation Letter
- B Agency Disaster Recovery Program ~~Plan~~ Certification
- C Agency Risk Management and Privacy Program Compliance Certification
- ~~D Agency Disaster Recovery Plan Transmittal Letter~~
- ~~E Agency Telework and Remote Access Security Compliance Certification (doc)~~

Changes to Schedule of Required Security Reporting Activities

Report/Activity	Policy Section	Instructions and Forms	Due Date
Agency Designation Letter	5360.1	SIMM 70A	Annually by January 31 and within ten (10) business days of any change in designee
Agency Risk Management and Privacy Program Compliance Certification	5360.1	SIMM 70C	Annually by January 31
Disaster Recovery Program ~~Plan (Complete)~~	5360.1	SIMM 65A SIMM 70B ~~D~~	Annually pursuant to the DRP Submission Schedule
~~Disaster Recovery Plan Certification (No-Change)~~	~~5360.1~~	~~SIMM 70B~~	~~Every other year pursuant to the DRP Submission Schedule in lieu of a complete plan when no changes have occurred since last submission.~~
Agency Information Security Incident Report	5360.1	SIMM 65B SIMM 65C SIMM 65D	Within ten (10) business days from the date of notification to CHP's Emergency Notification and Tactical Alert Center (ENTAC)
~~Agency Telework and Remote Access Security Compliance Certification~~	~~5340~~	~~SIMM 70E~~	~~Initial by July 1, 2010. Annually by January 31 thereafter, commencing January 31, 2011.~~