CALIFORNIA TECHNOLOGY AGENCY **TECHNOLOGY LETTER**	NUMBER: **TL 12-16**	DATE ISSUED: **DECEMBER 6, 2012**
SUBJECT: **INCIDENT RESPONSE REQUIREMENTS:** Update the requirements to respond to incidents involving a breach of personal information.	REFERENCES: State Administrative Manual Sections 5350 and 5350.4 Statewide Information Management Manual 65D Civil Code Section 1798.29	

BACKGROUND

State Administrative Manual (SAM) Section 5350 requires all state entities[1] to establish and maintain an incident management plan, and promptly investigate incidents involving the loss, damage, misuse of information assets or improper dissemination of information. SAM Section 5350.4 sets forth the requirements for state entity response to incidents involving a breach of personal information, including procedures detailed in Statewide Information Management Manual (SIMM) 65D.

California law, California Civil Code § 1798.29(a), requires a state entity to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. Pursuant to California Civil Code § 1798.29(e), as amended by Senate Bill 24 (Chapter 197, of the Statutes of 2011), effective, January 1, 2012, any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the California Attorney General (AG).

PURPOSE

The purpose of this Technology Letter is to announce the renaming of SIMM 65D, and updates to SAM Section 5350.4 and SIMM 65D to reflect the new requirement and add procedures to notify the AG of a security breach pursuant to California Civil Code § 1798.29(e).

Changes to SAM Section 5340.4 are included as Attachment A while changes to SIMM 65D are included as Attachment B.

QUESTIONS

Questions should be directed to the Office of Information Security (OIS) at (916) 445-5239 or Security@state.ca.gov.

SIGNATURE

/s/

Carlos Ramos, Secretary
California Technology Agency

[1] "State entity" refers to any office, department, board, bureau, commission, or other organizational entity in state government, including Agencies such as the Environmental Protection Agency or the Health and Human Services Agency.

STATE ADMINISTRATIVE MANUAL EXCERPTS

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

5350.4 INCIDENTS INVOLVING PERSONAL INFORMATION

(Revised ~~03/11~~ 12/12)

Every agency that collects, uses, or maintains records containing personal information shall establish and maintain in its incident management plan, procedures for ensuring that any breach of security involving personal information, regardless of its medium (e.g., paper, electronic, verbal) are reported and handled in the most expeditious and efficient manner. The agency's procedures must be documented and address, at a minimum, the following:

1. **Agency Incident Response Team.** An agency's procedures shall identify the positions responsible for responding to a breach of personal information. An agency's response team must include, at a minimum, an escalation manager, the Program Manager of the program or office experiencing the breach, the Information Security Officer (ISO), the Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy, the Public Information or Communications Officer, Legal Counsel, and a representative from the Office of Information Security. The escalation manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and driving the process to completion. Some incidents will require the involvement of others not mentioned above. For example, if the source of the compromised information was a computer system or database, the Chief Information Officer should also be involved in the response activity. If the incident involves unauthorized access, misuse, or other inappropriate behavior by a state employee, or the security breach involves state employee's personal information, the agency's Personnel Officer or Human Resource Manager should be involved. Furthermore, if the incident involves multiple agencies, the response team from each agency may be involved.

2. **Protocol for Internal Reporting.** An agency's procedures shall outline the method, manner, and progression of internal reporting, as to ensure that executive management is informed about breaches involving personal information, and the Agency Incident Response Team is assembled and the incident is addressed in the most expeditious and efficient manner.

3. **Protocol for Security Incident Reporting.** Any actual or suspected breach of personal information (notice-triggering and non-notice-triggering data elements) in any type of media (e.g., electronic, paper) is to be reported immediately to the CHP's ENTAC at (916) 843-4199. This telephone number is staffed 24-hours a day, seven days a week. The officers at ENTAC will require specific information about the incident and will forward that information to the Office of Information Security and to the CHP Computer Crimes Investigation Unit (CCIU). An agency should inform the officer taking the report that the incident involves a personal information breach and the type of media involved (e.g., electronic, paper, both electronic and paper, etc.). Representatives from the Office of Information Security and CCIU will contact the agency as soon as possible following their receipt of the ENTAC report.

   IMPORTANT: A report made to CHP, other law enforcement agencies, or the Office of Information Security outside of the ENTAC notification process by email or other means is NOT an acceptable substitute for the required report to ENTAC.

4. **Decision Making Criteria and Protocol for Notifying Individuals.** An agency's procedures shall include documentation of the methods and manner for determining when and how a notification is to be made. The procedures shall be consistent with and comply with applicable laws, state policies, and the *Requirements to Respond to Incidents Involving a Breach of Personal Information* (SIMM 65D). At a minimum, an agency's procedures will address the following elements:

    a. Whether the notification is required by law (i.e., California Government Code, IRS Publication 1075, HIPAA, PCI, and others).
    b. Whether the notification is required by state policy.
    c. Timeliness of notification.
    d. Source of notice.
    e. Content of notice.
    f. Approval of notice prior to release.
    g. Method(s) of notification.
    h. Preparation for follow-on inquiries.
    i. Other actions that agencies can take to mitigate harm to individuals.
    j. Other situations when notification should be considered.

    A more detailed description of these elements is set forth in the *SIMM 65D~~- Security Breach Involving Personal Information: Requirements and Decision-Making Criteria for State Agencies (SIMM 65D).~~*

5. **Notice to Affected Individuals.** Notice to individuals when a breach of unencrypted notice-triggering data elements occurs, regardless of the media involved (electronic or paper), and in accordance with criteria set forth above.

6. Office of Information Security's **Prior Review and Approval of Breach Notice.** The Office of Information Security provides review and approval of the breach notice prior to its release to any individual as set forth in SIMM 65D.

STATEWIDE INFORMATION MANAGEMENT MANUAL EXCERPTS

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

SIMM Section 65 Information Security Instructions and Forms

A Disaster Recovery Documentation for Agencies Preparation Instructions

B Agency Information Security Incident Notification and Reporting Instructions

C Agency Information Security Incident Report

D ~~Security Breach Involving Personal Information:~~ Requirements to Respond to Incidents Involving a Breach of Personal Information ~~and Decision-Making Criteria for State Agencies~~