CALIFORNIA DEPARTMENT OF TECHNOLOGY **TECHNOLOGY LETTER**	NUMBER: **TL 17-03**	DATE ISSUED: **March 2017**
SUBJECT: **UPDATES TO PERSONAL INFORMATION BREACH NOTIFICATION REQUIREMENTS**	REFERENCES: Government Code Section 11549.3 Civil Code Sections 1798.29 & 1798.82 Statewide Information Management Manual (SIMM) Section 5340-C Technology Letters 16-03 and 16-05	

BACKGROUND

California's landmark security breach notification law (Civil Code § 1798.29) was enacted in 2002 to help combat identity theft in a digital age. The law requires any agency that owns, licenses or maintains computerized data that includes personal information to disclose any breach of the security of the data. Notification must be given to any resident of California whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Existing law requires the disclosure to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Assembly Bill 964 (Chapter 522, Statutes of 2015), and Senate Bills 34 (Chapter 532, Statutes of 2015) and 570 (Chapter 543, Statutes of 2015) amended California's breach notification law (Civil Code Section § 1798.29 and § 1798.82) to define the term "encrypted", added Automated License Plate Recognition data as a notice triggering element, and specified the format and content for breach notifications.

In January 2017, Assembly Bill 2828 (Chapter 337, Statutes of 2016) amended Civil Code Section § 1798.29 and § 1798.82 to require notification also be made to impacted parties when it is reasonable to believe the encryption key or security credential were also compromised and could render that personal information readable or usable.

PURPOSE

The purpose of this Technology Letter (TL) is to announce:

- All Agencies/state entities are directed to review and update their internal processes and procedures to comply with the new requirement to report the disclosure of encrypted personal information.
- Ensure Agencies/state entities are made aware of the changes to breach notification requirements and incorporate the new requirements into their incident reporting and response processes and procedures.
- Revised SIMM Section 5340-C, Requirements to Respond to Incidents Involving a Breach of Personal Information, to include a Breach Response and Notification Assessment Checklist (Appendix A), which will assist Agencies/state entities comply with information security and privacy requirements.

QUESTIONS

Questions regarding this Technology Letter should be directed to the California Office of Information Security at (916) 445-5239 or Security@state.ca.gov

SIGNATURE

_____/s/_____

Amy Tong, Director

California Department of Technology