SENATE BILL **No. 30**

Introduced by Senator Simitian

December 4, 2006

An act to add and repeal Article 4 (commencing with Section 1798.10) of Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, and to add and repeal Article 13 (commencing with Section 11147) of Chapter 1 of Part 1 of Division 3 of Title 2 of the Government Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 30, as introduced, Simitian. Identity Information Protection Act of 2007.

(1) Existing law, the Information Practices Act of 1977, regulates the collection and disclosure of personal information regarding individuals by state agencies, except as specified. The intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains.

This bill would enact the Identity Information Protection Act of 2007. Until December 31, 2013, or as otherwise specified, the act would require identification documents, as defined and with specified exceptions, that are created, mandated, purchased, or issued by various public entities that use radio waves to transmit data, or to enable data to be read remotely, to meet specified requirements. The bill would provide that a person or entity that knowingly discloses, or causes to be disclosed, operational system keys, as described, shall be punished by imprisonment in a county jail for up to one year, a fine of not more than $5,000, or both that fine and imprisonment. The bill would further

authorize declaratory or injunctive relief or a writ of mandate and attorney's fees and costs under specified circumstances.

In addition, because the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the Information Practices Act of 1977, which would include this act, is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains, and because operational system keys would be punishable as a misdemeanor, this bill would create a new crime, thereby imposing a state-mandated local program.

(2) Existing law establishes in the Department of Consumer Affairs, the Office of Privacy Protection for the purpose of protecting the privacy of individuals' personal information and developing fair information practices for state agencies. Existing law establishes in the California State Library, the California Research Bureau with responsibilities to conduct research on various policy issues.

This bill would require the California Research Bureau to submit a report to the Legislature on security and privacy for government-issued, remotely readable identification documents. The bill would require the bureau to submit the report within 270 days of receiving a request from the Office of the President pro Tempore of the Senate or the Office of the Speaker of the Assembly, or before June 30, 2008, whichever is earlier. The bill would require the bureau to establish an advisory board, to be comprised of specified government officials and representatives from industry and privacy rights organizations, to make recommendations and provide technical advice to the bureau in preparing the report.

(3) The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. This act shall be known and may be cited as the Identity Information Protection Act of 2007.

SEC. 2. The Legislature hereby finds and declares all of the following:

(a) The right to privacy is a personal and fundamental right protected by Section 1 of Article I of the California Constitution and by the United States Constitution. All individuals have a right of privacy in information pertaining to them.

(b) This state has previously recognized the importance of protecting the confidentiality and privacy of an individual's personal information contained in identification documents such as drivers' licenses.

(c) It is the intent of the Legislature that the privacy and security protections in this article that apply to remotely readable identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, are interim measures until subsequent legislation or regulations are enacted based on new information, including, but not limited to, information provided by the California Research Bureau.

(d) Notwithstanding any other provision of this act, it is the intent of the Legislature that the interim measures contained herein be replaced by a statewide legislative or regulatory framework in the most timely and expeditious fashion possible following the issuance of recommendations by the California Research Bureau.

SEC. 3. Article 4 (commencing with Section 1798.10) is added to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, to read:

Article 4. Identity Documents

1798.10. (a) Except as provided in subdivision (b), all identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, that use radio waves to transmit data or to enable data to be read remotely shall meet these requirements:

(1) In order to prevent duplication, forgery, or cloning of the identification document, the identification document shall incorporate tamper-resistant features.

(2) In order to determine to a reasonable certainty that the identification document was legitimately issued by the issuing entity, is not cloned, and is authorized to be read, the identification

document and authorized reader, in conjunction with related, functionally integrated software, shall implement an authentication process.

(3) If personally identifiable information is transmitted remotely from the identification document, the identification document and authorized reader, in conjunction with related, functionally integrated software, shall not only meet the requirements of paragraph (2) but also shall implement mutual authentication in order to prevent the transmission of personally identifiable information between identification documents and unauthorized readers.

(4) If personally identifiable information is transmitted remotely from the identification document, the identification document shall make the data unreadable and unusable by an unauthorized person through means such as encryption of the data during transmission, access controls, data association, encoding, obfuscation, or any other measures, or combination of measures, that are effective to ensure the confidentiality of the data transmitted between the identification document and authorized reader.

(5) If personally identifiable information is transmitted remotely from the identification document, the identification document shall implement an access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves. This requirement may be satisfied by the implementation of one or more means including, but not limited to, the following:

(A) An access control protocol requiring the machine-readable or other nonradio frequency reading of information from the identification document prior to each transmission of data using radio waves, without which the identification document will not transmit data using radio waves.

(B) A data-carrying device, such as an integrated circuit or computer chip, that is normally not remotely readable, accessible, or otherwise operational under any circumstances, and only remotely readable, accessible, or operational while being temporarily switched on or otherwise intentionally activated by a person in physical possession of the identification document. The device shall only be remotely readable while the person intentionally enables the identification document to be read.

(C) Another access control protocol that enables the holder to exercise direct control over any transmission of the data using radio waves, not including a detachable shield device or bag.

(6) If a unique personal identifier number that is used to provide an individual with access to more than one type of application or service is transmitted remotely from the identification document, the issuing entity of the identification document shall do one or more of the following, commensurate with the sensitivity of the applications:

(A) Implement a secondary verification and identification procedure that does not use radio waves, including, but not limited to, the manual entry of a personal identification number on a keypad or the placement of an authorized individual at locations at which the identification document is to be read for a purpose other than facilitating secured access to a secured public building or parking area, in order to determine the authenticity of the document or the identity of the person.

(B) Implement the security protections described in paragraph (3).

(C) Implement the security protections described in paragraph (4).

(D) Implement the security protections described in paragraph (5).

(7) If the identification document remotely transmits a unique personal identifier number for the purposes of recording the attendance of a pupil at a public school, the issuing entity of the identification document shall meet the requirements of paragraph (6).

(8) If the identification document remotely transmits a unique personal identifier number for the purposes of accessing public transit services, is issued to a member of the public, as defined in Section 6252 of the Government Code, and is either required by the issuing public entity or confers a benefit that is unique to that class of remotely readable identification document, the issuing entity of the identification document shall meet the requirements of paragraph (6).

(9) The issuing entity of the identification document shall communicate in writing to the person to whom the document is issued at or before the time the document is issued, all of the following:

(A) That the identification document can transmit data or enable data to be read remotely without his or her knowledge.

(B) That countermeasures, such as shield devices or switches, may be used to help the person control the risk that his or her data will be read remotely without his or her knowledge.

(C) The location of readers used or intended to be used by the issuing authority to read the data on the identification document. This requirement shall be satisfied by doing one or more of the following:

(i) Posting or displaying a clear and conspicuous sign, placard, poster, or other similar written notice at each reader's actual location indicating that the issuing authority has placed an identification document reader at that location, that the reader is being used to read identification documents remotely using radio waves, and the commonly understood name of each document.

(ii) Providing each document holder with a list of the location of all readers used or intended to be used by the issuing authority to read the data on the identification document.

(iii) Providing each document holder with a direct Internet link to a Web page that clearly and conspicuously lists the location of all readers used or intended to be used by the issuing authority to read the data on the identification document. This Web page shall be updated regularly.

(D) All circumstances under which the issuing authority plans or intends to read the identification document and the reasons behind those circumstances.

(E) Any information, such as time and location, that is being collected or stored regarding the individual in a database at the time the identification document is being read.

(b) Subdivision (a) shall not apply to:

(1) Any contactless identification document system that began implementation prior to January 1, 2008, or for which a state, county, or municipal government request for proposal has been publicly issued prior to September 30, 2007, or for which a contract has been executed prior to September 30, 2007.

(2) An identification document issued to a person who is incarcerated in the state prison or a county jail, detained in a juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation, or housed in a mental health facility, pursuant to a court order after having been

charged with a crime, or to a person pursuant to court-ordered electronic monitoring.

(3) An identification document issued to a person employed by a state prison, county jail, or juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation if the document is not removed from the facility and the requirements of paragraph (9) of subdivision (a) apply.

(4) An identification document issued to a law enforcement officer or emergency response personnel if the document is used only while the law enforcement officer or emergency response personnel is on active duty and the requirements of paragraph (9) of subdivision (a) apply.

(5) An identification document issued to a patient who is in the care of a government-operated or government-owned hospital, ambulatory surgery center, or oncology or dialysis clinic if all of the following requirements are met:

(A) The identification document is valid for only a single episode of care.

(B) The identification document may be removed and reattached when used on a nonemergency outpatient.

(C) The identification document does not transmit or enable the remote reading using radio waves of personally identifiable information.

(D) The patient returning for a new episode of care is assigned a new unique personal identifier number.

(E) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient is notified, in writing, that the identification document transmits data using radio waves.

(F) The patient is not compelled or encouraged to wear, or keep on his or her person, the identification document beyond the facility property.

(6) An identification document issued to a person who is in the care of a skilled nursing facility operated or owned by the government, if all of the following requirements are met:

(A) The patient has been diagnosed by a doctor with dementia or other cognitive impairment that involves substantial limitation in function.

(B) The identification document does not transmit or enable the remote reading using radio waves of personally identifiable information.

(C) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient is notified, in writing, that the identification document transmits data using radio waves.

(D) The patient is not compelled or encouraged to wear or keep on his or her person the identification document beyond the facility property.

(E) The patient or the person who has been legally entrusted to make medical decisions on behalf of the patient has consented to the issuance of the identification document.

(7) An identification document issued to a patient by emergency medical services for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly related to a disaster, as defined by the local emergency medical services agency organized under Section 1797.200 of the Health and Safety Code.

(8) An identification document that is issued to a person for the limited purpose of facilitating secured access by the identification document holder to a secured public building or parking area, if the requirements of paragraph (9) of subdivision (a) are met and the identification document does not transmit or enable the remote reading using radio waves of personally identifiable information.

(9) A license, certificate, registration, or other authority for engaging in a business or profession regulated under the Business and Professions Code, if the requirements of paragraph (9) of subdivision (a) are met and the identification document does not transmit or enable the remote reading using radio waves of personally identifiable information.

1798.11. Except as provided in subdivision (d), a state, county, or municipal government, or subdivision or agency thereof, that creates, mandates, purchases, or issues an identification document in compliance with subdivision (a) of Section 1798.10:

(a) Shall not, under any circumstances, disclose any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10, either publicly or to any nongovernmental entity or other third party, including, but not limited to, contractors,

officers, and employees of other government agencies, that is not authorized under subdivision (d).

(b) Shall take all reasonable measures to keep any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10 secure and unavailable to any third party that is not authorized under subdivision (d).

(c) Shall not, under any circumstances, act in any way to allow a third party that is not authorized under subdivision (d) to read the data transmitted remotely by the identification document using radio waves.

(d) A state, county, or municipal government, or subdivision or agency thereof, that creates, mandates, purchases, or issues an identification document in compliance with subdivision (a) of Section 1798.10 may disclose any operational system keys used pursuant to paragraphs (3) and (4) of subdivision (a) of Section 1798.10 to authorized third parties that in the stream of commerce have a bona fide business relationship with the agency, or its contractors or subcontractors, and that are necessary to the operation, testing, or installation of the identification system, and to emergency response personnel for the sole purposes of locating and identifying a person or persons in the case of a disaster, as defined by the local Emergency Medical Services agency organized under Section 1797.200 of the Health and Safety Code.

(1) Any authorized third party that receives a disclosure pursuant to this exception is subject to the prohibitions of subdivisions (a) to (c), inclusive.

(2) Any authorized third party that receives a disclosure pursuant to this exception shall adopt procedures restricting access to the operational system keys and securing the keys from tampering and unauthorized access. These procedures shall include administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information.

(3) All information received pursuant to this exception shall be destroyed when the purpose of the disclosure is completed.

1798.115. A person or entity that knowingly discloses, or causes to be disclosed, the operational system keys described in Section 1798.11 in violation of Section 1798.11 shall be punished by imprisonment in a county jail for up to one year, a fine of not

more than five thousand dollars ($5,000), or both that fine and imprisonment.

1798.12. A state, county, or municipal government, or a political subdivision or agency thereof, that uses radio waves to transmit data or to enable data to be read remotely pursuant to subdivision (a) of Section 1798.10 or the authorized third parties with whom the governmental entity has a bona fide business relationship shall not disclose any data or information regarding the location of a person derived from the use of the radio waves, unless the disclosure comports with any of the following:

(a) The disclosure is made pursuant to an exigent circumstance and all of the following occur:

(1) The information that is requested is necessary to locate and respond to a person who is in immediate danger of death or serious bodily injury or a minor who is in immediate danger.

(2) The information that is disclosed solely regards the location of a person or an identification document and the time at which that person was or is at that location.

(3) The request by emergency response personnel to a governmental entity to which this section applies includes, at a minimum, all of the following information:

(A) The name and title of the emergency response personnel.

(B) The office location and telephone number for the emergency response personnel.

(C) The name and telephone number of the emergency response personnel's supervisor or the person who has the ultimate operational responsibility at the time.

(D) The assertion by the emergency response personnel that an exigent circumstance exists.

(4) The governmental entity provides the emergency response personnel with the requested location information upon verification of the information required by paragraph (3) with the emergency response personnel's supervisor or the person who has ultimate operational responsibility at the time. No governmental entity, or official or employee thereof, shall be subject to liability when it acts in a reasonable manner upon receiving the information required by paragraph (3).

(5) The governmental entity maintains for a period of not less than one year all requests from public safety or emergency response

agencies for location information that are made under exigent circumstances.

(6) Individuals whose location information has been released pursuant to this subdivision are notified in writing by the governmental entity within a reasonable period of time that their information has been released and the notice shall include the information required in paragraph (3). The notification required by this paragraph may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this paragraph shall be made after the law enforcement agency determines that it will not compromise the investigation.

(7) The location information obtained as the result of a request pursuant to this section is used solely for the purpose of rendering emergency aid by emergency response personnel to the person during the exigent circumstances forming the basis of the request.

(b) The disclosure is made pursuant to a request by law enforcement personnel in the course of a legitimate investigation and the information is derived only from the use of employee identification documents to facilitate secured access to public buildings or parking areas.

(c) The disclosure is required pursuant to a search warrant.

1798.125. Any interested person may institute proceedings against a governmental entity for injunctive or declaratory relief or a writ of mandate in any court of competent jurisdiction for the purpose of preventing or stopping any violation of this article, if all of the following occur:

(a) The person provides to the governmental entity, written notice of the alleged violation by certified mail.

(b) The governmental entity fails, for at least 30 days after receipt of that written notice, to fix the alleged violation, to comply with the provisions of the article, and to inform the demanding party in writing of its actions to fix the alleged violation or its decision not to correct the alleged violation.

1798.126. (a) In any proceedings brought pursuant to Section 1798.125, the court may assess against the governmental entity reasonable attorney’s fees and other litigation costs reasonably incurred in any proceedings under this article in which the complainant has prevailed.

(b) Nothing in this section affects or is intended to limit or supplant any other remedies that may be available in law or equity.

1798.135. For purposes of this article, the following definitions shall apply:

(a) "Access controls" means granting or denying permission to access information.

(b) "Authentication" means the process of applying a machine-readable process to data or identification documents, or both, so as to accomplish either of the following:

(1) Establish that the data and the identification document containing the data were issued by the responsible issuing state or local governmental body.

(2) Ensure that a reader, as defined in subdivision (p), is permitted under California law to access that data or identification document.

(c) "Authorized reader" means a reader, as defined in subdivision (p), that, with respect to a particular identification document, (1) is permitted under California law to remotely read the data transmitted by that identification document, (2) is being used for a lawful purpose, and (3) is fully in accord with the requirements of subdivision (a) of Section 1798.10.

(d) "Contactless identification document system" means a group of identification documents issued and operated under a single authority that use radio waves to transmit data remotely to readers intended to read that data. In a contactless identification document system, every reader must be able to read every identification document in the system.

(e) "Data" means information stored on an identification document in machine-readable form including, but not limited to, personally identifiable information and other unique personal identifier numbers.

(f) "Data association" means storing information in separate locations so that the information is not resident in a single location and is not usable if only one of such locations is accessed.

(g) "Emergency response personnel" means any of the following:

(1) "Emergency medical technician," as defined in Sections 1797.80 and 1797.82 of the Health and Safety Code.

(2) "Firefighter," as defined in Section 1797.182 of the Health and Safety Code.

(3) "Mobile intensive care nurse," as defined in Section 1797.56 of the Health and Safety Code.

(4) "Paramedic," as defined in Section 1797.84 of the Health and Safety Code.

(5) "Peace officer," as defined in Sections 830.1 and 830.2 of the Penal Code.

(h) "Encoding" means use of a mechanism that allows the message elements to be substituted for other elements.

(i) "Encryption" means the protection of data in electronic form in storage or while being transmitted using an encryption algorithm implemented within a cryptographic module that has been adopted or approved by the National Institute of Standards and Technology, the Institute of Electrical and Electronics Engineers, Inc., the Internet Engineering Task Force, the International Organization for Standardization, the Organization for the Advancement of Structured Information Standards, or any other similar standards setting body, rendering that data indecipherable in the absence of associated cryptographic keys necessary to enable decryption of that data. That encryption shall include appropriate management and safeguards of those keys to protect the integrity of the encryption.

(j) "Exigent circumstance" means a reasonable belief by emergency response personnel that either of the following situations exists:

(1) There is immediate danger of death or serious bodily injury to the person whose location information is being sought or to another individual who could be located through the reading of that identification document.

(2) There is immediate danger to a minor whose location information is being sought or to another minor who could be located through the reading of that identification document.

(k) (1) "Identification document" means any document containing data that is issued to an individual and which that individual, and only that individual, uses alone or in conjunction with any other information for the primary purpose of establishing his or her identity. Identification documents specifically include, but are not limited to, the following:

(A) Driver's licenses or identification cards issued pursuant to Section 13000 of the Vehicle Code.

(B) Identification cards for employees or contractors.

(C) Identification cards issued by educational institutions.

(D) Health insurance or benefit cards.

(E) Benefit cards issued in conjunction with any government-supported aid program.

(F) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the Business and Professions Code.

(G) Library cards issued by any public library.

(2) Identification documents do not include devices issued to persons for the limited purpose of collecting funds for the use of a toll bridge or toll road, such as devices used by the FasTrak system, if the device is not issued for the exclusive use of an individual and does not transmit or enable the remote reading using radio waves of personally identifiable information.

(*l*) "Key" means a string of bits of information used as part of a cryptographic algorithm used in encryption.

(m) "Mutual authentication" means a process by which identification documents and authorized readers securely challenge each other to verify authenticity and authorization of both readers and documents before any data is exchanged, except such data as is necessary to carry out mutual authentication. Mutual authentication accomplishes both of the following:

(1) Authorized readers, as defined in subdivision (c), can accurately assess whether the identification document and data stored are issued by the responsible issuing state or local governmental body to an authorized holder.

(2) Authorized identification documents can accurately assess whether a reader accessing them is authorized to read the documents, and authorized to then access data stored on the documents.

(n) "Obfuscation of information" means the transformation of information without the use of an encryption algorithm or key into a form in which the information is rendered unusable or unreadable.

(o) "Personally identifiable information" includes any of the following data elements to the extent that they are used alone or in conjunction with any other information to identify an individual:

(1) First or last name.

(2) Address.

(3) Telephone number.

(4) E-mail address.

(5) Date of birth.

(6) Driver's license number or California identification card number.

(7) Any unique personal identifier number contained or encoded on a driver's license or identification card issued pursuant to Section 13000 of the Vehicle Code.

(8) Bank, credit card, or other financial institution account number.

(9) Credit or debit card number.

(10) Any unique personal identifier number contained or encoded on a health insurance, health benefit, or benefit card issued in conjunction with any government-supported aid program.

(11) Religion.

(12) Ethnicity or nationality.

(13) Photograph.

(14) Fingerprint or other biometric identification.

(15) Social security number.

(p) "Reader" means a scanning device that is capable of using radio waves to communicate with an identification document and read the data transmitted by that identification document.

(q) "Remotely" means that no physical contact between the identification document and a reader is necessary in order to transmit data using radio waves.

(r) "Shield devices" mean physical or technological protections available to stop the transmission of data programmed on or into an identification document using radio waves.

(s) "Single episode of care" means an inpatient hospital stay through discharge or specific course of therapy or treatment for outpatient care.

(t) "Unique personal identifier number" means a randomly assigned string of numbers or symbols that is encoded onto the identification document and is intended to identify the identification document that has been issued to a particular individual.

1798.136. The provisions of this article shall become inoperative on December 31, 2013, or when alternative statewide regulations pertaining to the privacy and security of remotely readable identification documents are enacted or promulgated pursuant to later legislation, whichever is earlier.

SEC. 4. Article 13 (commencing with Section 11147) is added to Chapter 1 of Part 1 of Division 3 of Title 2 of the Government Code, to read:

Article 13. Report on Security and Privacy for Government-Issued Identification Documents

11147. The California Research Bureau in the California State Library, within 270 days of receiving a request from the Office of the President pro Tempore of the Senate or the Office of the Speaker of the Assembly, or before June 30, 2008, whichever is earlier, shall submit to the Legislature a report on security and privacy for government-issued, remotely readable identification documents.

11147.1. In preparing the report required by Section 11147, the bureau shall, at a minimum, do all of the following:

(a) Establish an advisory board that makes recommendations, provides technical advice, answers bureau questions, and outlines the strengths and weaknesses of potential approaches to privacy and security proposals for government-issued, remotely readable identification documents. The advisory board shall be composed of all of the following members:

(1) The State Chief Information Officer or his or her designee.

(2) The Chief of the Office of Privacy Protection or his or her designee.

(3) The Attorney General or his or her designee.

(4) A representative from the Office of Emergency Services.

(5) A representative from either the University of California or the California State University system.

(6) A representative from the Department of Motor Vehicles.

(7) A representative from the California State Information Security Office.

(8) A representative selected by the bureau from the California School Boards Association.

(9) A representative selected by the bureau from city or county government.

(10) One representative selected by the bureau, from each of the following industries:

(A) Remotely readable identification card manufacturers.

(B) Remotely readable identification chip manufacturers.

(C) Remotely readable identification reader manufacturers.
(D) Remotely readable component manufacturers.
(E) Enterprise or network information technology companies.
(11) Five representatives selected by the bureau from among privacy rights groups, including, but not limited to, the American Civil Liberties Union, the Electronic Frontier Foundation, and the Privacy Rights Clearinghouse.
(12) Other representatives selected by the bureau that would be necessary for the bureau to complete the report required by Section 11147.
(b) Review and document existing state and federal laws relating to privacy, security, and safeguards for remotely readable identification documents.
(c) Review privacy and security safeguards and technologies that are currently available or in development for remotely readable identification documents.
(d) Review best practices that have been established or that are under consideration to prevent identity theft, privacy invasion, and criminal use of personal and other data to determine their applicability to government-issued identification documents.
(e) Consider requirements for a privacy impact assessment and a security risk assessment conducted by issuing entities that would clearly define what personal information is to be collected, how the information will and could be used, who may and who could access the information, how the information will be protected from unauthorized access, and how an individual may control use of and update his or her information.
(f) Identify, develop, and evaluate options for the Legislature to review and consider for action for a legislative and regulatory framework that would ensure the safety and security of information contained on remotely readable identification documents and the privacy of the individuals to whom the documents are issued.
11147.2. The bureau shall be solely responsible for preparing the report required by this article. The report shall include information, suggestions, and comments from the advisory board. In making recommendations, the bureau shall maintain an approach that, when appropriate, is neutral with respect to specific technologies and methods, shall consider the multitude of ways of ensuring privacy and security, and shall consider the impact of any recommendations on innovation. The report may include

additional research and commentary that the bureau believes is necessary to prepare a complete and thorough report.

11147.3. The provisions of this article shall become inoperative on December 31, 2013, or when alternative statewide regulations pertaining to the privacy and security of remotely readable identification documents are enacted or promulgated pursuant to later legislation, whichever is earlier.

SEC. 5. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

O