

SUMMARY ANALYSIS OF AMENDED BILL

Author: Simitian Analyst: Deborah Barrett Bill Number: SB 682
 Related Bills: See Prior Analysis Telephone: 845-4301 Amended Date: 03-31-05
 Attorney: Patrick Kusiak Sponsor: _____

SUBJECT: Identity Information Protection Act Of 2005/ Prohibit Public Entities From Using Contactless Integrated Circuits In Identity Documents Created, Mandated, Or Issued By Public Entity

DEPARTMENT AMENDMENTS ACCEPTED. Amendments reflect suggestions of previous _____ analysis of bill as introduced/amended _____.

_____ AMENDMENTS IMPACT REVENUE. A new revenue estimate is provided.

_____ AMENDMENTS DID NOT RESOLVE THE DEPARTMENTS CONCERNS stated in the previous analysis of bill as introduced/amended _____.

_____ FURTHER AMENDMENTS NECESSARY.

_____ DEPARTMENT POSITION CHANGED TO _____.

REMAINDER OF PREVIOUS ANALYSIS OF BILL AS INTRODUCED/AMENDED February 22, 2005 STILL APPLIES.

OTHER – See comments below.

SUMMARY

This bill would prohibit, with certain exceptions, state entities from using identification documents containing a device that would enable personal information embedded in the card to be accessed remotely.

SUMMARY OF AMENDMENTS

The March 31, 2005, amendments provide exceptions to the restrictions for use of identification documents. The amendments require state agencies that issue the identification documents to provide notice in writing to recipients of identification documents of:

- The use and potential exposure of personal information,
- The location of scanners or readers, and
- The availability of blocking devices to protect personal information.

The amendments also provide a sunset date for the exception applicable to state agencies and sanctions to state agencies that remotely scan identification documents without the knowledge of the individual whose identity document is being scanned.

Board Position:	Department Director	Date
_____ S		
_____ SA	Brian Putler	5/6/05
_____ N		
_____ NA		
_____ O		
_____ OUA		
_____ NP		
_____ NAR		
<input checked="" type="checkbox"/> PENDING		

As a result of the amendments, the “This Bill,” “Implementation Concerns,” “Policy Concerns,” and “Fiscal Impact” portions of the prior analysis have been revised. A technical consideration has been included in this analysis as well. The remainder of the department’s analysis of the bill as introduced February 22, 2005, still applies.

POSITION

Pending.

ANALYSIS

THIS BILL

This bill would establish the Identity Information Protection Act of 2005. This bill would prohibit state, county, or municipal governments, or agencies thereof, from creating or issuing identification documents that contain a contactless integrated circuit or other device that can broadcast personal information or enable personal information to be scanned remotely.

This bill defines identification document to mean any document that an individual uses alone or in conjunction with any other information to establish his or her identity. Identification documents include but are not limited to the following:

- Driver’s licenses or identification cards,
- Identification cards for employees or contractors,
- Identification cards issued by educational institutions,
- Health insurance or benefit cards,
- Benefit cards issued in conjunction with any government supported aid program,
- Licenses, certificates, registration, or other means to engage in a business or profession regulated by the California Business and Professions Code, and
- Library cards issued by a public library.

Personal Information as defined in this bill includes an individual’s name, address, telephone number, email address, date of birth, race, religion, ethnicity, nationality, photograph, fingerprint or other biometric identification, social security number, or any other unique personal identifier.

This bill provides exceptions to the restrictions on use of identification documents. The exceptions exclude identification documents that are:

- Used on a toll road or bridge for purpose of collecting funds for the use of that road or bridge,
- Used in prisons, county jails, or mental health facilities,
- Given to a child four years old or younger in the custodial care of a government operated medical facility,
- Part of a contactless integrated system used by state, county, or municipal governments and is in use and operational no later than December 31, 2005, and
- Any other exceptions legislatively determined to be necessary to meet a compelling state interest.

The identification documents used in these exceptions may not contain personal information as defined; however, they may contain a unique personal identifier number. The exception provided for state agency use is only valid until January 1, 2011.

This bill also requires state agencies that use a contactless identification document to inform recipients of identification documents in writing that:

- The document contains a device that can broadcast a unique personal identifier number or enable that number to be scanned remotely without their knowledge,
- The location of all scanners and readers used or intended to be used by the issuing agency, and
- Countermeasures exist, such as shield devices, to help one control the risk that their unique personal identifier number will be broadcast or scanned remotely without their knowledge.

This bill establishes punishment against a person or state entity that remotely scans or attempts to remotely scan, a person's identification document without the knowledge of that person. The punishment ranges from imprisonment in a county jail for up to one year, a fine of not less than \$1,000 and no more than \$5,000, or both the imprisonment and the fine.

IMPLEMENTATION CONSIDERATIONS

The department has identified the following implementation concerns. Department staff is available to work with the author's office to resolve these and other concerns that may be identified.

The bill would define remotely as no physical contact between the card and the reader. The department's security badge system meets the remote definition, but requires the card to be less than six inches from the reading device to be activated. This device does not broadcast the information contained on the card any further than the distance between the card reader and the card and does not appear to pose the potential threat of personal information theft the bill intends to eliminate. To meet the provisions of this bill, it appears the department would be required to replace its current badge reader security system.

The department currently uses a badge reader system for employees and vendors to access department buildings. This bill could impose penalties where an employee passes a reader too closely. Such an accidental scanning could be construed as a crime. The author may want to consider additional requirements that the remote scanning be done intentionally or knowingly by the state agency.

In addition, the department deactivates cards when notified that the card has been lost or stolen. Under the provisions of this bill, if an individual's card is stolen or lost and scanned by a third party before the department deactivates the card, the department may be subject to penalties because the card was scanned without the employees knowledge. The author may want to consider exceptions to provide for instances beyond the control of the department especially when no damage has been caused to the individual.

TECHNICAL CONSIDERATIONS

On page 3, line 5, "Identity Documents" should be changed to "Identification Documents" to remain consistent with the March 31, 2005, amendments.

Fiscal Impact

The department would incur significant costs to comply with the provisions of this bill as described above under "Implementation Considerations." It appears this bill would require the department to replace the current security badge system with a contact required security badge system by 2011. Replacement of the card system for the department's facility space would entail replacement of approximately 220 card readers and acquisition of additional software and hardware. The complete replacement of the existing security system is estimated to cost approximately \$8 million.

Policy Concerns

The requirement to inform recipients of identification documents of the location of all card readers in the department is contrary to acceptable security practices recommended by industry, military, and Homeland Security. Recommended practice is that information involving security forces and security infrastructure be kept confidential to reduce vulnerabilities to facilities or critical Information Technology infrastructure and protect employees. Publication of this information provides a blueprint for individuals that may want to circumvent those measures and minimizes the effectiveness of the security procedures in place.

LEGISLATIVE STAFF CONTACT

Deborah Barrett
Franchise Tax Board
(916) 845-4301
deborah.barrett@ftb.ca.gov

Brian Putler
Franchise Tax Board
(916) 845-6333
brian.putler@ftb.ca.gov