



---

## *Detailed Fiscal Analysis*

### *Summary of the bill*

The bill requires state agencies to adopt and implement rules to protect the security and privacy of the confidential personal information maintained by the state. Confidential personal information (referred to as sensitive personal information in the Governor's November 20, 2008 Management Directive) includes social security numbers, federal tax identification numbers, financial information, and so forth. The bill requires the Auditor of State to review state agencies' compliance with data security practices as part of that office's auditing function. The bill's requirements affect all state agencies except institutions of higher education and those whose principal function relates to the enforcement of criminal laws. Finally, the bill also allows a person who is harmed by an intentional violation of the agency rules to recover damages and attorney's fees in a civil action and imposes a criminal penalty for such a violation.

### *Current policies and practices*

Currently, executive agencies are required to maintain and administer their own sensitive personal information (SPI) systems under guidance of the chief privacy officer and the chief information security officer of the Office of Information Technology (OIT). This office is housed within the Department of Administrative Services. Under the Governor's Executive Order 2007 - 013S and the November 20, 2008, Management Directive, all agencies that maintain a system containing SPI are required to:

- appoint a data privacy point of contact to be responsible for the system;
- implement rules for the operation and maintenance of the system and the information it contains; and
- take precautions to protect SPI from unauthorized modification or use.

Since September 1, 2008, state agencies have been required to complete a Privacy Impact Statement before collecting or compiling any sort of new personal information. This assessment is reviewed by the chief privacy officer to help agencies determine exactly what information is to be collected, how SPI might be at risk, and what steps should be taken to protect it. However, these privacy assessments are only for new data collection systems. Sensitive information that is already stored or being collected is not subject to this sort of review. Further guidance concerning SPI security and executive agency policies concerning the use of such data was provided in the November 20, 2008, Management Directive, which required agencies to implement these standards by March 31, 2009. The bill would require that similar measures be taken.

### *New requirements in the bill*

The bill adds to the standards set out in the management directive by statutorily requiring agencies to:

- (1) notify individuals of improperly accessed information;
- (2) respond to queries regarding what personal information is kept;
- (3) train employees in the proper use of private information;
- (4) incorporate new logging functionalities into new or upgraded personal information systems; and
- (5) record each specific access to confidential personal information until existing systems are replaced.

The first two requirements could be absorbed into state agencies' existing administrative duties and would therefore not generate significant, if any, new costs. The third requirement might incur a slight cost to those agencies that do not already have such training programs in place. State agencies, however, could incur significant new costs for complying with the fourth and fifth requirements: that agencies incorporate logging functionalities into new personal information systems, and that agencies record every use of confidential personal information until existing systems are replaced.

Adding new functions to systems at the time of replacement or upgrade would increase the cost of this sort of system maintenance, though it is unclear by how much. The cost for designing and implementing access logs would vary depending on the complexity of the computer coding required, the age of the system requiring upgrades, and so forth. The cumulative cost could be tens of millions of dollars. Additionally, for larger systems there could also be ongoing new personnel costs and new hardware costs for the management, administration, and storage of the access log requirements. However, as these upgrades would only occur as needed, these additional expenses will most likely be distributed over several years.

Until existing systems are replaced or upgraded, agencies will be required to record every use of confidential personal information. The bill does not explicitly state how agencies are to fulfill this requirement, and so the fiscal impact of this provision is unclear. It could require that agencies track this information by hand on written logs or kept on another computer. Alternatively, if agencies opted to incorporate a logging tool in their existing information systems, they would incur some costs for making these changes.

In an attempt to determine new implementation costs, DAS' chief privacy officer distributed a survey to all state agencies that would be affected by the bill. OIT has shared the survey results with LSC. Twenty responses indicated that over 270 applications containing confidential personal information would need some modification to comply with the bill's access log requirement. According to OIT, records within these systems are accessed approximately 1.3 million times per day, and that approximately 120,000 people, including state employees, local government employees, contractors, and consultants have access to this information. Incorporating logging functionality into the applications specified by the bill would be the greatest cost.

### **Criminal penalties and civil action**

Under the bill, public officials, public employees, or those contracted by the state to work with confidential personal information who refuse to comply with the requirements in the bill are guilty of a minor misdemeanor, the penalty for which is a fine of up to \$150. Those individuals who improperly access or use confidential personal information would be subject to a first degree misdemeanor. The penalty for such a violation is a jail term of up to 180 days and up to a one thousand dollar fine. LSC assumes that in either instance, violations would be few. In the first case, it would be reasonable to assume that most employees, officials, or contractors would comply with the law and related rules and management directives concerning data security. In the second case, the existence of access logs in place would deter unauthorized access to confidential personal information. Nevertheless, county and municipal courts could incur costs for prosecuting and adjudicating these cases. The bill also allows a person who is harmed from an intentional violation of the rules to recover damages and attorney's fees. This provision is unlikely to have significant impact on the state.

*LSC fiscal staff: Nick Thomas, Budget Analyst*

*HB0648HR.doc/th*