
Detailed Fiscal Analysis

Summary of the bill

The bill requires that state agencies – excluding state colleges and universities, the courts, and judicial agencies – adopt and implement rules to protect the security and privacy of confidential personal information they possess in written or electronic form. Confidential personal information (referred to as sensitive personal information (SPI) in the Governor's November 20, 2008 Management Directive) includes social security numbers, federal tax identification numbers, financial information, and so forth. To ensure compliance, the bill requires the Auditor of State to review state agencies' data security practices as part of that office's auditing function. 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 on anyone who commits any such violation.

Overall, the major costs in the bill stems from the requirement that agencies implement some means of recording employee access to confidential personal information on their existing systems. This would have to be tracked by written logs or recorded on separate electronic files, increasing administrative burden and perhaps adding new data storage costs. Adding logging functionality to systems when they are upgraded or bought new might also add considerable expense, depending on the system.

Overview of systems affected by the bill

In an attempt to determine the cost of implementing the bill's requirements, the Department of Administrative Services' Office of Information Technology (OIT) distributed a survey to all state agencies affected by the bill. The results were shared with LSC. Twenty responses indicated that over 270 applications containing SPI 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 approximately 120,000 people—including state employees, local government employees, contractors, and consultants—have access to this information.

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 OIT. Under the Governor's Executive Order 2007 - 013S and current OIT policies, 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 is provided in the Governor's November 20, 2008, Management Directive, which requires agencies to implement standards very similar to those outlined in the bill. The Management Directive requires that agencies meet these standards by March 31, 2009. Agencies that are unable to meet this deadline are required to inform the Governor of when they will be able to do so. As there is no absolute deadline for when these measures are to be implemented, the Governor's Directive presents uncertainty as to exactly what new costs generated by implementing privacy protection standards would be directly attributable to the bill. Depending upon when agencies are able to comply with the Directive, certain costs that would have otherwise been attributed to the bill would rather be the result of the Management Directive.

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. To comply with the fourth requirement, agencies would incur new costs, perhaps significant, for implementing logging functionality when they upgrade, replace, or buy new systems.

State agencies, however, could also incur significant new costs for complying with the fifth requirement: that they record every use of SPI obtained from existing systems. Presumably, agencies would have to develop some form of access log in parallel with the systems containing SPI. These records might be kept in written form or stored in electronic file format. Any new costs resulting from this provision would depend on how labor intensive these tracking processes would be to implement and data storage needs. For agencies that access SPI frequently, these costs could be high.

Criminal penalties and civil action

Under the bill, public officials, public employees, or those contracted by the state to work with confidential personal information that 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 intentionally misuse 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. The state would be prohibited from hiring anyone who is convicted of improperly using personal information.

County and municipal courts could incur costs for prosecuting and adjudicating any new cases arising from the new penalties, but LSC assumes that there would be few violations of either crime. In the first case, once employees, officials, and contractors become aware of the bill's privacy standards, they would presumably comply with the laws, rules, and management directives concerning data security. In the second case, the existence of access logs would deter unauthorized use of confidential personal information. The bill also allows a person who is harmed from an intentional violation of the rules to recover damages and attorney's fees. As a whole, these penalty provisions are unlikely to have significant impact on the state.

LSC fiscal staff: Nick Thomas, Budget Analyst

HB0648EN.docx / th