CONGRESSIONAL BUDGET OFFICE
COST ESTIMATE

December 11, 2009

S. 139
Data Breach Notification Act

As ordered reported by the Senate Committee on the Judiciary on November 5, 2009

SUMMARY

S. 139 would require most government and business entities that collect, transmit, store, or use sensitive personal information to notify any individuals whose information has been unlawfully accessed through a breach in the security systems designed to protect such information from unauthorized access. The legislation defines sensitive personal information as combinations of an individual's name, address or phone number, and Social Security number, driver's license number, financial account information, or biometric data (that is, finger print, voice print, or retina scan). Under certain circumstances, entities could apply to the Secret Service for exemptions from the notification requirements. In addition, S. 139 would create civil penalties for entities that fail to provide notice to affected individuals.

CBO expects that agencies would incur negligible costs to implement the legislation because they already comply with the notification requirements in the bill. Implementing S. 139 could increase collections of civil penalties that would affect revenues, but CBO estimates that any such effect would not be significant in any year. In addition, enacting S. 139 could affect direct spending for notification requirements by agencies not funded through annual appropriations. CBO estimates, however, that any changes in net spending by those agencies would be negligible. Complying with the bill's provisions could increase the expenses of the Secret Service, but CBO estimates that such costs would be less than $500,000 annually and subject to the availability of appropriated funds.

S. 139 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the cost of complying with the requirements would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted annually for inflation).

The notification requirements in S. 139 would impose private-sector mandates as defined in UMRA. Because most businesses already comply with similar state requirements, CBO estimates that the incremental cost to comply with the mandates would fall below the annual threshold established in UMRA for private-sector mandate ($139 million in 2009, adjusted annually for inflation).

ESTIMATED COST TO THE FEDERAL GOVERNMENT

Enacting S. 139 could affect both direct spending and revenues, but CBO estimates that any such effects would be negligible.

In the event of a security breach, S. 139 would require most government agencies to notify individuals whose personal information has been unlawfully accessed. Notification would be in the form of an individual notice (a written notice to a home mailing address, a telephone call, or an e-mail) as well as through the mass media for breaches involving the sensitive information of 5,000 or more individuals. The legislation also would require the agency to provide affected individuals with a description of the accessed information, a toll-free number to contact the agency, the names and toll-free telephone numbers of the major credit-reporting agencies, and in some instances, information on an individual state's victim protection assistance.

This provision would codify the current practice of the federal government regarding notifications of security breaches. While existing laws generally do not require agencies to notify affected individuals of data breaches, this has been the practice of agencies that have experienced such breaches. Therefore, CBO expects that implementing those notification provisions would probably not lead to a significant increase in spending. Nonetheless, the federal government is also one of the largest providers, collectors, consumers, and disseminators of personal information in the United States. Although CBO cannot anticipate the number of security breaches, a significant breach of security involving a major collector of personal information, such as the Internal Revenue Service or the Social Security Administration, could involve millions of individuals, and there would be significant costs to notify individuals of such a security breach.

The legislation also would require a business entity or federal agency (under certain circumstances) to notify the Secret Service that a security breach has occurred, but would permit entities or agencies to apply to the Secret Service for exemption from notice under certain circumstances. Based on information from the Secret Service, CBO estimates any additional investigative or administrative costs to that agency would likely total less than $500,000 annually and would be subject to the availability of appropriated funds.

IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

S. 139 contains intergovernmental mandates as defined in UMRA. The bill would explicitly preempt laws in at least 45 states regarding the treatment of personal information and would impose notification requirements and limitations on State Attorneys General and state insurance authorities. Because the limits on state authority would impose no duties with costs and because the notification requirements would result in minimal additional spending, CBO estimates the costs of the mandates would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted annually for inflation).

ESTIMATED IMPACT ON PRIVATE SECTOR

S. 139 would impose private-sector mandates as defined in UMRA. The bill would require business entities engaged in interstate commerce that use, access, transmit, store, dispose of, or collect sensitive personally identifiable information to notify individuals if a security breach occurs that affects the individuals' sensitive, personally identifiable information. Entities would be able to notify individuals using written letter, the telephone, or email under certain circumstances. The bill also would require those entities to notify the owner or licensee of any such information that the entity does not own or license and would require notice in major media outlets serving a state or jurisdiction for any breach of more than 5,000 residents' records within a particular state. In addition, business entities would be required to notify other entities and agencies in the event of a large security breach. Entities that experience the breach of such data would have to notify the affected victims and consumer reporting agencies if the breach involves more than 5,000 individuals, and the U.S. Secret Service if the breach involves more than 10,000 individuals. The bill, however, would exempt business entities from the notification requirements under certain circumstances.

According to industry sources, millions of individuals' sensitive personally identifiable information is breached every year. However, according to those sources, 45 states already have laws requiring notification in the event of a security breach. In addition, it is the standard practice of most businesses to notify individuals if a security breach occurs. CBO therefore estimates that the incremental costs incurred by businesses to comply with the requirements in the bill would fall below the annual threshold established in UMRA for private-sector mandate ($139 million in 2009, adjusted annually for inflation).

PREVIOUS CBO ESTIMATES

On December 2, 2009, CBO transmitted a cost estimate for S. 1490, the Personal Data Privacy and Security Act of 2009, as ordered reported by the Senate Committee on the Judiciary on November 5, 2009. On December 7, 2009, CBO transmitted a cost estimate for H.R. 2221, the Data Accountability and Trust Act, as ordered reported by the House Committee on Energy and Commerce on September 30, 2009. Those bills address security breaches of sensitive personal information and notification requirements for the federal government and private industry. S. 1490 would require agencies to prepare additional reports for the Congress on the security of sensitive personal information held by the federal government. CBO estimates that preparing those reports and other security assessments would cost $25 million over the 2010-2014 period. H.R. 2221 would require the Federal Trade Commission to develop regulations to enforce new notification requirements. CBO estimates that it would cost that agency $5 million over the 2010-2014 period to carry out those activities.

CBO determined that S. 1490 and H.R. 2221 also contained intergovernmental mandates, but any costs would be small and would not exceed the threshold established in UMRA ($69 million in 2009, adjusted for inflation). In addition, CBO determined that S. 1490 and H.R. 2221 would impose private-sector mandates that would exceed the annual threshold established in UMRA ($139 million in 2009, adjusted annually for inflation) in at least one of the first five years the mandate are in effect.

ESTIMATE PREPARED BY:

Federal Costs: Mark Grabowicz and Matthew Pickford
Impact on State, Local, and Tribal Governments: Elizabeth Cove Delisle
Impact on the Private Sector: Marin Randall

ESTIMATE APPROVED BY:

Theresa Gullo
Deputy Assistant Director for Budget Analysis