SENATE BILL NO. 33

INTRODUCED BY D. STEINBEISSER

BY REQUEST OF THE ECONOMIC AFFAIRS INTERIM COMMITTEE

A BILL FOR AN ACT ENTITLED: "AN ACT REQUIRING STATE AND LOCAL GOVERNMENT AGENCIES TO DEVELOP PROCEDURES REGARDING SOCIAL SECURITY NUMBERS AND TO PROVIDE NOTIFICATION OF A COMPUTER SECURITY BREACH OF A GOVERNMENT AGENCY OR THIRD PARTY CONTRACTING WITH GOVERNMENT."

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MONTANA:

NEW SECTION. **Section 1. Definitions.** For the purposes of [sections 1 through 3], the following definitions apply:

(1) (a) "Breach of the security of a data system" or "breach" means unauthorized acquisition of computerized data that:

(i) materially compromises the security, confidentiality, or integrity of the personal information maintained by a governmental entity or by a third party on behalf of the governmental entity; and

(ii) causes or is reasonably believed to cause loss or injury to a person.

(b) Good faith acquisition of personal information by a governmental entity or a third party is not a breach of the security of a data system if the personal information is not used or subject to further unauthorized disclosure.

(2) (a) "Governmental entity" means:

(i) an agency, authority, board, bureau, commission, committee, council, department, office, institution, hospital, college, university, or other instrumentality of the legislative, judicial, and executive branches of the state; or

(ii) a county, city, municipal corporation, school district, or special improvement or taxing district, any other political subdivision or public corporation, or any entity created by an enumerated public entity.

(b) The term includes an employee of a governmental entity acting within the course and scope of employment.

(3) "Individual" means a human being.

(4) "Person" means an individual, partnership, corporation, association, governmental entity, or public

organization of any character.

(5) (a) "Personal information" means a first name or first initial and last name in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

(i) social security number or tax identification number;

(ii) driver's license number, an identification number issued pursuant to 61-12-501, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa; or

(iii) an account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial account.

(b) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(6) "Redaction" means the alteration of personal information contained within data to make all or a significant part of the data unreadable. The term includes truncation, which means that no more than the last four digits of an identification number are accessible as part of the data.

(7) "Third party" means a person with a contractual obligation to perform a function for a governmental entity or a separate governmental entity providing a function for another governmental entity.

NEW SECTION. **Section 2. Protection of social security numbers -- report.** (1) Each governmental entity that maintains the social security number of an individual shall develop procedures to protect the social security number while enabling the governmental entity to use the social security number as necessary for the performance of its duties under federal or state law.

(2) The procedures must include measures to:

(a) eliminate unnecessary use of social security numbers;

(b) identify the persons or governmental entities authorized to have access to the social security numbers;

(c) restrict access to social security numbers by unauthorized persons or governmental entities;

(d) identify circumstances when redaction of social security numbers is appropriate;

(e) dispose of documents that contain social security numbers in a manner consistent with other record retention requirements applicable to the governmental entity;

(f) eliminate the unnecessary storage of social security numbers on portable devices; and

(g) protect data on portable devices containing social security numbers.

(3) Each governmental entity shall complete the requirements of this section by September 1, 2008.

NEW SECTION. **Section 3. Notification of government computer data breach.** (1) A governmental entity that maintains computerized data containing personal information shall make reasonable efforts to provide notification of any breach of the security of a data system following discovery or notification of the breach to any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (3), or consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system.

(2) (a) A third party that receives personal information from a governmental entity and maintains that information in a computerized data system in order to perform a governmental entity function shall:

(i) notify the governmental entity immediately following discovery of the breach of the security of a data system if the personal information is reasonably believed to have been acquired by an unauthorized person; and

(ii) make reasonable efforts to provide notification of any breach following discovery or notification of the breach to any person whose unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. This notification must be provided in the same manner as the notification required in subsection (1).

(b) The governmental entity notified of a breach by a third party has no independent duty to provide notification of the breach if the third party has provided notification of the breach in the manner required by subsection (2)(a) but shall provide notification if the third party fails to do so in a reasonable time and may recover from the third party its reasonable costs for providing the notice.

(3) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation and requests a delay of notification. The notification required by this section must be made after the law enforcement agency determines that the notification will not compromise the investigation.

(4) All governmental entities and third parties to whom personal information is disclosed by a governmental entity shall develop and maintain:

(a) an information security policy designed to safeguard personal information; and

(b) breach notification procedures that provide reasonable notice to individuals as provided in subsections (1) and (2).

NEW SECTION. **Section 4. Codification instruction.** [Sections 1 through 3] are intended to be codified as an integral part of Title 2, and the provisions of Title 2 apply to [sections 1 through 3].

- END -