SENATE BILL NO. 50

INTRODUCED BY D. BARTEL

BY REQUEST OF THE DEPARTMENT OF ADMINISTRATION

A BILL FOR AN ACT ENTITLED: “AN ACT REQUIRING STATE AGENCIES AND THIRD PARTIES TO REPORT SECURITY INCIDENTS; DEFINING "CHIEF INFORMATION SECURITY OFFICER" AND "SECURITY INCIDENT"; AND AMENDING SECTIONS 2-6-1501, 2-6-1502, AND 2-6-1503, MCA.”

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

NEW SECTION. **Section 1. Immediate notification.** On discovery or notification of a security incident, a state agency shall provide immediate notification without unreasonable delay to the chief information security officer.

Section 2. Section 2-6-1501, MCA, is amended to read:

"**2-6-1501. Definitions.** As used in this part, the following definitions apply:

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

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

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

(2) "Chief information security officer" means an employee at the department of administration designated by the chief information officer who is responsible for protecting the state's information assets and citizens' data by:

(a) advising and overseeing information security strategy and programs for executive branch state agencies without elected officials; and

(b) advising and consulting information security strategy and programs for executive branch state agencies with elected officials and the legislative and judicial branches.

~~(2)~~(3) "Individual" means a human being.

~~(3)~~(4) "Person" means an individual, a partnership, a corporation, an association, or a public organization of any character.

~~(4)~~(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 data elements are not encrypted:

(i) a social security number;

(ii) a driver's license number, an identification card number issued pursuant to 61-12-501, a tribal identification number or enrollment number, 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;

(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;

(iv) medical record information as defined in 33-19-104;

(v) a taxpayer identification number; or

(vi) an identity protection personal identification number issued by the United States internal revenue service.

(b) The term does not include publicly available information from federal, state, local, or tribal government records.

~~(5)~~(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) "Security incident" means an occurrence that:

(a) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits; or

(b) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

~~(6)~~(8) (a) "State agency" means an agency, authority, board, bureau, college, commission, committee, council, department, hospital, institution, office, university, or other instrumentality of the legislative or executive branch of state government. The term includes an employee of a state agency acting within the

course and scope of employment.

(b) The term does not include an entity of the judicial branch.

~~(7)~~(9) "Third party" means:

(a) a person with a contractual obligation to perform a function for a state agency; or

(b) a state agency with a contractual or other obligation to perform a function for another state agency."

Section 3. Section 2-6-1502, MCA, is amended to read:

"**2-6-1502. Protection of personal information -- compliance -- extensions.** (1) Each state agency that maintains the personal information of an individual shall develop procedures to protect the personal information while enabling the state agency to use the personal information as necessary for the performance of its duties under federal or state law.

(2) The procedures must include measures to:

(a) eliminate the unnecessary use of personal information;

(b) identify the person or state agency authorized to have access to personal information;

(c) restrict access to personal information by unauthorized persons or state agencies;

(d) identify circumstances in which redaction of personal information is appropriate;

(e) dispose of documents that contain personal information in a manner consistent with other record retention requirements applicable to the state agency;

(f) eliminate the unnecessary storage of personal information on portable devices; and

(g) protect data containing personal information if that data is on a portable device.

(3) Except as provided in subsection (4), each state agency that is created after October 1, 2015, shall complete the requirements of this section within 1 year of its creation.

(4) The chief information officer provided for in 2-17-511 may grant an extension to any state agency subject to the provisions of the Montana Information Technology Act provided for in Title 2, chapter 17, part 5. The chief information officer shall inform ~~the information technology board~~ the governor, the office of budget and program planning, and the legislative finance committee of all extensions that are granted and of the rationale for granting the extensions. The chief information officer shall maintain written documentation that

identifies the terms and conditions of each extension and the rationale for the extension."

Section 4. Section 2-6-1503, MCA, is amended to read:

"**2-6-1503. Notification of breach of security of data system.** (1) (a) Upon discovery or notification of a breach of the security of a data system, a state agency that maintains computerized data containing personal information in the data system shall make reasonable efforts to notify any person whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person.

(b) The notification must be made without unreasonable delay, consistent with the legitimate needs of law enforcement as provided in subsection (3) or 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 state agency and maintains that information in a computerized data system to perform a state agency function shall:

(i) notify the state agency immediately following discovery of the breach if the personal information is reasonably believed to have been acquired by an unauthorized person; and

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

(b) A state agency 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 state agencies and third parties to whom personal information is disclosed by a state agency 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).

(5) A state agency or third party that is required to issue a notification to an individual pursuant to this section shall simultaneously submit to the state's chief information security officer at the department of administration and to the attorney general's consumer protection office an electronic copy of the notification and a statement providing the date and method of distribution of the notification. The electronic copy and statement of notification must exclude any information that identifies the person who is entitled to receive notification. If notification is made to more than one person, a single copy of the notification that includes the number of people who were notified must be submitted to the chief information officer and the consumer protection office."

NEW SECTION. **Section 5. Codification instruction.** [Section 1] is intended to be codified as an integral part of Title 2, chapter 6, part 15, and the provisions of Title 2, chapter 6, part 15, apply to [section 1].

- END -