LC7800 Explanation:

Government Regulation of Social Security Numbers, Data Breaches

Background:

- Work group on Identity Theft requested survey to determine how government uses social security numbers (SSNs).
  - Survey presented at July 14, 2006, meeting. Various uses, some because of federal law, some required by state law, some by rule. Lack of uniformity on whether an agency says the request for a SSN is mandatory or voluntary.
- Work group requested that government be responsible for notifying about computer security data breaches -- as business now is required under 30-14-1704, MCA (see endnote)[1] and its similar version for the insurance industry, 33-19-321, MCA.
- Staff developed for review at the July 14, 2006, meeting:
  - LC zzzz, regarding regulation of collection and use of SSNs;
  - LC8800, regarding computer breach notification; and
  - LC8899, regarding government employees' use of portable devices, etc., to safeguard any personal information contained on the devices.
- Economic Affairs Committee recommended staff work with government representatives to address SSN, breach issues. Staff met August 10, 2006, to review bill drafts provided by Gov. Schweitzer's legal counsel, Ann Brodsky.
- The combined draft, LC7800, is a product of the discussions at the August 10 meeting plus some additional fine tuning.

Issues:

- State agencies worried in general that specific regulations -- a one-size-fits-all approach would be problematic for the many ways that state agencies use SSNs. The suggested bill allows governmental entities to set their own policies.
  - **LC7800 SECTION 1:** Definitions.
    - "Agency head" – see subissue below under subsection 2(3). This language may need clarification or may not be needed if no report is to be made to agency heads.
    - "Breach of the security..." -- basically uses definition in 30-14-1704. Includes the word "materially" - which is missing in insurance industry reference due to amending of HB732's business section, which was missed for insurance section.
    - "Governmental entity" -- includes all branches of government (state and local). Also includes employee of governmental entity acting within scope of job.
    - "Personal information" -- covers only an individual's personal information, and not the personal information (tax ID number) of any business. There is an argument for changing this to cover all "persons" and if that is done, then equivalent changes should be made in 30-14-1704 and 33-19-321.
  - **LC7800, SECTION 2 (1):** Allows each agency to adopt own policy on protecting SSNs.
  - Subsection 2(2): Outlines measures that policies need to address.
  - Subsection 2(3): Provides for a report to an agency head, or a representative.
    - **Subissues**:
    - regarding whether the "executive" branch power lies with the governor and, if so,

whether requiring governmental entities to report to agency heads could be confusing – does everyone in the "executive" branch (including, for example, the attorney general) report to the governor? May need clarification language.
    - regarding reporting provision. Is a report necessary? Many laws are enacted without a report required. Alternately, should the report be to the Economic Affairs Committee and, if so, just a one-time report?
- **LC7800, SECTION 3.** Breach notification procedures for government.
    - Some emphasis on third party notification (not the same as in business/ insurance bills). Presumably a state contract with a third party would cover terms of computer security breaches, but -- if not -- the language in this section is intended to cover what happens in the event of a security breach at the third party that would result in state-gathered personal information being disclosed.
    - Subsection (4) requires policy for safeguarding personal information and breach notification procedures. 30-14-1704 and 33-19-321 spell out what the notification procedures are to be. Question of whether there should be uniformity in notification procedures. Original LC8800 provided for Lewis and Clark County Attorney to act if the Attorney General's office had a computer security breach. No longer needed with this approach.
    - A representative of the Montana Association of Counties worried in particular about LC8899's approach that said "course and scope of work" explanation was an insufficient defense if someone violated terms of use of portable devices containing personal data.

- Codification instruction needed. Suggest this be in Title 2, which deals with government. Part of the problem with LC8800 was that the inclusion of the government security breach regulation with the consumer protection part of MCA was problematic on many fronts. A separate section codified in the government code portion of MCA is preferable.

1. **30-14-1704. (Effective March 1, 2006) Computer security breach.** (1) Any person or business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. The disclosure 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 restore the reasonable integrity of the data system.

(2) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person.

(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 in notification. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

(4) For purposes of this section, the following definitions apply:

(a) "Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person or business and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (i) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) social security number;

(B) driver's license number or state identification card number;

LC7800 Explanation:
Government Regulation of Social Security Numbers, Data Breaches

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

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

(5) (a) For purposes of this section, notice may be provided by one of the following methods:

(i) written notice;

(ii) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. 7001;

(iii) telephonic notice; or

(iv) substitute notice, if the person or business demonstrates that:

(A) the cost of providing notice would exceed $250,000;

(B) the affected class of subject persons to be notified exceeds 500,000; or

(C) the person or business does not have sufficient contact information.

(b) Substitute notice must consist of the following:

(i) an electronic mail notice when the person or business has an electronic mail address for the subject persons; and

(ii) conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; or

(iii) notification to applicable local or statewide media.

(6) Notwithstanding subsection (5), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and that does not unreasonably delay notice is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the data system.

(7) If a business discloses a security breach to any individual pursuant to this section and gives a notice to the individual that suggests, indicates, or implies to the individual that the individual may obtain a copy of the file on the individual from a consumer credit reporting agency, the business shall coordinate with the consumer reporting agency as to the timing, content, and distribution of the notice to the individual. The coordination may not unreasonably delay the notice to the affected individuals.