COLORADO RURAL ELECTRIC ASSOCIATION

Legislative Memorandum

HB18-1128 – *Concerning Strengthening protections for consumer data privacy*.
Representatives Bridges (D-Greenwood Village), Wist (R-Centennial)
Senators Lambert (R-Colorado Springs) Court (D-Denver)

The purpose of this memo is to provide a high-level review of House Bill 18-1128, which is a very complicated, 22-page piece of legislation. The bill clearly requires co-ops to develop policies for the protection and disposal of personal identifying information that is "maintained" by the co-op during the course of business. We believe co-ops already have such policies, but may want to review them in light of the new requirements in the bill. We also believe co-ops should take appropriate steps to comply with the requirements of HB18-1128 as they apply to security breaches. Again, we believe co-ops already have policies in place for such events, but may want to compare existing policies to the requirements of HB18-1128.

Colorado Consumer Protection Act & HB18-1128
The Colorado Consumer Protection Act (CCPA) requires individuals, businesses and other legal and commercial entities to protect the "personal identifying information" of Colorado residents. The CCPA requires businesses and individuals who use documents that contain personal identifying information to develop policies for the "destruction or proper disposal" of the information. Personal identifying information includes social security numbers, other personal identification numbers, passwords, passcodes, driver's license or passport numbers, biometric data, and financial transaction devices such as credit and debit cards.

The purpose of HB 18-1128 is to clarify and expand the current protections for personal identifying information, to require remedial measures to be taken in the event of a security breach, and to establish similar requirements for governmental agencies.

Protection and disposal of personal identifying information by <u>non-governmental</u> entities :
HB18-1128 requires each "covered entity" in the state that maintains personal identifying information in the course of the person's business, vocation or occupation to protect that information from unauthorized use and to implement reasonable security procedures that are "appropriate to the nature of the personal identifying information and the nature and size of

the business and its operations." The bill further requires covered entities to develop a written policy ensuring that all records are destroyed and rendered unreadable when they are no longer needed by the covered entity.

The bill specifically authorizes covered entities to disclose personal identifying information to third parties (i.e., co-ops providing customer information to NISC for billing purposes) so long as the covered entity requires the third-party service provider to implement appropriate security measures.

Notification of security breach:

HB18-1128 also expands the existing law with respect to requirements for disclosure of security breaches. A "security breach" means the "unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity." The bill provides that if a covered entity determines that personal information has been or will be misused as the result of a security breach, the covered entity is required, at its own cost, to notify affected individuals no later than 30 days after the date of determination that a security breach has occurred. The bill sets out certain requirements for the notice, including the dates of the breach; a description of the personal information that was acquired; contact information for the covered entity that can be used by the person whose information was misused; and other contact information. If the covered entity uses a third party service provider to maintain computerized data that includes personal information, the third party service provider is required to give notice to the covered entity about any security breach "in the most expedient time possible."

In addition to the notice, the covered entity is required to contact the person whose personal information has been breached and ask them to change passwords or other security questions and answers or take other appropriate steps to protect the online accounts with the covered entity.

If the security breach impacts 500 or more Colorado residents, HB18-1128 requires that the Colorado attorney general be notified within 30 days of the breach unless the attorney general determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur. The attorney general is required to designate a point of contact for a breach such as this and make that person's contact information public.

It is important to note that the term "personal information" that is used in the security breach section is different than the term "personal identifying information" that is used in the section requiring protection of that information. For purposes of the security breach section, "personal information" includes a Colorado resident's first name or first initial, and last name in combination with one or more of the following:

- social security number;
- student, military, or passport identification number;
- driver's license or identification card number;

- medical information;
- health insurance identification number;
- biometric data;
- a Colorado resident's username or email address in combination with a password that would permit access to an online account;
- a Colorado resident's account number or credit or debit card number in combination with any required security code or password that would permit access to that account.

Personal information does not include publicly available information made available to the general public from federal, state, or local government records.

Protection and disposal of personal identifying information by <u>governmental</u> entities:
In general, HB18-1128 extends the same obligations for protecting personal identifying information and providing notifications of security breaches that apply to private individuals and businesses to governmental entities (there are some provisions that are unique to governmental entities). "Governmental entity" includes the state, counties, cities, school districts, special districts and all other political subdivisions of the state.