..... moves to amend H.F. No. 183, in conference committee, as follows:

Page R1, Senate language (UEH0183-1)

Page 2, after line 3 insert:

"Section 1. Minnesota Statutes 2012, section 13.04, subdivision 4, is amended to read:

Subd. 4. **Procedure when data is not accurate or complete, or is improperly accessed.** (a) An individual subject of the data may contest the accuracy or completeness of public or private data. To exercise this right, an individual shall notify in writing the responsible authority describing the nature of the disagreement.

The responsible authority shall, within 30 days, either:

(1) correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or

(2) notify the individual that the authority believes the data to be correct. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

(b) If an individual subject of private data believes that the individual's private data has been accessed by a government entity, or an employee, contractor, or agent of the entity, in a manner not authorized by law, the individual may contest the access to the data. To exercise this right, the individual shall notify the responsible authority of the contest, in writing, and describe the grounds for believing the individual's private data was accessed in a manner not authorized by law. In response to a contest under this paragraph, the responsible authority shall, within 30 days, either:

(1) justify the government entity's access to the data by describing the purpose for the access and the statute that authorizes access for that purpose; or

(2) notify the individual of a breach in the security of the individual's data, and proceed in the manner required by section 13.055.

(c) The determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act relating to contested cases. Upon receipt

of an appeal by an individual, the commissioner shall, before issuing the order and notice of a contested case hearing required by chapter 14, try to resolve the dispute through education, conference, conciliation, or persuasion. If the parties consent, the commissioner may refer the matter to mediation. Following these efforts, the commissioner shall dismiss the appeal or issue the order and notice of hearing.

~~(b)~~ (d) Data on individuals that have been successfully challenged by an individual as inaccurate or incomplete must be completed, corrected, or destroyed by a government entity without regard to the requirements of section 138.17.

After completing, correcting, or destroying successfully challenged data, a government entity may retain a copy of the commissioner of administration's order issued under chapter 14 or, if no order were issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data."

On R4, Senate language, (UEH0183-1)

Page 5, after line 9 insert:

"(c) A public employee whose conduct constitutes an unauthorized acquisition of not public data, as defined in section 13.055, subdivision 1, must be issued a letter of reprimand for that conduct, provided that the issuance of a letter of reprimand does not prohibit additional penalties allowed by this section or other law related to the conduct. Nothing in this paragraph limits any right of appeal or grievance procedure afforded to the public employee pursuant to law or contract."

On R4, Senate language (UEH0183-2)

Page 5, after line 11 insert:

"Sec. 4. Minnesota Statutes 2012, section 16E.03, subdivision 7, is amended to read:

Subd. 7. **Cyber security systems.** In consultation with the attorney general and appropriate agency heads, the chief information officer shall develop cyber security policies, guidelines, and standards, and shall install and administer state data security systems on the state's computer facilities consistent with these policies, guidelines, standards, and state law to ensure the integrity of computer-based and other data and to ensure applicable limitations on access to data, consistent with the public's right to know as defined in chapter 13. The data security systems must include the capacity to audit access to not public data maintained by a state agency, including tracking the identities of individuals who access not public data and the purposes for which the access occurs. The chief information officer is responsible for overall security of state agency networks connected to the Internet. Each department or agency head is responsible for the security of the department's or agency's data within the guidelines of established enterprise policy."

Renumber the sections in sequence and correct the internal references

Amend the title accordingly