Senator Dziedzic from the Committee on State and Local Government and Veterans, to which was referred

S.F. No. 4874: A bill for an act relating to cybersecurity; requiring reporting of cybersecurity incidents impacting public-sector organizations in Minnesota; proposing coding for new law in Minnesota Statutes, chapter 16E.

Reports the same back with the recommendation that the bill be amended as follows:

Page 1, after line 8, insert:

"(b) "Bureau" means the Bureau of Criminal Apprehension."

Reletter the paragraphs in sequence

Page 1, line 9, delete "actions" and insert "an action"

Page 1, line 10, delete "result" and insert "results"

Page 2, line 28, after the period, insert "The term information technology also has the meaning described to information and telecommunications technology systems and services in section 16E.03, subdivision 1, paragraph (b)."

Page 2, delete lines 29 to 31

Page 3, line 5, delete "and"

Page 3, line 6, before the period, insert ", and public postsecondary education institutions"

Page 3, after line 6, insert:

"(l) "Superintendent" means the superintendent of the Bureau of Criminal Apprehension."

Page 3, delete subdivision 2 and insert:

"Subd. 2. **Report on cybersecurity incidents.** (a) Beginning December 1, 2024, the head of or the decision making body for a public agency must report a cybersecurity incident that impacts the public agency to the commissioner. A government contractor or vendor that provides goods or services to a public agency must report a cybersecurity incident to the public agency if the incident impacts the public agency.

(b) The report must be made within 72 hours of when the public agency or government contractor reasonably identifies or believes that a cybersecurity incident has occurred.

(c) The commissioner must coordinate with the superintendent to promptly share reported cybersecurity incidents.

(d) By September 30, 2024, the commissioner, in coordination with the superintendent, must establish a cyber incident reporting system having capabilities to facilitate submission

of timely, secure, and confidential cybersecurity incident notifications from public agencies, government contractors, and private entities to the office.

(e) By September 30, 2024, the commissioner must develop, in coordination with the superintendent, and prominently post instructions for submitting cybersecurity incident reports on the websites for the department and for the bureau. The instructions must include, at a minimum, the types of cybersecurity incidents to be reported and a list of other information to be included in the report made through the cyber incident reporting system.

(f) The cyber incident reporting system must permit the commissioner, in coordination with the superintendent, to:

(1) securely accept a cybersecurity incident notification from any individual or private entity, regardless of whether the entity is a public agency or government contractor;

(2) track and identify trends in cybersecurity incidents reported through the cyber incident reporting system; and

(3) produce reports on the types of incidents, cyber threat, indicators, defensive measures, and entities reported through the cyber incident reporting system.

(g) Any cybersecurity incident report submitted to the commissioner is security information pursuant to section 13.37 and is not discoverable in a civil or criminal action absent a court or a search warrant, and is not subject to subpoena.

(h) Notwithstanding the provisions of paragraph (g), the commissioner may anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks and share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

(i) Information submitted to the commissioner through the cyber incident reporting system shall be subject to privacy and protection procedures developed and implemented by the office, which shall be based on the comparable privacy protection procedures developed for information received and shared pursuant to the federal Cybersecurity Information Sharing Act of 2015, United States Code, title 6, section 1501, et seq."

Page 4, delete subdivision 3 and insert:

"Subd. 3. **Annual report to the governor and legislature.** Beginning January 31, 2026, and annually thereafter, the commissioner, in coordination with the superintendent, must submit a report on its cyber security incident report collection and resolution activities to the governor and to the legislative commission on cybersecurity. The report must include, at a minimum:

(1) information on the number of notifications received and a description of the cybersecurity incident types during the one-year period preceding the publication of the report;

(2) the categories of reporting entities that submitted cybersecurity reports; and

(3) any other information required in the submission of a cybersecurity incident report, noting any changes from the report published in the previous year."

Page 4, delete line 25

And when so amended the bill do pass and be re-referred to the Committee on Judiciary and Public Safety. Amendments adopted. Report adopted.

.....
(Committee Chair)

April 5, 2024.....
(Date of Committee recommendation)