

- 1.1 Senator moves to amend S.F. No. 4874 as follows:
- 1.2 Page 1, after line 8, insert:
- 1.3 "(b) "Bureau" means the Bureau of Criminal Apprehension."
- 1.4 Page 1, line 9, delete "(b)" and insert "(c)" and delete "actions" and insert "an action"
- 1.5 Page 1, line 10, delete "result" and insert "results"
- 1.6 Page 1, line 12, delete "(c)" and insert "(d)"
- 1.7 Page 2, line 6, delete "(d)" and insert "(e)"
- 1.8 Page 2, line 14, delete "(e)" and insert "(f)"
- 1.9 Page 2, line 17, delete "(f)" and insert "(g)"
- 1.10 Page 2, line 19, delete "(g)" and insert "(h)"
- 1.11 Page 2, line 22, delete "(h)" and insert "(i)"
- 1.12 Page 2, line 28, after the period, insert "The term information technology also has the
- 1.13 meaning described to information and telecommunications technology systems and services
- 1.14 in section 16E.03, subdivision 1, paragraph (b)."
- 1.15 Page 2, delete lines 29 to 31
- 1.16 Page 3, line 1, delete "(i)" and insert "(j)"
- 1.17 Page 3, line 4, delete "(j)" and insert "(k)"
- 1.18 Page 3, line 5, delete "and"
- 1.19 Page 3, line 6, before the period, insert ", and public postsecondary education institutions"
- 1.20 Page 3, after line 6, insert:
- 1.21 "(l) "Superintendent" means the superintendent of the Bureau of Criminal Apprehension."
- 1.22 Page 3, delete subdivision 2 and insert:
- 1.23 "Subd. 2. **Report on cybersecurity incidents.** (a) Beginning December 1, 2024, the
- 1.24 head of or the decision making body for a public agency must report a cybersecurity incident
- 1.25 that impacts the public agency, to the commissioner. A government contractor or vendor
- 1.26 that provides goods or services to a public agency must report a cybersecurity incident to
- 1.27 the public agency if the incident impacts the public agency.
- 1.28 (b) The report must be made within 72 hours of when the public agency or government
- 1.29 contractor reasonably identifies or believes that a cybersecurity incident has occurred.

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

2.3 (d) By September 30, 2024, the commissioner, in coordination with the superintendent,
2.4 must establish a cyber incident reporting system having capabilities to facilitate submission
2.5 of timely, secure, and confidential cybersecurity incident notifications from public agencies,
2.6 government contractors, and private entities to the office.

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

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

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

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

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

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

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

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

2.32 Page 4, delete subdivision 3 and insert:

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

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

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

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

3.12 Page 4, delete line 25