



Reprinted
February 18, 2025

SENATE BILL No. 472

DIGEST OF SB 472 (Updated February 17, 2025 3:34 pm - DI 119)

Citations Affected: IC 4-13.1; IC 4-13.2; IC 24-4; IC 24-4.9; IC 24-15.

Synopsis: Cybersecurity. Requires political subdivisions, state agencies, school corporations, and state educational institutions (public entities), with the exception of specified categories of hospitals, to adopt not later than December 31, 2027, a: (1) technology resources policy; and (2) cybersecurity policy; that meet specified requirements. Requires the office of technology (office) to develop: (1) standards and guidelines regarding cybersecurity for use by political subdivisions and state educational institutions; and (2) a uniform cybersecurity policy for use by state agencies. Requires the office to develop, in collaboration with the department of education: (1) a uniform technology resources policy governing use of technology resources by the employees of school corporations; and (2) a uniform cybersecurity policy for use by school corporations. Requires: (1) a public entity to biennially submit
(Continued next page)

Effective: July 1, 2025; January 1, 2026.

**Brown L, Buchanan,
Randolph Lonnie M**

January 13, 2025, read first time and referred to Committee on Commerce and Technology.
January 23, 2025, amended, reported favorably — Do Pass; reassigned to Committee on Appropriations.
February 13, 2025, amended, reported favorably — Do Pass.
February 17, 2025, read second time, amended, ordered engrossed.

SB 472—LS 7298/DI 119



to the office the cybersecurity policy adopted by the public entity; and (2) the office to establish a procedure for collecting and maintaining a record of submitted cybersecurity policies. Requires a public entity that engages a third party to conduct an assessment of the public entity's cybersecurity policy to provide the results of the assessment to the office. Establishes: (1) the cybersecurity insurance program (program) for the purpose of providing coverage to a participating government entity for losses incurred by the government entity as a result of a cybersecurity incident; and (2) the cybersecurity insurance board (board) to administer the program. Provides that coverage for losses incurred by a participating government entity as a result of a cybersecurity incident are paid under the program from premiums paid into a trust fund by participating government entities. Specifies that claims from the fund shall not be paid until the balance in the fund reaches \$10,000,000. Provides that the board shall contract with cybersecurity professionals who can be dispatched by the board to assist a participating government entity in the event of a cybersecurity incident. Provides that fines recovered by the attorney general for any of the following violations are deposited in the trust fund: (1) Failure of an adult oriented website to implement or properly use a reasonable age verification method. (2) Failure of a data base owner to safeguard personal information of Indiana residents. (3) Failure of a data base owner to disclose or provide notice of a security breach. (4) Violation of consumer data protection law. Makes an appropriation.



Reprinted
February 18, 2025

First Regular Session of the 124th General Assembly (2025)

PRINTING CODE. Amendments: Whenever an existing statute (or a section of the Indiana Constitution) is being amended, the text of the existing provision will appear in this style type, additions will appear in **this style type**, and deletions will appear in ~~this style type~~.

Additions: Whenever a new statutory provision is being enacted (or a new constitutional provision adopted), the text of the new provision will appear in **this style type**. Also, the word **NEW** will appear in that style type in the introductory clause of each SECTION that adds a new provision to the Indiana Code or the Indiana Constitution.

Conflict reconciliation: Text in a statute in *this style type* or ~~this style type~~ reconciles conflicts between statutes enacted by the 2024 Regular Session of the General Assembly.

SENATE BILL No. 472

A BILL FOR AN ACT to amend the Indiana Code concerning state offices and administration and to make an appropriation.

Be it enacted by the General Assembly of the State of Indiana:

- 1 SECTION 1. IC 4-13.1-4-2, AS ADDED BY P.L.108-2024,
2 SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
3 JULY 1, 2025]: Sec. 2. **(a) Except as provided in subsection (b), as**
4 **used in this chapter, "public entity" means a:**
5 (1) political subdivision;
6 (2) state agency;
7 (3) school corporation; or
8 (4) state educational institution.
9 **(b) The term does not include an acute care hospital licensed**
10 **under IC 16-21 that is established and operated under IC 16-22-2,**
11 **IC 16-22-8, or IC 16-23.**
12 SECTION 2. IC 4-13.1-4-5, AS ADDED BY P.L.108-2024,
13 SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
14 JULY 1, 2025]: Sec. 5. **(a) The office shall:**
15 (1) **develop:**
16 (A) **standards and guidelines regarding cybersecurity for**

SB 472—LS 7298/DI 119



- 1 use by political subdivisions and state educational
 2 institutions; and
 3 (B) a uniform cybersecurity policy for use by state
 4 agencies; and
 5 (2) develop, in collaboration with the department of
 6 education:
 7 (A) a uniform technology resources policy governing use of
 8 technology resources by the employees of a school
 9 corporation; and
 10 (B) a uniform cybersecurity policy for use by school
 11 corporations.
 12 (b) Not later than December 31, 2027, each public entity may
 13 shall adopt the following:
 14 (1) A policy governing use of technology resources by the public
 15 entity's employees. The policy may: If the public entity is a
 16 school corporation, the public entity shall adopt the uniform
 17 technology resources policy developed under subsection
 18 (a)(2)(A).
 19 (A) prohibit an employee of the public entity from using the
 20 public entity's technology resources to:
 21 (i) engage in lobbying (as defined in IC 2-7-1-9) that is
 22 outside the scope of the employee's duties;
 23 (ii) engage in illegal activity; or
 24 (iii) violate the public entity's cybersecurity policy; and
 25 (B) include disciplinary procedures for violation of the
 26 technology resources policy.
 27 (2) A cybersecurity policy If the public entity is: as follows:
 28 (A) If the public entity is a political subdivision or state
 29 educational institution, the public entity shall adopt a
 30 cybersecurity policy may be based on standards and
 31 guidelines developed by the office under subsection
 32 (a)(1)(A).
 33 (B) If the public entity is a school corporation, the policy may
 34 be based on public entity shall adopt the uniform
 35 cybersecurity policy standards and guidelines developed by the
 36 office, in collaboration with the department of education; and
 37 under subsection (a)(2)(B).
 38 (C) If the public entity is a state agency, the public entity
 39 shall adopt the uniform cybersecurity policy is developed by
 40 the office: under subsection (a)(1)(B).
 41 (3) A training program regarding the public entity's technology
 42 resources policy adopted under subdivision (1) and cybersecurity



policy adopted under subdivision (2), completion of which is mandatory for the public entity's employees.

(c) The uniform technology resources policy developed under subsection (a)(2)(A) and a technology resources policy adopted by a public entity other than a school corporation under subsection (b)(1) must:

(1) prohibit an employee of the public entity from using the public entity's technology resources to:

(A) engage in lobbying (as defined in IC 2-7-1-9) that is outside the scope of the employee's duties;

(B) engage in illegal activity; or

(C) violate the public entity's cybersecurity policy; and

(2) include disciplinary procedures for violation of the technology resources policy.

SECTION 3. IC 4-13.1-4-6, AS ADDED BY P.L.108-2024, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 6. (a) Not later than December 31 of each odd-numbered year, a public entity ~~may~~ **shall** submit to the office the public entity's cybersecurity policy adopted by the public entity under section 5 of this chapter.

(b) The office ~~may~~ **shall** establish a procedure for collecting and maintaining a record of cybersecurity policies submitted to the office under subsection (a).

(c) If a public entity engages a third party to conduct an assessment of the public entity's cybersecurity policy, the public entity shall provide the results of the assessment to the office.

SECTION 4. IC 4-13.2 IS ADDED TO THE INDIANA CODE AS A NEW ARTICLE TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]:

ARTICLE 13.2. CYBERSECURITY INSURANCE PROGRAM

Chapter 1. Definitions

Sec. 1. The definitions in this chapter apply throughout this article.

Sec. 2. "Board" means the cybersecurity insurance board established by IC 4-13.2-4-1.

Sec. 3. "Covered cybersecurity incident" means a cybersecurity incident that is determined by the board to be eligible for coverage under IC 4-13.2-4-2.

Sec. 4. "Cyber response agent" means a cybersecurity professional with which the board enters into a contract under IC 4-13.2-4-2.

Sec. 5. "Cybersecurity incident" has the meaning set forth in



1 **IC 4-13.1-1-1.5.**

2 **Sec. 6. "Cybersecurity professional" means an individual who:**

3 **(1) has documented experience in responding to cybersecurity**
 4 **incidents; and**

5 **(2) is qualified to provide services such as:**

6 **(A) forensic analysis of a cybersecurity incident; and**

7 **(B) software, hardware, and data restoration after a**
 8 **cybersecurity incident.**

9 **Sec. 7. "Designated contact" means the person designated by the**
 10 **board under IC 4-13.2-4-2(5).**

11 **Sec. 8. "Executive" means:**

12 **(1) the governor, with respect to the state;**

13 **(2) the:**

14 **(A) board of county commissioners, with respect to a**
 15 **county that does not have a consolidated city; or**

16 **(B) mayor of the consolidated city, with respect to a county**
 17 **that has a consolidated city;**

18 **(3) the mayor, with respect to a city;**

19 **(4) the president of the town council, with respect to a town;**

20 **(5) the superintendent, with respect to a school corporation;**
 21 **and**

22 **(6) the president of the state educational institution, with**
 23 **respect to a state educational institution.**

24 **Sec. 9. "Fund" means the cybersecurity insurance trust fund**
 25 **established by IC 4-13.2-3-1.**

26 **Sec. 10. "Government entity" means:**

27 **(1) the state;**

28 **(2) a county;**

29 **(3) a city;**

30 **(4) a town;**

31 **(5) a school corporation; or**

32 **(6) a state educational institution.**

33 **Sec. 11. "Office" means the office of technology established by**
 34 **IC 4-13.1-2-1.**

35 **Sec. 12. "Participating government entity" means a government**
 36 **entity that has enrolled in the program under IC 4-13.2-2-3.**

37 **Sec. 13. "Program" refers to the cybersecurity insurance**
 38 **program established by IC 4-13.2-2-1.**

39 **Sec. 14. "School corporation" means:**

40 **(1) a school corporation (as defined in IC 20-18-2-16(a)); and**

41 **(2) a charter school.**

42 **Sec. 15. "State educational institution" has the meaning set**



1 forth in IC 21-7-13-32.

2 **Chapter 2. Program Establishment and Participation**

3 **Sec. 1.** The cybersecurity insurance program is established for
4 the purpose of providing coverage to a participating government
5 entity for losses incurred by the government entity as a result of a
6 cybersecurity incident.

7 **Sec. 2.** The board shall administer the program.

8 **Sec. 3.** The executive of a government entity may enroll the
9 government entity in the program by submitting an application:

10 (1) to the board; and

11 (2) in the form and manner specified by the board;
12 on behalf of the government entity.

13 **Chapter 3. Cybersecurity Insurance Trust Fund**

14 **Sec. 1. (a)** The cybersecurity insurance trust fund is established
15 for the purposes of:

16 (1) paying claims to participating government entities under
17 the program;

18 (2) making payments to cybersecurity professionals under
19 contracts entered into by the board under IC 4-13.2-4-2; and

20 (3) paying the operating expenses of the board.

21 (b) The fund is a trust fund for purposes of IC 4-9.1-1-7.

22 (c) The budget agency shall administer the fund.

23 (d) The fund consists of:

24 (1) premiums paid by participating government entities under
25 IC 4-13.2-6;

26 (2) appropriations to the fund by the general assembly;

27 (3) civil penalties collected under:

28 (A) IC 24-4-23-15;

29 (B) IC 24-4.9-3-3.5;

30 (C) IC 24-4.9-4-2; and

31 (D) IC 24-15-10-2; and

32 (4) grants, gifts, and donations intended for deposit in the
33 fund.

34 (e) Money in the fund at the end of a state fiscal year does not
35 revert to the state general fund.

36 (f) Notwithstanding any other provision, claims from the fund
37 shall not be paid until the balance in the fund reaches ten million
38 dollars (\$10,000,000).

39 **Chapter 4. Cybersecurity Insurance Board**

40 **Sec. 1. (a)** The cybersecurity insurance board is established as
41 a continuing board under the executive branch of state government
42 for the purpose of administering the cybersecurity insurance



1 program.

2 (b) The board consists of the following members:

3 (1) The chief information officer of the office or a designee of
4 the chief information officer.

5 (2) Three (3) members appointed by the governor:

6 (A) one (1) of whom is a representative of Indiana
7 counties;

8 (B) one (1) of whom is a representative of Indiana cities;
9 and

10 (C) one (1) of whom is a representative of Indiana towns.

11 (3) If the state participates in the program, the governor or
12 the governor's designee.

13 (4) If a state educational institution participates in the
14 program, one (1) representative of state educational
15 institutions who is appointed to the board by the governor.

16 (5) The insurance commissioner or a designee of the insurance
17 commissioner.

18 (6) The secretary of education or a designee of the secretary
19 of education.

20 (7) The executive director of the department of homeland
21 security or a designee of the executive director of the
22 department of homeland security.

23 (8) The state comptroller or a designee of the state
24 comptroller.

25 (c) The chief information officer, or the chief information
26 officer's designee under subsection (b)(1), serves as:

27 (1) chair; and

28 (2) a nonvoting member;

29 of the board.

30 (d) If a member of the general assembly is appointed to the
31 board, the member is a nonvoting member.

32 (e) An appointed member of the board serves at the will of the
33 member's appointing authority.

34 (f) The term of an appointed member of the board is as follows:

35 (1) An appointed member who is not a member of the general
36 assembly serves a six (6) year term that ends June 30, 2031,
37 and June 30 of every sixth year thereafter.

38 (2) An appointed member who is a member of the general
39 assembly serves a two (2) year term that ends June 30, 2027,
40 and June 30 of every odd-numbered year thereafter.

41 An appointed member of the board may be reappointed at the
42 conclusion of the member's term.



(g) A vacancy on the board shall be filled by the appointing authority of the member whose position on the board is vacant to meet the same qualifications as the vacating member.

(h) The board:

(1) shall meet:

(A) for the first time not later than September 30, 2025;
and

(B) for the second time not later than December 31, 2025;
at the call of the chair;

(2) subject to subsection (i), shall meet at the call of the chair at least one (1) time each quarter during 2026 and each year thereafter;

(3) shall meet as required under IC 4-13.2-7-3; and

(4) may meet at any time at the call of:

(A) the chair; or

(B) a majority of the members of the board.

(i) The chair may cancel a meeting of the board scheduled under subsection (h)(2) if the chair determines that, as of twenty-four (24) hours before the scheduled time of the meeting:

(1) no claim has been submitted under this article requiring the board's consideration; and

(2) no other matter requires the board's consideration.

(j) A majority of the members of the board constitutes a quorum. The affirmative votes of a majority of the voting members of the board are required for the board to take action.

(k) The office shall staff the board.

(l) Except as provided in subsection (o), the expenses of the board shall be paid from the fund.

(m) A member of the board who is not a state employee is not entitled to the minimum salary per diem provided by IC 4-10-11-2.1(b). The member is, however, entitled to reimbursement for mileage and traveling expenses as provided under IC 4-13-1-4 and other expenses actually incurred in connection with the member's duties as provided in the state policies and procedures established by the Indiana department of administration and approved by the budget agency.

(n) Each member of the board who is a state employee, but who is not a member of the general assembly, is entitled to reimbursement for traveling expenses as provided under IC 4-13-1-4 and other expenses actually incurred in connection with the member's duties as provided in the state policies and procedures established by the Indiana department of



administration and approved by the budget agency.

(o) Each member of the board who is a member of the general assembly is entitled to receive the same per diem, mileage, and travel allowances paid to legislative members of interim study committees established by the legislative council. Per diem, mileage, and travel allowances paid under this section shall be paid from appropriations made to the legislative council or the legislative services agency.

Sec. 2. The board shall do the following:

(1) Prescribe the form and manner in which a government entity must apply to enroll in the program.

(2) Determine the types of cybersecurity incidents that are eligible for coverage under the program. The board shall review the board's determination under this subdivision at least annually and revise the determination as the board considers appropriate.

(3) Establish standards for:

(A) proof of loss, including standards for documentation of losses; and

(B) valuation of losses for purposes of determining coverage amounts.

(4) Prescribe the form and manner for submission of claims by participating government entities under IC 4-13.2-7.

(5) Designate a person to act as a single point of contact to which a participating government entity may submit a claim under IC 4-13.2-7.

(6) Prescribe procedures to be followed by a participating government entity in response to a cybersecurity incident, including procedures for:

(A) securing the government entity's assets against further loss; and

(B) preserving electronic evidence.

(7) Establish and maintain a team of cyber response agents by:

(A) procuring the services of cybersecurity professionals under IC 5-22; and

(B) entering into contracts with the cybersecurity professionals under which the cybersecurity professionals agree to provide services described in IC 4-13.2-1-6 to a participating government entity at the direction of the designated contact under IC 4-13.2-7-2.

(8) Establish standards for annual review of the program's



income, expenditures, and balances.

Sec. 3. (a) Subject to subsection (c), meetings of the board are open to the public in accordance with and subject to IC 5-14-1.5.

(b) Subject to subsection (d), records of the board are subject to the requirements of IC 5-14-3.

(c) The board shall meet in executive session under IC 5-14-1.5 to discuss claims filed under this chapter.

(d) Except as provided under section 4 of this chapter, a claim filed under this article, and any record or information relating to a claim filed under this article, is confidential and may not be disclosed to the public under IC 5-14-3.

Sec. 4. (a) Not later than July 1, 2026, and not later than July 1 of each year thereafter, the board shall submit to the executive director of the legislative services agency, for distribution to the members of the interim study committee on financial institutions and insurance, a report of the:

(1) number of claims made under this article in the preceding calendar year; and

(2) amount of coverage paid from the fund with respect to each claim under subdivision (1).

(b) The board's report under this section may not divulge:

(1) the identity of a government entity that filed a claim; or

(2) except as provided in subsection (a)(2), any information regarding a claim filed;

under this article.

(c) The board's report under this section must be in an electronic format under IC 5-14-6.

Chapter 5. Coverage

Sec. 1. (a) The board:

(1) shall establish:

(A) minimum coverage amounts under the program; and

(B) maximum coverage amounts under the program, subject to section 2 of this chapter; and

(2) may establish a schedule of deductions and copayments applicable to coverage;

for a claim under the program.

(b) The board may establish different minimum and maximum coverage amounts under subsection (a) based on:

(1) whether a participating government entity is the state, a county, a city, a town, a school corporation, or a state educational institution;

(2) the size of a participating government entity;



(3) the type of covered cybersecurity incident; and

(4) any other factor the board considers appropriate.

Sec. 2. (a) To be eligible to receive the maximum coverage amount for a loss, a participating government entity must be in compliance with the following at the time of the loss:

(1) If the participating government entity is the state, a city, a town, a county, or a state educational institution, the participating government entity must have adopted, and be in compliance with, a cybersecurity policy that is based on standards and guidelines developed under IC 4-13.1-4-5(a)(1)(A).

(2) If the participating government entity is a school corporation, the participating government entity must have adopted, and be in compliance with, the uniform cybersecurity policy developed under IC 4-13.1-4-5(a)(2)(B).

(b) The board shall establish a maximum coverage amount of not more than fifty thousand dollars (\$50,000) for a loss incurred by a participating government entity that is determined by the board to have not been in compliance with subsection (a) at the time of a cybersecurity incident for which the government entity submits a claim under this article.

Chapter 6. Premiums

Sec. 1. (a) Subject to section 3 of this chapter, the board shall establish a schedule of premiums for participating government entities.

(b) The board shall establish the form and manner in which a participating government entity must remit premiums under the program.

Sec. 2. The schedule of premiums established under section 1 of this chapter may provide for adjustment of the premium of a participating government entity that files a claim under this article, based on the amount of:

(1) coverage paid to the participating government entity with regard to the claim; and

(2) costs incurred by the board in responding to the claim, including the cost of assistance provided to the participating government entity by a cyber response agent at the direction of the board.

Sec. 3. The schedule of premiums established by the board under section 1 of this chapter must provide that the total amount of premiums payable by a participating government entity in the first two (2) years of the program's operation does not exceed three



1 hundred thousand dollars (\$300,000).

2 **Chapter 7. Claims**

3 **Sec. 1. A participating government entity that incurs a loss as**
 4 **the result of a covered cybersecurity incident may obtain coverage**
 5 **for the loss under the program by submitting a claim:**

6 (1) to the designated contact in the form and manner
 7 prescribed by the board; and

8 (2) not more than twenty-four (24) hours after the
 9 government entity becomes aware of the cybersecurity
 10 incident.

11 **Sec. 2. Upon receiving a claim from a participating government**
 12 **entity under section 1 of this chapter, the designated contact shall,**
 13 **not later than the next business day:**

14 (1) send to the board:

15 (A) notice of the claim; and

16 (B) a description of the cybersecurity incident;

17 (2) direct the participating government entity's initial
 18 response to the cybersecurity incident in accordance with
 19 procedures established by the board under IC 4-13.2-4-2(6);
 20 and

21 (3) at the request of the participating government entity,
 22 direct a cyber response agent to assist the participating
 23 government entity in responding to the cybersecurity incident.

24 **Sec. 3. (a) As soon as practicable after receipt of a claim by the**
 25 **designated contact under section 2 of this chapter, the board shall**
 26 **meet and:**

27 (1) determine whether the claim is substantiated; and

28 (2) if the board determines that the claim is substantiated,
 29 determine the coverage amount applicable to the claim.

30 (b) If the board determines that a participating government
 31 entity's claim is substantiated under subsection (a), the board shall
 32 reimburse the participating government entity from the fund in the
 33 amount of the lesser of:

34 (1) the amount of the participating government entity's actual
 35 losses as a result of the cybersecurity incident:

36 (A) including the cash value, as of the date on which the
 37 claim was filed, of property damaged or lost by the
 38 participating government entity as a result of the
 39 cybersecurity incident; and

40 (B) not including the amount:

41 (i) of a ransom or other payment made by the
 42 participating government entity to the perpetrator of the



cybersecurity incident; or

(ii) paid by the participating government entity in indemnifying or defending an employee of the participating government entity against liability incurred by the employee as a result of the cybersecurity incident; or

(2) the lesser of:

(A) the maximum coverage amount under the program as established by the board under IC 4-13.2-5-1; or

(B) one hundred thousand dollars (\$100,000);

minus any deduction or copayment applicable to the claim.

Sec. 4. (a) If:

(1) a participating government entity:

(A) incurs a loss due to a cybersecurity incident the amount of which is greater than the coverage provided for the loss under the program; and

(B) obtains additional recovery for the loss from a source other than the program; and

(2) the sum of:

(A) the amount of the coverage provided for the loss by the program; plus

(B) the amount of the participating government entity's recovery described in subdivision (1)(B);

exceeds the amount of the participating government entity's actual losses as a result of the cybersecurity incident;

the participating government entity shall remit to the board, for deposit in the fund, the difference between the amount calculated under subdivision (2) and the amount of the participating government entity's actual losses as a result of the cybersecurity incident.

(b) If a participating government entity fails to remit to the board the amount of an excess recovery as required under subsection (a), the board may withhold payment from coverage provided to the participating government entity for future claims under the program until the amount withheld equals the amount of the excess recovery.

Chapter 8. Adoption of Rules

Sec. 1. The board may adopt rules under IC 4-22-2 necessary to administer this article.

SECTION 5. IC 24-4-23-15, AS ADDED BY P.L.98-2024, SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 15. The attorney general may bring an action



under this chapter to obtain any or all of the following against an adult oriented website, accessible by an Indiana resident, that does not implement or properly use a reasonable age verification method:

- (1) An injunction to enjoin future violations of this chapter.
- (2) A civil penalty of not more than two hundred fifty thousand dollars (\$250,000).
- (3) The attorney general's reasonable costs in:
 - (A) the investigation of the violations under this chapter; and
 - (B) maintaining the action.

The attorney general shall remit a civil penalty collected under this section to the office of technology established by IC 4-13.1-2-1 for deposit in the cybersecurity insurance trust fund established by IC 4-13.2-3-1.

SECTION 6. IC 24-4.9-3-3.5, AS AMENDED BY P.L.76-2017, SECTION 4, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 3.5. (a) Except as provided in subsection (b), this section does not apply to a data base owner that maintains its own data security procedures as part of an information privacy, security policy, or compliance plan under:

- (1) the federal USA PATRIOT Act (P.L. 107-56);
- (2) Executive Order 13224;
- (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.);
- (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- (5) the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or
- (6) the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191);

if the data base owner's information privacy, security policy, or compliance plan requires the data base owner to maintain reasonable procedures to protect and safeguard from unlawful use or disclosure personal information of Indiana residents that is collected or maintained by the data base owner and the data base owner complies with the data base owner's information privacy, security policy, or compliance plan.

(b) This section applies to a current or former health care provider (as defined by IC 4-6-14-2) who is a data base owner or former data base owner:

- (1) to which an exemption under subsection (a)(6) applies or applied; and
- (2) whose information privacy, security policy, or compliance plan:



- 1 (A) does not require the data base owner or former data base
 2 owner to maintain and implement reasonable procedures; or
 3 (B) is not implemented by the data base owner or former data
 4 base owner;
 5 to ensure that the personal information described in subsection
 6 (a), including health records (as defined by IC 4-6-14-2.5), is
 7 protected and safeguarded from unlawful use or disclosure after
 8 the data base owner or former data base owner ceases to be a
 9 covered entity under the federal Health Insurance Portability and
 10 Accountability Act (P.L. 104-191).
- 11 (c) A data base owner shall implement and maintain reasonable
 12 procedures, including taking any appropriate corrective action, to
 13 protect and safeguard from unlawful use or disclosure any personal
 14 information of Indiana residents collected or maintained by the data
 15 base owner.
- 16 (d) A data base owner shall not dispose of or abandon records or
 17 documents containing unencrypted and unredacted personal
 18 information of Indiana residents without shredding, incinerating,
 19 mutilating, erasing, or otherwise rendering the personal information
 20 illegible or unusable.
- 21 (e) A person that knowingly or intentionally fails to comply with any
 22 provision of this section commits a deceptive act that is actionable only
 23 by the attorney general under this section.
- 24 (f) The attorney general may bring an action under this section to
 25 obtain any or all of the following:
- 26 (1) An injunction to enjoin further violations of this section.
 27 (2) A civil penalty of not more than five thousand dollars (\$5,000)
 28 per deceptive act.
 29 (3) The attorney general's reasonable costs in:
 30 (A) the investigation of the deceptive act; and
 31 (B) maintaining the action.
- 32 **The attorney general shall remit a civil penalty collected under this**
 33 **subsection to the office of technology established by IC 4-13.1-2-1**
 34 **for deposit in the cybersecurity insurance trust fund established by**
 35 **IC 4-13.2-3-1.**
- 36 (g) A failure to comply with subsection (c) or (d) in connection with
 37 related acts or omissions constitutes one (1) deceptive act.
- 38 SECTION 7. IC 24-4.9-4-2, AS ADDED BY P.L.125-2006,
 39 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
 40 JULY 1, 2025]: Sec. 2. (a) The attorney general may bring an action
 41 under this chapter to obtain any or all of the following:
 42 (1) An injunction to enjoin future violations of IC 24-4.9-3.



1 (2) A civil penalty of not more than one hundred fifty thousand
2 dollars (\$150,000) per deceptive act.

3 (3) The attorney general's reasonable costs in:

4 (A) the investigation of the deceptive act; and

5 (B) maintaining the action.

6 **(b) The attorney general shall remit a civil penalty collected**
7 **under this section to the office of technology established by**
8 **IC 4-13.1-2-1 for deposit in the cybersecurity insurance trust fund**
9 **established by IC 4-13.2-3-1.**

10 SECTION 8. IC 24-15-10-2, AS ADDED BY P.L.94-2023,
11 SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
12 JANUARY 1, 2026]: Sec. 2. (a) The attorney general may initiate an
13 action in the name of the state and may seek an injunction to restrain
14 any violations of this article and a civil penalty not to exceed seven
15 thousand five hundred dollars (\$7,500) for each violation under this
16 article.

17 (b) The attorney general may recover reasonable expenses incurred
18 in investigating and preparing the case, including attorney's fees, in any
19 action initiated under this chapter.

20 **(c) The attorney general shall remit a civil penalty collected**
21 **under this section to the office of technology established by**
22 **IC 4-13.1-2-1 for deposit in the cybersecurity insurance trust fund**
23 **established by IC 4-13.2-3-1.**



COMMITTEE REPORT

Mr. President: The Senate Committee on Commerce and Technology, to which was referred Senate Bill No. 472, has had the same under consideration and begs leave to report the same back to the Senate with the recommendation that said bill be AMENDED as follows:

Page 1, between the enacting clause and line 1, begin a new paragraph and insert:

"SECTION 1. IC 4-13.1-4-2, AS ADDED BY P.L.108-2024, SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE JULY 1, 2025]: Sec. 2. **(a) Except as provided in subsection (b),** as used in this chapter, "public entity" means a:

- (1) political subdivision;
- (2) state agency;
- (3) school corporation; or
- (4) state educational institution.

(b) The term does not include an acute care hospital licensed under IC 16-21 that is established and operated under IC 16-22-2, IC 16-22-8, or IC 16-23."

Renumber all SECTIONS consecutively.

and when so amended that said bill do pass and be reassigned to the Senate Committee on Appropriations.

(Reference is to SB 472 as introduced.)

BUCHANAN, Chairperson

Committee Vote: Yeas 11, Nays 0.

COMMITTEE REPORT

Mr. President: The Senate Committee on Appropriations, to which was referred Senate Bill No. 472, has had the same under consideration and begs leave to report the same back to the Senate with the recommendation that said bill be AMENDED as follows:

Page 2, line 12, delete "Not later than December 31, 2025," and insert "**Not later than December 31, 2027,**".

Page 5, line 19, delete "office" and insert "**budget agency**".

Page 5, delete lines 31 through 36.

Page 5, line 37, delete "(g)" and insert "(e)".

SB 472—LS 7298/DI 119



Page 5, between lines 38 and 39, begin a new paragraph and insert:
"(f) Notwithstanding any other provision, claims from the fund shall not be paid until the balance in the fund reaches ten million dollars (\$10,000,000)."

Page 7, line 2, delete "second" and insert **"first"**.

Page 7, line 4, delete "third" and insert **"second"**.

Page 8, line 35, after "described" insert **"in"**.

and when so amended that said bill do pass.

(Reference is to SB 472 as printed January 24, 2025.)

MISHLER, Chairperson

Committee Vote: Yeas 12, Nays 0.

SENATE MOTION

Mr. President: I move that Senate Bill 472 be amended to read as follows:

Page 3, between lines 23 and 24, begin a new paragraph and insert:
"(c) If a public entity engages a third party to conduct an assessment of the public entity's cybersecurity policy, the public entity shall provide the results of the assessment to the office."

Page 6, delete lines 31 through 35, begin a new paragraph and insert:

"(f) The term of an appointed member of the board is as follows:

(1) An appointed member who is not a member of the general assembly serves a six (6) year term that ends June 30, 2031, and June 30 of every sixth year thereafter.

(2) An appointed member who is a member of the general assembly serves a two (2) year term that ends June 30, 2027, and June 30 of every odd-numbered year thereafter.

An appointed member of the board may be reappointed at the conclusion of the member's term."

Page 7, line 32, delete "mileage and".

(Reference is to SB 472 as printed February 14, 2025.)

BROWN L

