

SENATE BILL No. 472

DIGEST OF INTRODUCED BILL

Citations Affected: IC 4-13.1-4; IC 4-13.2; IC 24-4-23-15; IC 24-4.9; IC 24-15-10-2.

Synopsis: Cybersecurity. Requires political subdivisions, state agencies, school corporations, and state educational institutions (public entities) to adopt, not later than December 31, 2025, 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 a school corporation; and (2) a uniform cybersecurity policy for use by school corporations. Requires: (1) a public entity to biennially submit 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. 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. 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
(Continued next page)

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

Brown L

January 13, 2025, read first time and referred to Committee on Commerce and Technology.



Digest Continued

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.



Introduced

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 4-13.1-4-5, AS ADDED BY P.L.108-2024,
 2 SECTION 2, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
 3 JULY 1, 2025]: Sec. 5. (a) **The office shall:**
 4 (1) **develop:**
 5 (A) **standards and guidelines regarding cybersecurity for**
 6 **use by political subdivisions and state educational**
 7 **institutions; and**
 8 (B) **a uniform cybersecurity policy for use by state**
 9 **agencies; and**
 10 (2) **develop, in collaboration with the department of**
 11 **education:**
 12 (A) **a uniform technology resources policy governing use of**
 13 **technology resources by the employees of a school**
 14 **corporation; and**
 15 (B) **a uniform cybersecurity policy for use by school**



- 1 **corporations.**
- 2 **(b) Not later than December 31, 2025, each public entity may**
- 3 **shall** adopt the following:
- 4 (1) A policy governing use of technology resources by the public
- 5 entity's employees. ~~The policy may:~~ **If the public entity is a**
- 6 **school corporation, the public entity shall adopt the uniform**
- 7 **technology resources policy developed under subsection**
- 8 **(a)(2)(A).**
- 9 (A) ~~prohibit an employee of the public entity from using the~~
- 10 ~~public entity's technology resources to:~~
- 11 (i) ~~engage in lobbying (as defined in IC 2-7-1-9) that is~~
- 12 ~~outside the scope of the employee's duties;~~
- 13 (ii) ~~engage in illegal activity; or~~
- 14 (iii) ~~violate the public entity's cybersecurity policy; and~~
- 15 ~~(B) include disciplinary procedures for violation of the~~
- 16 ~~technology resources policy.~~
- 17 (2) A cybersecurity policy ~~If the public entity is:~~ **as follows:**
- 18 (A) **If the public entity is** a political subdivision or state
- 19 **educational institution, the public entity shall adopt a**
- 20 **cybersecurity policy may be based on standards and**
- 21 **guidelines developed by the office under subsection**
- 22 **(a)(1)(A).**
- 23 (B) **If the public entity is** a school corporation, the ~~policy may~~
- 24 ~~be based on~~ **public entity shall adopt the uniform**
- 25 **cybersecurity policy standards and guidelines developed by the**
- 26 **office, in collaboration with the department of education; and**
- 27 **under subsection (a)(2)(B).**
- 28 (C) **If the public entity is** a state agency, the **public entity**
- 29 **shall adopt the uniform cybersecurity policy is developed by**
- 30 **the office: under subsection (a)(1)(B).**
- 31 (3) A training program regarding the public entity's technology
- 32 resources policy adopted under subdivision (1) and cybersecurity
- 33 policy adopted under subdivision (2), completion of which is
- 34 mandatory for the public entity's employees.
- 35 **(c) The uniform technology resources policy developed under**
- 36 **subsection (a)(2)(A) and a technology resources policy adopted by**
- 37 **a public entity other than a school corporation under subsection**
- 38 **(b)(1) must:**
- 39 (1) **prohibit an employee of the public entity from using the**
- 40 **public entity's technology resources to:**
- 41 (A) **engage in lobbying (as defined in IC 2-7-1-9) that is**
- 42 **outside the scope of the employee's duties;**



- 1 **(B) engage in illegal activity; or**
 2 **(C) violate the public entity's cybersecurity policy; and**
 3 **(2) include disciplinary procedures for violation of the**
 4 **technology resources policy.**

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

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

14 SECTION 3. IC 4-13.2 IS ADDED TO THE INDIANA CODE AS
 15 A NEW ARTICLE TO READ AS FOLLOWS [EFFECTIVE JULY 1,
 16 2025]:

17 **ARTICLE 13.2. CYBERSECURITY INSURANCE PROGRAM**
 18 **Chapter 1. Definitions**

19 **Sec. 1. The definitions in this chapter apply throughout this**
 20 **article.**

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

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

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

29 **Sec. 5. "Cybersecurity incident" has the meaning set forth in**
 30 **IC 4-13.1-1-1.5.**

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

- 32 **(1) has documented experience in responding to cybersecurity**
 33 **incidents; and**
 34 **(2) is qualified to provide services such as:**
 35 **(A) forensic analysis of a cybersecurity incident; and**
 36 **(B) software, hardware, and data restoration after a**
 37 **cybersecurity incident.**

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

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

- 41 **(1) the governor, with respect to the state;**
 42 **(2) the:**



- 1 (A) board of county commissioners, with respect to a
- 2 county that does not have a consolidated city; or
- 3 (B) mayor of the consolidated city, with respect to a county
- 4 that has a consolidated city;
- 5 (3) the mayor, with respect to a city;
- 6 (4) the president of the town council, with respect to a town;
- 7 (5) the superintendent, with respect to a school corporation;
- 8 and
- 9 (6) the president of the state educational institution, with
- 10 respect to a state educational institution.

11 Sec. 9. "Fund" means the cybersecurity insurance trust fund

12 established by IC 4-13.2-3-1.

13 Sec. 10. "Government entity" means:

- 14 (1) the state;
- 15 (2) a county;
- 16 (3) a city;
- 17 (4) a town;
- 18 (5) a school corporation; or
- 19 (6) a state educational institution.

20 Sec. 11. "Office" means the office of technology established by

21 IC 4-13.1-2-1.

22 Sec. 12. "Participating government entity" means a government

23 entity that has enrolled in the program under IC 4-13.2-2-3.

24 Sec. 13. "Program" refers to the cybersecurity insurance

25 program established by IC 4-13.2-2-1.

26 Sec. 14. "School corporation" means:

- 27 (1) a school corporation (as defined in IC 20-18-2-16(a)); and
- 28 (2) a charter school.

29 Sec. 15. "State educational institution" has the meaning set

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

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

32 Sec. 1. The cybersecurity insurance program is established for

33 the purpose of providing coverage to a participating government

34 entity for losses incurred by the government entity as a result of a

35 cybersecurity incident.

36 Sec. 2. The board shall administer the program.

37 Sec. 3. The executive of a government entity may enroll the

38 government entity in the program by submitting an application:

- 39 (1) to the board; and
- 40 (2) in the form and manner specified by the board;

41 on behalf of the government entity.

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



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

3 **(1) paying claims to participating government entities under**
 4 **the program;**

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

7 **(3) paying the operating expenses of the board.**

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

9 **(c) The office shall administer the fund.**

10 **(d) The fund consists of:**

11 **(1) premiums paid by participating government entities under**
 12 **IC 4-13.2-6;**

13 **(2) appropriations to the fund by the general assembly;**

14 **(3) civil penalties collected under:**

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

16 **(B) IC 24-4.9-3-3.5;**

17 **(C) IC 24-4.9-4-2; and**

18 **(D) IC 24-15-10-2; and**

19 **(4) grants, gifts, and donations intended for deposit in the**
 20 **fund.**

21 **(e) The expenses of administering the fund shall be paid from**
 22 **money in the fund. The board may use not more than five percent**
 23 **(5%) of the premiums deposited into the fund under subsection**
 24 **(d)(1) for purposes of administering the fund and the program.**

25 **(f) Money in the fund is continuously appropriated for the**
 26 **purposes of this article.**

27 **(g) Money in the fund at the end of a state fiscal year does not**
 28 **revert to the state general fund.**

29 **Chapter 4. Cybersecurity Insurance Board**

30 **Sec. 1. (a) The cybersecurity insurance board is established as**
 31 **a continuing board under the executive branch of state government**
 32 **for the purpose of administering the cybersecurity insurance**
 33 **program.**

34 **(b) The board consists of the following members:**

35 **(1) The chief information officer of the office or a designee of**
 36 **the chief information officer.**

37 **(2) Three (3) members appointed by the governor:**

38 **(A) one (1) of whom is a representative of Indiana**
 39 **counties;**

40 **(B) one (1) of whom is a representative of Indiana cities;**
 41 **and**

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



- 1 (3) If the state participates in the program, the governor or
 2 the governor's designee.
 3 (4) If a state educational institution participates in the
 4 program, one (1) representative of state educational
 5 institutions who is appointed to the board by the governor.
 6 (5) The insurance commissioner or a designee of the insurance
 7 commissioner.
 8 (6) The secretary of education or a designee of the secretary
 9 of education.
 10 (7) The executive director of the department of homeland
 11 security or a designee of the executive director of the
 12 department of homeland security.
 13 (8) The state comptroller or a designee of the state
 14 comptroller.
- 15 (c) The chief information officer, or the chief information
 16 officer's designee under subsection (b)(1), serves as:
 17 (1) chair; and
 18 (2) a nonvoting member;
 19 of the board.
- 20 (d) If a member of the general assembly is appointed to the
 21 board, the member is a nonvoting member.
- 22 (e) An appointed member of the board serves at the will of the
 23 member's appointing authority.
- 24 (f) An appointed member of the board:
 25 (1) serves a term that ends June 30 of the sixth year following
 26 the year in which the member is appointed; and
 27 (2) may be reappointed at the conclusion of the member's
 28 term.
- 29 (g) A vacancy on the board shall be filled by the appointing
 30 authority of the member whose position on the board is vacant to
 31 meet the same qualifications as the vacating member.
- 32 (h) The board:
 33 (1) shall meet:
 34 (A) for the second time not later than September 30, 2025;
 35 and
 36 (B) for the third time not later than December 31, 2025;
 37 at the call of the chair;
 38 (2) subject to subsection (i), shall meet at the call of the chair
 39 at least one (1) time each quarter during 2026 and each year
 40 thereafter;
 41 (3) shall meet as required under IC 4-13.2-7-3; and
 42 (4) may meet at any time at the call of:



- 1 (A) the chair; or
2 (B) a majority of the members of the board.
- 3 (i) The chair may cancel a meeting of the board scheduled under
4 subsection (h)(2) if the chair determines that, as of twenty-four (24)
5 hours before the scheduled time of the meeting:
- 6 (1) no claim has been submitted under this article requiring
7 the board's consideration; and
8 (2) no other matter requires the board's consideration.
- 9 (j) A majority of the members of the board constitutes a
10 quorum. The affirmative votes of a majority of the voting members
11 of the board are required for the board to take action.
- 12 (k) The office shall staff the board.
- 13 (l) Except as provided in subsection (o), the expenses of the
14 board shall be paid from the fund.
- 15 (m) A member of the board who is not a state employee is not
16 entitled to the minimum salary per diem provided by
17 IC 4-10-11-2.1(b). The member is, however, entitled to
18 reimbursement for mileage and traveling expenses as provided
19 under IC 4-13-1-4 and other expenses actually incurred in
20 connection with the member's duties as provided in the state
21 policies and procedures established by the Indiana department of
22 administration and approved by the budget agency.
- 23 (n) Each member of the board who is a state employee, but who
24 is not a member of the general assembly, is entitled to
25 reimbursement for mileage and traveling expenses as provided
26 under IC 4-13-1-4 and other expenses actually incurred in
27 connection with the member's duties as provided in the state
28 policies and procedures established by the Indiana department of
29 administration and approved by the budget agency.
- 30 (o) Each member of the board who is a member of the general
31 assembly is entitled to receive the same per diem, mileage, and
32 travel allowances paid to legislative members of interim study
33 committees established by the legislative council. Per diem,
34 mileage, and travel allowances paid under this section shall be paid
35 from appropriations made to the legislative council or the
36 legislative services agency.
- 37 **Sec. 2. The board shall do the following:**
- 38 (1) Prescribe the form and manner in which a government
39 entity must apply to enroll in the program.
- 40 (2) Determine the types of cybersecurity incidents that are
41 eligible for coverage under the program. The board shall
42 review the board's determination under this subdivision at



1 least annually and revise the determination as the board
2 considers appropriate.

3 **(3) Establish standards for:**

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

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

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

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

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

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

18 **(B) preserving electronic evidence.**

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

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

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

28 **(8) Establish standards for annual review of the program's**
29 **income, expenditures, and balances.**

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

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

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

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

40 **Sec. 4. (a) Not later than July 1, 2026, and not later than July 1**
41 **of each year thereafter, the board shall submit to the executive**
42 **director of the legislative services agency, for distribution to the**



1 members of the interim study committee on financial institutions
2 and insurance, a report of the:

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

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

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

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

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

11 under this article.

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

14 **Chapter 5. Coverage**

15 **Sec. 1. (a) The board:**

16 (1) shall establish:

17 (A) minimum coverage amounts under the program; and

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

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

22 for a claim under the program.

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

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

28 (2) the size of a participating government entity;

29 (3) the type of covered cybersecurity incident; and

30 (4) any other factor the board considers appropriate.

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

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

40 (2) If the participating government entity is a school
41 corporation, the participating government entity must have
42 adopted, and be in compliance with, the uniform



1 cybersecurity policy developed under IC 4-13.1-4-5(a)(2)(B).
 2 (b) The board shall establish a maximum coverage amount of
 3 not more than fifty thousand dollars (\$50,000) for a loss incurred
 4 by a participating government entity that is determined by the
 5 board to have not been in compliance with subsection (a) at the
 6 time of a cybersecurity incident for which the government entity
 7 submits a claim under this article.

8 Chapter 6. Premiums

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

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

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

- 19 (1) coverage paid to the participating government entity with
 20 regard to the claim; and
- 21 (2) costs incurred by the board in responding to the claim,
 22 including the cost of assistance provided to the participating
 23 government entity by a cyber response agent at the direction
 24 of the board.

25 Sec. 3. The schedule of premiums established by the board
 26 under section 1 of this chapter must provide that the total amount
 27 of premiums payable by a participating government entity in the
 28 first two (2) years of the program's operation does not exceed three
 29 hundred thousand dollars (\$300,000).

30 Chapter 7. Claims

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

- 34 (1) to the designated contact in the form and manner
 35 prescribed by the board; and
- 36 (2) not more than twenty-four (24) hours after the
 37 government entity becomes aware of the cybersecurity
 38 incident.

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

- 42 (1) send to the board:



- 1 (A) notice of the claim; and
- 2 (B) a description of the cybersecurity incident;
- 3 (2) direct the participating government entity's initial
- 4 response to the cybersecurity incident in accordance with
- 5 procedures established by the board under IC 4-13.2-4-2(6);
- 6 and
- 7 (3) at the request of the participating government entity,
- 8 direct a cyber response agent to assist the participating
- 9 government entity in responding to the cybersecurity incident.
- 10 Sec. 3. (a) As soon as practicable after receipt of a claim by the
- 11 designated contact under section 2 of this chapter, the board shall
- 12 meet and:
- 13 (1) determine whether the claim is substantiated; and
- 14 (2) if the board determines that the claim is substantiated,
- 15 determine the coverage amount applicable to the claim.
- 16 (b) If the board determines that a participating government
- 17 entity's claim is substantiated under subsection (a), the board shall
- 18 reimburse the participating government entity from the fund in the
- 19 amount of the lesser of:
- 20 (1) the amount of the participating government entity's actual
- 21 losses as a result of the cybersecurity incident:
- 22 (A) including the cash value, as of the date on which the
- 23 claim was filed, of property damaged or lost by the
- 24 participating government entity as a result of the
- 25 cybersecurity incident; and
- 26 (B) not including the amount:
- 27 (i) of a ransom or other payment made by the
- 28 participating government entity to the perpetrator of the
- 29 cybersecurity incident; or
- 30 (ii) paid by the participating government entity in
- 31 indemnifying or defending an employee of the
- 32 participating government entity against liability
- 33 incurred by the employee as a result of the cybersecurity
- 34 incident; or
- 35 (2) the lesser of:
- 36 (A) the maximum coverage amount under the program as
- 37 established by the board under IC 4-13.2-5-1; or
- 38 (B) one hundred thousand dollars (\$100,000);
- 39 minus any deduction or copayment applicable to the claim.
- 40 Sec. 4. (a) If:
- 41 (1) a participating government entity:
- 42 (A) incurs a loss due to a cybersecurity incident the



1 amount of which is greater than the coverage provided for
 2 the loss under the program; and
 3 (B) obtains additional recovery for the loss from a source
 4 other than the program; and
 5 (2) the sum of:
 6 (A) the amount of the coverage provided for the loss by the
 7 program; plus
 8 (B) the amount of the participating government entity's
 9 recovery described in subdivision (1)(B);
 10 exceeds the amount of the participating government entity's
 11 actual losses as a result of the cybersecurity incident;
 12 the participating government entity shall remit to the board, for
 13 deposit in the fund, the difference between the amount calculated
 14 under subdivision (2) and the amount of the participating
 15 government entity's actual losses as a result of the cybersecurity
 16 incident.
 17 (b) If a participating government entity fails to remit to the
 18 board the amount of an excess recovery as required under
 19 subsection (a), the board may withhold payment from coverage
 20 provided to the participating government entity for future claims
 21 under the program until the amount withheld equals the amount
 22 of the excess recovery.

23 Chapter 8. Adoption of Rules

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

26 SECTION 4. IC 24-4-23-15, AS ADDED BY P.L.98-2024,
 27 SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
 28 JULY 1, 2025]: Sec. 15. The attorney general may bring an action
 29 under this chapter to obtain any or all of the following against an adult
 30 oriented website, accessible by an Indiana resident, that does not
 31 implement or properly use a reasonable age verification method:

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

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

42 SECTION 5. IC 24-4.9-3-3.5, AS AMENDED BY P.L.76-2017,



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

- 6 (1) the federal USA PATRIOT Act (P.L. 107-56);
- 7 (2) Executive Order 13224;
- 8 (3) the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et
9 seq.);
- 10 (4) the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
- 11 (5) the federal Financial Modernization Act of 1999 (15 U.S.C.
12 6801 et seq.); or
- 13 (6) the federal Health Insurance Portability and Accountability
14 Act (HIPAA) (P.L. 104-191);

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

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

- 25 (1) to which an exemption under subsection (a)(6) applies or
26 applied; and
- 27 (2) whose information privacy, security policy, or compliance
28 plan:
 - 29 (A) does not require the data base owner or former data base
30 owner to maintain and implement reasonable procedures; or
 - 31 (B) is not implemented by the data base owner or former data
32 base owner;

33 to ensure that the personal information described in subsection
34 (a), including health records (as defined by IC 4-6-14-2.5), is
35 protected and safeguarded from unlawful use or disclosure after
36 the data base owner or former data base owner ceases to be a
37 covered entity under the federal Health Insurance Portability and
38 Accountability Act (P.L. 104-191).

39 (c) A data base owner shall implement and maintain reasonable
40 procedures, including taking any appropriate corrective action, to
41 protect and safeguard from unlawful use or disclosure any personal
42 information of Indiana residents collected or maintained by the data



1 base owner.

2 (d) A data base owner shall not dispose of or abandon records or
3 documents containing unencrypted and unredacted personal
4 information of Indiana residents without shredding, incinerating,
5 mutilating, erasing, or otherwise rendering the personal information
6 illegible or unusable.

7 (e) A person that knowingly or intentionally fails to comply with any
8 provision of this section commits a deceptive act that is actionable only
9 by the attorney general under this section.

10 (f) The attorney general may bring an action under this section to
11 obtain any or all of the following:

- 12 (1) An injunction to enjoin further violations of this section.
13 (2) A civil penalty of not more than five thousand dollars (\$5,000)
14 per deceptive act.
15 (3) The attorney general's reasonable costs in:
16 (A) the investigation of the deceptive act; and
17 (B) maintaining the action.

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

22 (g) A failure to comply with subsection (c) or (d) in connection with
23 related acts or omissions constitutes one (1) deceptive act.

24 SECTION 6. IC 24-4.9-4-2, AS ADDED BY P.L.125-2006,
25 SECTION 6, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
26 JULY 1, 2025]: Sec. 2. (a) The attorney general may bring an action
27 under this chapter to obtain any or all of the following:

- 28 (1) An injunction to enjoin future violations of IC 24-4.9-3.
29 (2) A civil penalty of not more than one hundred fifty thousand
30 dollars (\$150,000) per deceptive act.
31 (3) The attorney general's reasonable costs in:
32 (A) the investigation of the deceptive act; and
33 (B) maintaining the action.

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

38 SECTION 7. IC 24-15-10-2, AS ADDED BY P.L.94-2023,
39 SECTION 1, IS AMENDED TO READ AS FOLLOWS [EFFECTIVE
40 JANUARY 1, 2026]: Sec. 2. (a) The attorney general may initiate an
41 action in the name of the state and may seek an injunction to restrain
42 any violations of this article and a civil penalty not to exceed seven



1 thousand five hundred dollars (\$7,500) for each violation under this
2 article.

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

6 (c) **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.**

