LEGISLATIVE SERVICES AGENCY
OFFICE OF FISCAL AND MANAGEMENT ANALYSIS
FISCAL IMPACT STATEMENT

LS 7298
BILL NUMBER: SB 472

NOTE PREPARED: Jan 8, 2025
BILL AMENDED:

SUBJECT: Cybersecurity.

FIRST AUTHOR: Sen. Brown L
FIRST SPONSOR:

BILL STATUS: As Introduced

FUNDS AFFECTED: X **GENERAL**
X **DEDICATED**
FEDERAL

IMPACT: State & Local

Summary of Legislation: *Cybersecurity Policy* - This bill 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. It 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. It 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. It also 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.

Cybersecurity Insurance - The bill 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. It 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. It also 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.

The bill 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.

The bill also makes an appropriation.

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

Explanation of State Expenditures: *Summary* - The bill creates the Cybersecurity Insurance Program which is operated through the Cybersecurity Insurance Board and funded by the Cybersecurity Insurance Trust Fund. It would increase expenditures significantly for Cybersecurity Insurance Trust Fund to administer the program, pay claims, pay for expenses of the board, and hire a team of cyber response agents. In addition, funds are continuously appropriated to the fund.

Workload is expected to increase for the Indiana Office of Technology (IOT) administer the Cybersecurity Insurance Trust Fund and develop cybersecurity standards. In addition, workload would increase for the members of the Cybersecurity Insurance Board. Workload increases are expected to be done within current staffing and resources.

Additional information -

Claims: The bill would increase expenditures for Cybersecurity Insurance Trust Fund to pay out claims for a cybersecurity incident. The board will set the minimum and maximum coverage. Noncompliance members may only receive a maximum coverage of $50,000. Otherwise, the maximum claim is $100,000. Claims do not cover the cost of ransom or defending an employee against liability. However, if a governmental entity receives coverage and funds from an outside source that are greater than the amount of the cybersecurity incident, the governmental entity would need to remit the access funds to the Cybersecurity Insurance Board. The increase in expenditures may be potentially significant to the extent of the number of claims made due to a cybersecurity incident but the amount is currently indeterminable.

Cybersecurity Insurance Trust Fund: The bill creates the Cybersecurity Insurance Trust Fund to be administered by IOT. It is established to pay for claims for the program, payments to cybersecurity professionals, operating expenses for the Cybersecurity Insurance Board. It is funded through premiums, appropriations, and certain civil penalties. Expenditures of administering the fund are paid through the fund but it is restricted in only using 5% of the premiums deposited to be used for administering the fund and program. A continuous appropriation is made for the Cybersecurity Insurance Trust Fund.

Cybersecurity Insurance Board: The bill creates the Cybersecurity Insurance Board. It consists of 10 members consisting of the IOT chief information officer, a representative of Indiana counties, a representative of Indiana cities, a representative of Indiana towns, the Governor, a state educational institutions representative, insurance commission, secretary of education, Department of Homeland Security executive director, and State Comptroller. The board shall meet three times in 2025 and starting in 2026, one in each quarter of the year. IOT would staff the board and pay the expenditures from the Cybersecurity Insurance Trust Fund. The board would establish the enrollment, eligibility, and standards for the program. The board would submit a report to Legislative Services Agency to distribution to the members of the Interim Study Committee on Financial Institutions.

The board would need to hire a team of cyber response agents. According the Bureau of Labor Statistics as of 2023, the median salary for an Information Security Analyst is $120,360. Board members who are not state employees would be entitled reimbursement for travel and other expenses incurred in connection with the member's duties. Board members who are a state employees would be entitled to salary per diem and reimbursement for travel and other expenses incurred in connection with the member's duties. Board members from the General Assembly are entitled to the same per diem, mileage, and travel allowances paid for interim study committees. Expenditures from the Cybersecurity Insurance Trust Fund could be potentially significant depending on the amount of cyber response agents needed and per diem paid.

Cybersecurity Policy: The bill will increase workload for IOT to develop cybersecurity standards and guidelines for political subdivisions and state educational institutions and also developing a uniform cybersecurity policy for state agencies. IOT would work with DOE to create a uniform cybersecurity policy for school corporations. In addition, IOT would need to establish a procedure for collection cybersecurity polices. The bill's requirements are within the agency's routine administrative functions and should be able to be implemented with no additional appropriations, assuming near customary agency staffing and resource levels.

The bill will increase workload for state agencies and state educational institutions to adopt a cybersecurity policy by December 31, 2025 and submit the cybersecurity policy each year to IOT. The bill's requirements are within the agency's routine administrative functions and should be able to be implemented with no additional appropriations, assuming near customary agency staffing and resource levels.

Explanation of State Revenues: *Premiums:* Revenue to the Cybersecurity Insurance Trust Fund would increase to the extent of the established premium schedule and number of governmental entities participating in the program. The revenue is indeterminable but expected to be significant. The cap in premiums payable by a participating governmental entity is $300,000 for the first two years in the program.

Distribution of Civil Penalties: The bill changes the distribution of certain civil penalties collected from the Attorney General from the General Fund to the Cybersecurity Insurance Trust Fund. The change in distribution is indeterminable but could potentially be significant depending on prosecution of alleged violations. The civil penalties and the maximum amount are shown in the table below.

Affected Civil Penalties		
IC Code	**Description**	**Maximum Amount**
IC 24-4-23-15	Failure of an adult oriented website to implement or properly use a reasonable age verification method	$250,000
IC 24-4.9-3-3.5	Failure of a data base owner to safeguard personal information of Indiana residents	$5,000
IC 24-4.9-4-2	Failure of a data base owner to disclose or provide notice of a security breach	$150,000
IC 24-15-10-2	Violation of consumer data protection law	$7,500

Explanation of Local Expenditures: *Cybersecurity Policy:* The bill will increase workload for school corporations and political subdivisions to adopt a cybersecurity policy by December 31, 2025 and submit the cybersecurity policy every odd number year to IOT. The bill's requirements are within the agency's routine administrative functions and should be able to be implemented with no additional appropriations, assuming near customary agency staffing and resource levels.

Explanation of Local Revenues:

State Agencies Affected: All.

Local Agencies Affected: School Corporations; political subdivisions.

Information Sources: Bureau of Labor Statistics,
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Fiscal Analyst: Nate Bodnar, 317-234-9476.