Paul D. Joyce, CPA
State Examiner

INDIANA STATE BOARD OF ACCOUNTS
302 WEST WASHINGTON STREET
ROOM E418
INDIANAPOLIS, INDIANA 46204-2769
Telephone: (317) 232-2513
Fax: (317) 232-4711
www.in.gov/sboa

STATE EXAMINER DIRECTIVE 2026-04

Date: July 29, 2026

Subject: Required Reporting to the SBOA Regarding a "Cybersecurity incident"

Authority: IC 5-11-1-2, IC 5-11-1-21, IC 5-11-1-27

Application: Any county, township, city, town, school corporation, library district, fire protection district, public transportation corporation, local hospital authority or corporation, local airport authority district, special service district, special taxing district, or other separate local governmental entity that may sue and be sued.

See IC 5-11-10.5-1 and IC 5-11-1-27(d)

Issued By: Paul D. Joyce, CPA, State Examiner

This State Examiner Directive applies to all the audited entities referenced above and all public employees and officials working for those entities that are responsible for and entrusted with public funds.

Indiana Code 5-11-1-27(j) provides, in relevant part, that "[a]ll erroneous or irregular material variances, losses, shortages, or thefts of political subdivision funds or property shall be reported immediately to the state board of accounts. . . ."

A "cybersecurity incident" often involves a hacker's use of malicious software against an audited entity in a manner that prevents the audited entity from accessing its own data (i.e. employee records, payroll, vendor info, etc.) while demanding a ransom payment to the hacker.

"Cybersecurity incident" is defined as:

> (a) . . . a malicious or suspicious occurrence that consists of one (1) or more of the categories of attack vectors described in subsection (b) and defined on the office's website that:
>
> (1) jeopardizes or may potentially jeopardize the confidentiality, integrity, or availability of an information system, an operational system, or the information that such systems process, store, or transmit;
> (2) jeopardizes or may potentially jeopardize the health and safety of the public; or
> (3) violates security policies, security procedures, or acceptable use policies.

IC 4-13.1-1-1.5(a).

A "cybersecurity incident" might involve one or more of the following:

(1) Ransomware.
(2) Business electronic mail compromise.
(3) Vulnerability exploitation.
(4) Zero-day exploitation.
(5) Distributed denial of service.
(6) Website defacement.
(7) Other sophisticated attacks as defined by the chief information officer and that are posted on the office's website.

IC 4-13.1-1-1.5(b).

This directive instructs that any amount of public funds associated with any "cybersecurity incident" are subject to the reporting requirements of IC 5-11-1-27(j) and must be reported to the SBOA immediately. This directive applies when the audited entity makes payment to the hacker directly or through a third party.

This web link shall be utilized for the reporting required by this directive: Reporting Portal

Respectfully,

Paul D. Joyce

Paul D. Joyce, CPA
State Examiner