

**LEGISLATIVE SERVICES AGENCY
OFFICE OF FISCAL AND MANAGEMENT ANALYSIS**

200 W. Washington St., Suite 301
Indianapolis, IN 46204
(317) 233-0696
iga.in.gov

FISCAL IMPACT STATEMENT

LS 6993

BILL NUMBER: HB 1169

NOTE PREPARED: Mar 23, 2021

BILL AMENDED: Mar 23, 2021

SUBJECT: Cybersecurity Incidents.

FIRST AUTHOR: Rep. Karickhoff

FIRST SPONSOR: Sen. Crider

BILL STATUS: CR Adopted - 2nd House

FUNDS AFFECTED: **GENERAL**
 DEDICATED
 FEDERAL

IMPACT: State & Local

Summary of Legislation: (Amended) This bill has the following provisions:

- (1) Requires the Indiana Office of Technology (IOT) to maintain a repository of cybersecurity incidents.
- (2) Provides that a state agency and a political subdivision shall: (a) report any cybersecurity incident to the IOT without unreasonable delay and not later than two business days after discovery of the cybersecurity incident in a format prescribed by the chief information officer; and (b) provide the IOT with the name and contact information of any individual who will act as the primary reporter of a cybersecurity incident before September 1, 2021, and before September 1 of every year thereafter.
- (3) Allows the IOT to assist a state agency with certain issues concerning information technology.
- (4) Provides that if requested by a political subdivision or a state agency, the IOT may develop a list of third party technology providers that work with the Office.
- (5) Requires a state educational institution to submit a quarterly analysis with certain conditions.
- (6) Makes conforming changes.

Effective Date: July 1, 2021.

Explanation of State Expenditures: This bill expands the responsibilities of the IOT to include maintaining a repository of cybersecurity incidents, as well as assist state agencies with information technology issues and providing a list of third party providers to local units of government. The IOT reports the provisions of the bill can be accomplished with no additional fiscal impact to the state.

(Revised) The bill will also increase state agency workload to report cybersecurity incidents within two business days to the IOT. The bill also places reporting requirements for state educational institutions

concerning cybersecurity incidents that differ from those of other state agencies. Increases in workload are expected to be minimal.

Explanation of State Revenues:

Explanation of Local Expenditures: The bill will also increase local unit of government workload to report cybersecurity incidents within two business days to the IOT. Increases in workload are expected to be minimal.

Explanation of Local Revenues:

State Agencies Affected: All.

Local Agencies Affected: All.

Information Sources: Graig Lubsen, IOT.

Fiscal Analyst: Bill Brumbach, 317-232-9559.