OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 283
136th General Assembly

# Bill Analysis

**Version:** As Introduced

**Primary Sponsors:** Reps. A. Mathews and Ghanbari

Daniel DeSantis, Research Analyst

## SUMMARY


- Requires political subdivisions to adopt a cybersecurity program.
- Prohibits a political subdivision experiencing a ransomware incident from paying or otherwise complying with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance.


## DETAILED ANALYSIS

### Cybersecurity program

The bill requires that the legislative authority of each political subdivision (a county, township, municipal corporation, or other body corporate and politic responsible for governmental activities in a geographic area smaller than that of the state) adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The program must be consistent with generally accepted best practices for cybersecurity, such as the National Institute of Standards and Technology Cybersecurity Framework, and the Center for Internet Security Cybersecurity Best Practices. The program should do at least all of the following:

- Identify and address the critical functions and cybersecurity risks of the political subdivision.
- Identify the potential impacts of a cybersecurity breach.
- Specify mechanisms to detect potential threats and cybersecurity events.
- Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents.
- Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident.

- Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which must correspond to the duties of each employee. The bill specifies that annual cybersecurity training provided by the state, and training provided for local governments by the Ohio Persistent Cyber Initiative Program of the Ohio Cyber Range Institute, satisfy this requirement.[1]

Under the bill, "cybersecurity incident" means any of the following:

- A substantial loss of confidentiality, integrity, or availability of a covered entity's information system or network;
- A serious impact on the safety and resiliency of a covered entity's operational systems and processes;
- A disruption of a covered entity's ability to engage in business or industrial operations, or deliver goods or services;
- Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated through or is caused by:
  - A compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or
  - A supply chain compromise.

"Cybersecurity incident" does not include mere threats of disruption as extortion; events perpetrated in good faith in response to a request by the system owner or operator; or lawfully authorized activity of a U.S., state, local, tribal, or territorial government entity.[2]

## Ransomware incident

The bill prohibits a political subdivision experiencing a ransomware incident from paying or otherwise complying with a ransom demand unless the political subdivision's legislative authority formally approves the payment or compliance with the ransom demand in a resolution or ordinance that specifically states why the payment or compliance with the ransom demand is in the best interest of the political subdivision.[3]

If the requirements regarding a political subdivision's response to a ransom demand were challenged, a court might examine it with respect to home rule.[4] Municipal corporations and charter counties have local self-government authority, which according to the Ohio Supreme Court includes powers of government that are local in nature, or stated differently, that relate solely to the government and administration of the internal affairs of the municipality or charter

[1] R.C. 9.64(C).

[2] R.C. 9.64(A).

[3] R.C. 9.64(B).

[4] Ohio Constitution, Article XVIII, Section 3 and Article X, Section 3.

county.[5] A court might examine whether managing the response to an incident regarding data and information technology falls within this authority.

Under the bill, a "ransomware incident" means a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a political subdivision's information technology systems or data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.[6]

## Notification of cybersecurity incident or ransomware incident

The bill requires the legislative authority of a political subdivision, following each cybersecurity incident or ransomware incident, to notify both of the following:

- The Executive Director of the Division of Homeland Security within the Department of Public Safety, in a manner prescribed by the Executive Director, as soon as possible but not later than seven days after the political subdivision discovers the incident;
- The Auditor of State, in a manner prescribed by the Auditor, as soon as possible but not later than 30 days after the political subdivision discovers the incident.[7]

## Public records

The bill specifies that any records, documents, or reports related to the cybersecurity program and framework, and the reports of a cybersecurity incident or ransomware incident, are not public records, and are not subject to the disclosure requirements of Ohio Public Records Law.[8] A record identifying cybersecurity-related software, hardware, goods, and services, that are being considered for procurement, have been procured, or are being used by a political subdivision, including the vendor name, product name, project name, or project description, is a security record and also not subject to disclosure.[9]

# HISTORY

| Action | Date |
|---|---|
| Introduced | 05-20-25 |

ANHB0283IN-136/ks

[5] *Beachwood v. Bd. of Elections of Cuyahoga Cty.*, 167 Ohio St. 369 (1958) and *State ex rel. Toledo v. Lynch*, 88 Ohio St. 71 (1913).

[6] R.C. 9.64(A).

[7] R.C. 9.64(D).

[8] R.C. 9.64(E) and 149.43, not in the bill.

[9] R.C. 9.64(F) and 149.433, not in the bill.