

As Introduced

136th General Assembly

Regular Session

2025-2026

H. B. No. 283

Representatives Mathews, A., Ghanbari

To enact section 9.64 of the Revised Code to  
require political subdivisions to adopt a  
cybersecurity program.

1  
2  
3

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF OHIO:

**Section 1.** That section 9.64 of the Revised Code be  
enacted to read as follows:

4  
5

**Sec. 9.64.** (A) As used in this section:

6

(1) "Cybersecurity incident" means any of the following:

7

(a) A substantial loss of confidentiality, integrity, or  
availability of a covered entity's information system or  
network;

8  
9  
10

(b) A serious impact on the safety and resiliency of a  
covered entity's operational systems and processes;

11  
12

(c) A disruption of a covered entity's ability to engage  
in business or industrial operations, or deliver goods or  
services;

13  
14  
15

(d) Unauthorized access to an entity's information system  
or network, or nonpublic information contained therein, that is  
facilitated through or is caused by:

16  
17  
18

(i) A compromise of a cloud service provider, managed 19  
service provider, or other third-party data hosting provider; or 20

(ii) A supply chain compromise. 21

"Cybersecurity incident" does not include mere threats of 22  
disruption as extortion; events perpetrated in good faith in 23  
response to a request by the system owner or operator; or 24  
lawfully authorized activity of a United States, state, local, 25  
tribal, or territorial government entity. 26

(2) "Political subdivision" means a county, township, 27  
municipal corporation, or other body corporate and politic 28  
responsible for governmental activities in a geographic area 29  
smaller than that of the state. 30

(3) "Ransomware incident" means a malicious cybersecurity 31  
incident in which a person or entity introduces software that 32  
gains unauthorized access to or encrypts, modifies, or otherwise 33  
renders unavailable a political subdivision's information 34  
technology systems or data and thereafter the person or entity 35  
demand a ransom to prevent the publication of the data, restore 36  
access to the data, or otherwise remediate the impact of the 37  
software. 38

(B) A political subdivision experiencing a ransomware 39  
incident shall not pay or otherwise comply with a ransom demand 40  
unless the political subdivision's legislative authority 41  
formally approves the payment or compliance with the ransom 42  
demand in a resolution or ordinance that specifically states why 43  
the payment or compliance with the ransom demand is in the best 44  
interest of the political subdivision. 45

(C) The legislative authority of a political subdivision 46  
shall adopt a cybersecurity program that safeguards the 47

political subdivision's data, information technology, and 48  
information technology resources to ensure availability, 49  
confidentiality, and integrity. The program shall be consistent 50  
with generally accepted best practices for cybersecurity, such 51  
as the national institute of standards and technology 52  
cybersecurity framework, and the center for internet security 53  
cybersecurity best practices, and may include, but are not 54  
limited to, the following: 55

(1) Identify and address the critical functions and 56  
cybersecurity risks of the political subdivision. 57

(2) Identify the potential impacts of a cybersecurity 58  
breach. 59

(3) Specify mechanisms to detect potential threats and 60  
cybersecurity events. 61

(4) Specify procedures for the political subdivision to 62  
establish communication channels, analyze incidents, and take 63  
actions to contain cybersecurity incidents. 64

(5) Establish procedures for the repair of infrastructure 65  
impacted by a cybersecurity incident, and the maintenance of 66  
security after the incident. 67

(6) Establish cybersecurity training requirements for all 68  
employees of the political subdivision; the frequency, duration, 69  
and detail of which shall correspond to the duties of each 70  
employee. Annual cybersecurity training provided by the state, 71  
and training provided for local governments by the Ohio 72  
persistent cyber initiative program of the Ohio cyber range 73  
institute, satisfy the requirements of this division. 74

(D) The legislative authority of a political subdivision, 75  
following each cybersecurity incident or ransomware incident, 76

shall notify both of the following: 77

(1) The executive director of the division of homeland 78  
security within the department of public safety, in a manner 79  
prescribed by the executive director, as soon as possible but 80  
not later than seven days after the political subdivision 81  
discovers the incident; 82

(2) The auditor of state, in a manner prescribed by the 83  
auditor of state, as soon as possible but not later than thirty 84  
days after the political subdivision discovers the incident. 85

(E) Any records, documents, or reports related to the 86  
cybersecurity program and framework in division (C) of this 87  
section, and the reports of a cybersecurity incident or 88  
ransomware incident under division (D) of this section, are not 89  
public records under section 149.43 of the Revised Code. 90

(F) A record identifying cybersecurity-related software, 91  
hardware, goods, and services, that are being considered for 92  
procurement, have been procured, or are being used by a 93  
political subdivision, including the vendor name, product name, 94  
project name, or project description, is a security record under 95  
section 149.433 of the Revised Code. 96