OHIO AUDITOR OF STATE
KEITH FABER

Auditor of State
Bulletin 2025-007

DATE ISSUED: **August 27, 2025**

TO: **All Public Offices**
Independent Public Accountants

FROM: **Keith Faber**
Ohio Auditor of State

SUBJECT: **Adoption of Cybersecurity Program**

Background

Ohio Rev. Code § 9.64, enacted through House Bill 96, requires political subdivisions to set and adopt standards safeguarding against cybersecurity threats and ransomware attacks. This bulletin details the requirements of Ohio Rev. Code § 9.64, which are effective September 30, 2025.

Local governments, typically defined as "political subdivisions"[1], have increasingly become targets for cybercriminals. They are vulnerable to cyber-attack schemes because of limited cybersecurity budgets, outdated systems and a range of accessible electronic and digital services. Cyber-attacks—such as ransomware, phishing, social engineering, and data breaches—disrupt government services, expose personal and financial information, incur significant costs, and reduce public trust.

Cybersecurity Program Compliance Requirements

Under this new law, each political subdivision's legislative authority **shall** adopt a "cybersecurity program" that safeguards the entity's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. *See* Ohio Rev. Code § 9.64 (C).

[1] Political subdivision is defined as 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.

The program shall be consistent with generally accepted best practices for cybersecurity[2] and may include, but are not limited to 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. The frequency, duration, and detail of which shall correspond to the duties of each employee. Annual training provided by the state and the Ohio Persistent Cyber Initiative (O-PCI) program of the Ohio Cyber Range Institute, satisfies the training requirements. The O-PCI program delivered by the Ohio Cyber Range Institute (https://www.ohiocyberrangeinstitute.org/opci) and the Ohio Cyber Reserve (https://homelandsecurity.ohio.gov/ohio-cyber-integration-center/overview) includes online, hybrid and in person modules tailored to various types of organizations, from small to large, rural to urban and is funded by the State and Local Cybersecurity Grant Program.

Political subdivisions should adopt a cybersecurity program/policy that is tailored to the unique environment/needs of their entity.

Cyber Security Program Implementation Due Dates

Entity Type	**Due Date**
County	January 1, 2026
City	January 1, 2026
All Other Entity Types	July 1, 2026

Reporting Requirements after Discovery of Cybersecurity or Ransomware Incident

Upon discovering a cybersecurity incident or ransomware incident, the legislative authority of a political subdivision shall notify both:

- The Executive Director of Ohio Homeland Security within the Ohio Department of Public Safety as soon as possible but not later than 7 days after discovering the incident. Incidents can be reported to Homeland Security's Ohio Cyber Integration Center (OCIC)

[2] Examples of generally accepted cybersecurity standards that entities use to build best practices for cybersecurity include, but are not limited to, the National Institute of Standards and Technology (NIST) cybersecurity framework and the Center for Internet Security (CIS) cybersecurity best practices.

at: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center, OCIC@dps.ohio.gov or 614-387-1089.

- The Ohio Auditor of State as soon as possible but not later than thirty (30) days after discovering the incident. Incidents can be reported to the Ohio Auditor of State via email to Cyber@ohioauditor.gov using the form located at: https://ohioauditor.gov/fraud/cybersecurity.html

Cybersecurity Incident Defined

A cybersecurity incident includes *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 operation systems and processes.
- A disruption of a covered entity's ability to engage in business or industrial operations or deliver goods or services.
    - A disruption could include payment re-direct, payroll re-direct, spear phishing. Refer to AOS Audit Bulletin 2024-003 for additional examples.
- Unauthorized access to an entity's information system or network, or nonpublic information contained therein, that is facilitated 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.

A 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 United States, state, local, tribal, or territorial government entity.

Ransomware Incident Defined

Ransomware incident is defined as 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.

Ransomware Payment Only Permitted after Public Vote by Legislative Authority

A political subdivision experiencing a ransomware incident shall not pay or otherwise comply 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.

Public Records Exemption

Records, documents, or reports related to the cybersecurity program and framework, and reports of a cybersecurity incident or ransomware incident are not public records under Ohio Rev. Code § 9.64. Records 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 vendor name, product name, project name, or project description constitute "security records" and are exempt from the requirements to produce those records in response to a public records request.

Testing Compliance Requirements

Compliance procedures will be developed and incorporated into the Ohio Compliance Supplement.

Guidance

Additional cybersecurity resources, including incident response tips and free training are available on the Auditor of State's website at https://ohioauditor.gov/fraud/cybersecurity.html.

Questions

If you have any questions regarding the information presented in the Bulletin, please contact the Special Investigations Unit at the Auditor of State's Office at 800-282-0370.

Keith Faber
Ohio Auditor of State