COUNTY ADVISORY BULLETIN
CAB
Published by the County Commissioners Association of Ohio

209 East State Street • Columbus, Ohio 43215-4309
Phone: 614-221-5627 • Fax: 614-221-6986 • www.ccao.org

Bulletin 2025-13 September 2025

COUNTY CYBERSECURITY PROGRAMS

APPLICABLE LEGISLATION: House Bill 96 (136th General Assembly)

REVISED CODE SECTIONS ENACTED: 9.64

LEAD SPONSORS: Rep. Brian Stewart

HOUSE COSPONSORS: Bird, John, Click, Creech, Daniels, Demetriou, Dovilla, Ghanbari, Hall, T., McClain, Miller, K., Miller, M., Plummer, Santucci, Thomas, D., Williams, Willis, Young

SENATE COSPONSORS: Brenner, Cirino, Gavarone, Johnson, Lang, Roegner, Romanchuk

EFFECTIVE DATE: September 30, 2025

BACKGROUND

In 2024, the Auditor of State's office began leading conversations with local government organizations, including CCAO, about state law regarding cybersecurity and ransomware. Initially, proposed legislative drafts would have banned political subdivisions from complying with a ransom in any situation. Through interested party conversations, the policy recommendations evolved into requiring political subdivisions to adopt cybersecurity programs and be transparent with the public about compliance with any ransom demands.

In the 136th General Assembly, Representatives Adam Mathews and Haraz Ghanbari introduced House Bill 283 to address these issues. Senator Tim Schaffer introduced Senate Bill 203, a companion to the House bill. The contents of these bills were ultimately adopted in House Bill 96, the state operating budget.

DEFINITIONS

The bill adds definitions of cybersecurity incident and ransomware incident to the Revised Code. Previously these terms were undefined.

Cybersecurity incident: Defined as 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.

A cybersecurity incident is explicitly not 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: 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.

The provisions in R.C. 9.64 apply to political subdivisions, which are 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.”

This CAB speaks specifically in terms of counties, but all political subdivisions are subject to the same requirements under R.C. 9.64.

(R.C. 9.64(A))

MANDATORY CYBERSECURITY PROGRAM

Counties are required to adopt a cybersecurity program. The purpose of the program is to safeguard the county’s data, information technology and information technology resources to ensure availability, confidentiality and integrity.

The legislative authority of a political subdivision is required to adopt the program. In counties, this is the board of commissioners or the county council. The program will apply to all entities within the county, including other officeholders’ systems.

In implementation webinars with CyberOhio and the Auditor of State offices, the emphasis has been on implementing a “program” not a “policy.” A “program” implies there is a person and/or entity in charge of these cybersecurity functions for the county. The goal, and what the state is looking for, is not a binder full of policies, but rather a framework for performing these cybersecurity functions in the county on an ongoing basis.

(R.C. 9.64(C))

CYBERSECURITY PROGRAM INITIAL IMPLEMENTATION TIMELINE

While the effective date of R.C. 9.64 is September 30, 2025, the Auditor of State's office will begin auditing counties and cities for compliance with the cybersecurity program requirement beginning January 1, 2026.

For all other political subdivisions, the deadline for adoption is July 1, 2026.

The January 1, 2026 implementation deadline applies to county government for which the board of county commissioners or county council is the legislative authority.

(Auditor of State Bulletin 2025-007)

CYBERSECURITY PROGRAM REQUIREMENTS

Cybersecurity programs should be tailored to the needs of the county.

The statute mandates the program to be consistent with generally accepted best practices for cybersecurity. Examples included in the statute include the National Institute of Standards and Technology Cybersecurity Framework and the Center for Internet Security Cybersecurity Best Practices.

The following are items that a county's cybersecurity program may include. Programs are not limited to these items.

- 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 shall correspond to the duties of each employee. 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 the requirements of this division.

CCAO and the County Risk Sharing Authority (CORSA) have developed model program recommendations included as Appendix A of this bulletin. CORSA members may obtain a copy of CORSA's Cyber Best Practice Guide and Cyber Model Policy at www.corsa.org by clicking on the Risk Management and then the Cyber Risk Management tab.

(R.C. 9.64(C))

AUDIT REQUIREMENTS

The Auditor of State's office is in the process of developing the updated Ohio Compliance Supplement. The auditors use the Supplement to complete their testing of local governments through the audit process. The updated Supplement will include direction with respect to the implementation of the new cybersecurity program law.

The Supplement will be publicly available at https://ohioauditor.gov/references/compliancemanuals.html when the updates are complete.

The Auditor of State is still developing compliance procedures. Failure to comply with the January 1, 2026 timeline could result in an item of noncompliance for a county during the audit process.

(Auditor of State Bulletin 2025-007)

FUNDING

HB 96 did not include any funding specifically for implementation of cybersecurity programs.

RANSOM PAYMENTS AND DEMANDS

Effective September 30, 2025, if a county experiencing a ransomware incident wishes to pay or otherwise comply with a ransom demand, the board of commissioners or county executive and council must formally approve the payment or compliance in a resolution. The resolution must specifically state why the payment or compliance is in the best interest of the county.

If a county does not adopt such a resolution, the payment or compliance of a ransom demand is prohibited.

(R.C. 9.64(B))

NOTIFICATION OF INCIDENT

The statute implements new notification requirements when an incident occurs, effective September 30, 2025. If a cybersecurity incident or ransomware incident occurs, a board of county commissioners or, in a charter county, the county council, must notify, as soon as possible:

- Within 7 days, the Executive Director of the Division of Homeland Security within the Ohio Department of Public Safety (Ohio Cyber Integration Center); and

- Within 30 days, the Auditor of State.

Both entities listed above have released the required reporting processes which are described below.

Ohio Cyber Integration Center (OCIC) Reporting Process (within 7 days of incident)

Step 1: County contacts OCIC at 614-387-1089 or OCIC@dps.ohio.gov. An intake form will be completed under a nondisclosure agreement. OCIC will generate a case number and notify stakeholders.

Required reporting information to OCIC includes:

- County contact information including: name, address, phone number;
- Point of contact and contact information including name, title, phone number, and email;
- Date and time of incident;
- Type of incident and any mitigation steps taken prior to reporting;
- Information on affected devices and if such devices have been removed or powered off;
- Status of cyber insurance and information on if the provider has been contacted;
- Other entities contacted regarding the incident; and
- Security team details including device count, protected personal information (PPI) presence, state connected devices involved, and date of last backup.

Step 2: A coordination call will take place including the Department of Administrative Services, Department of Public Safety, Secretary of State (if elections are impacted), Federal Bureau of Investigation, Department of Homeland Security, and Cybersecurity and Infrastructure Security Agency.

Step 3: OCIC will facilitate response coordination and tracking, using a case management system for tracking and documentation.

Step 4 (if needed): Follow up calls will occur as needed for forensics, mitigative actions, etc.

Step 5: OCIC will share final disposition and lessons learned.

To request additional information from OCIC, please use the following contact information:
Phone: 614-387-1089
Email: OCIC@dps.ohio.gov
Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center

Auditor of State Reporting Process (within 30 days of incident)

In the event of an incident, the Auditor of State requires counties to fill out the cybersecurity reporting form (found here) and submit the completed form to Cyber@ohioauditor.gov. These instructions and the link to the form are available on the Auditor of State's website. These instructions can also be found in Auditor of State Bulletin 2025-007.

(R.C. 9.64 (D); Auditor of State Bulletin 2025-007)

PUBLIC RECORDS EXEMPTIONS

The statute exempts the following from public records:

- Records, documents or reports related to the mandated cybersecurity programs required under R.C. 9.64(C);

- Reports of a cybersecurity incident or ransomware incident under R.C. 9.64(D).

  (R.C. 9.64(E))

The statute further defines 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, as a security record under R.C. 149.433. Security records are not subject to disclosure.

(R.C. 9.64(F))

CyberOhio plans to release additional information about what is exempt from disclosure and what is not.

RESOURCES FOR IMPLEMENTATION

In addition to resources mentioned throughout this bulletin, the following sources are available to political subdivisions.

CyberOhio

Landing Page for Implementation: https://cyber.ohio.gov/priorities/assisting-local-government-entities/ohio-hb-96-new-cybersecurity-requirements-for-public-entities
The landing page will include Frequently Asked Questions and upcoming webinar opportunities.

Ohio Cyber Reserve

Ohio Cyber Range Institute

Cyber Frontline First Aid Kit

Training

Ohio Cyber Range Institute Ohio-Persistent Cyber Initiative

Ohio Cyber Reserve

CISA Learning on NICCS

CISA Cybersecurity Training and Exercises

ESET Free Cybersecurity Awareness Training

National Cybersecurity Alliance Security Awareness Episodes

Auditor of State

Auditor of State Bulletin 2025-007

Landing Page for Implementation: https://ohioauditor.gov/fraud/cybersecurity.html

Ohio Department of Administrative Services

State Incident Response and Cybersecurity Policies

Appendix A: Model Cybersecurity Program Resources

Introduction

House Bill 96 of the 136th General Assembly requires counties and all political subdivisions to adopt a cybersecurity program. In implementation webinars with CyberOhio and the Auditor of State offices, the emphasis has been on implementing a "program" not a "policy." A "program" implies there is a person and/or entity in charge of these cybersecurity functions for the county. The goal, and what the state is looking for, is not a binder full of policies, but rather a framework for performing these cybersecurity functions in the county on an ongoing basis.

R.C. 9.64 references the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security Cybersecurity Best Practices as examples of best practices. Simply put, NIST is the "gold standard" of cybersecurity practices. As you identify your cybersecurity program leads in your counties, CCAO recommends remaining aware and knowledgeable of NIST recommendations and resources.

R.C. 9.64 recommends every cybersecurity program cover six categories. CCAO and CORSA have provided sample procedural steps and, in some cases, policies that counties can take to address each category in their cybersecurity programs. R.C. 9.64 becomes effective on September 30, 2025. The Auditor of State will begin auditing for compliance with the cybersecurity program requirement in R.C. 9.64 beginning January 1, 2026.

As each county is unique, counties are advised to consult with their IT Manager, Risk Manager and/or Loss Control Coordinator in order to modify sample policies as necessary to meet the county's specific needs.

1. Identify critical functions and risks

The first step of implementing a cybersecurity program is to identify critical functions and risks. Start this process by identifying the roles that various individuals/positions in the county will hold throughout the cybersecurity process. Key individuals throughout the organization (not just IT) should be identified to participate in cybersecurity program activities.

Once the team has been identified, risk assessments need to be performed to identify where the county is vulnerable. These assessments will establish the baseline for subsequent steps to build upon. This exercise should be performed at least once per year to keep documentation up-to-date and to also set the coming year's security goals.

Resources:

EXAMPLE CYBER TEAM & ROLES

CYBER TEAM & ROLES TEMPLATE

EXAMPLE OF RISK ANALYSIS

RISK ANALYSIS TEMPLATE

2. Assess the potential impact of breaches

The second step is to analyze the possible scenarios when a potential breach occurs. The goal is to identify ways to contain the damage and devise strategies detailing how to recover when damage occurs. Knowing what type of data has been accessed is critical. Unauthorized access to Personal Identifiable Information (PII) would require notices to the individuals involved.

Resources:

IMPACT ANALYSIS

IMPACT ANALYSIS TEMPLATE

3. Implement threat detection mechanisms

Once the risks have been identified, deploy tools and resources to help protect the assets that have been identified. A range of strategies, vendors, tools, etc. can be deployed. Here is a short list to provide some recommendations of threat detection and protection mechanisms:

Phishing

- Advanced Filtering and Detection
  - Anti-Impersonation, Anti-Phishing & Spam, Attachment & Link scanning, DKIM, DMARC, etc.
- Perimeter network firewall configuration
- Geo-Location blocking
- User Training

Endpoint Protection

- Antivirus (AV) and Endpoint Detection and Response (EDR) software
- Remote Monitoring and Management (RMM) software

Server Protection

- Network Segmentation
  - Create multiple segments that the network firewall can inspect
  - Create barriers between users and servers
  - Create barriers between application servers and infrastructure servers
  - Inspect everything
- Antivirus (AV) and Endpoint Detection and Response (EDR) software
- Remote Monitoring and Management (RMM) software

Network & System Monitoring

- Log Aggregation & Storage
- Alert & Notify based on logs

- Network Scanning & Assessments – Internal & External
  - Should be performed several times per year

4. Establish incident response procedures

Incident Response Procedures should include exact steps that users should take if something nefarious should occur. These steps typically involve reporting to a superior the potential incident. The superior then should have clear guidelines on how to handle the potential incident. If it is deemed to be a cyber incident, the Incident Response Team is engaged. This team will include the IT team and the organization leadership team. A template Incident Response Policy is included below. As a reminder, HB 96 implemented new reporting requirements. For details, please reference the "**NOTIFICATION OF INCIDENT**" section of County Advisory Bulletin 2025-13.

Resources:

INCIDENT RESPONSE PLAN

INCIDENT RESPONSE PLAN PLANNING TOOL

5. Plan for recovery and continuity

Disaster Recovery Planning (DRP) and Business Continuity (BC) are critical for responding to a cybersecurity incident, especially ransomware.

DRP is a formal, documented strategy outlining the steps an organization takes to resume critical IT systems and operations after a disruption, such as a natural disaster, cyberattack, or system failure. A DRP focuses on the technical recovery of IT infrastructure and data, serving as a subset of a broader business continuity plan (BCP) to minimize downtime and financial losses. Key components include an IT inventory, backup procedures, defined recovery time and point objectives (RTO/RPO), and an incident response team with communication protocols. Data backups and procedures should be tested throughout the year to prove viability.

A BC plan is a structured strategy and set of documented procedures designed to ensure an organization can continue its essential functions and operations during and after a disruptive event, such as a natural disaster, cyber incident, or pandemic. The plan helps minimize downtime, safeguard critical assets, protect employees and customers, and preserve the company's reputation and financial stability by outlining how to respond to, recover from, and restore operations after a crisis.

Resources:

DISASTER RECOVERY PLAN TEMPLATE

BUSINESS CONTINUITY PLAN TEMPLATE

6. Define employee training requirements

Employee cybersecurity training teaches staff to recognize cyber threats and adopt secure online practices to protect themselves and the organization's data. This training is crucial for reducing human error, preventing attacks like phishing and malware, and fostering a stronger security culture. Key topics include password management, email security, data privacy, identifying social engineering, and secure remote work practices. Organizations can use interactive programs, simulations, and regular updates to keep employees informed and engaged, with many options available from vendors like KnowBe4 and Infosec. The Ohio Cyber Range Institute's Ohio Persistent Cyber Improvement (O-PCI) program offers free cybersecurity training to all local government entities.

All employees should be required to take Cyber Awareness Training. Employees whose roles have more authority (and therefore more risk), including in the financial transactions space, should be required to take additional training to empower them to handle the additional threats and exposure that they face.

Resources:

SAMPLE TRAINING POLICY

OHIO DEPARTMENT OF ADMINISTRATIVE SERVICES IT SECURITY AWARENESS AND TRAINING (POLICY IT-15)

Appendix B: Auditor of State Bulletin 2025-007

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

Keith Faber
Ohio Auditor of State