CyberOhio

NEW CYBERSECURITY REQUIREMENTS

For Ohio Local Governments

Overview of New Language Passed in Am. Sub. House Bill 96

Kirk Herath

Cybersecurity Strategic Advisor to Governor DeWine

Chair, CyberOhio

LEGISLATIVE BACKGROUND – HB 96 NEW CYBER LAW

- Signed by Governor DeWine on June 30, 2025
- Takes effect **September 30, 2025**
- Language can be found in ORC Section 9.64
- Applies to all Ohio political subdivision

HB 96: KEY CYBER MANDATES FOR LOCAL GOVERNMENT ENTITIES

- **Local Government Entities Must:**
    - Implement a cybersecurity program
    - Obtain approval from their legislative body for ransomware payments
    - Cyber incidents must be reported within specific timeframes to DPS and AOS.
    - While support is available from several state programs, if you have an existing private-sector or third-party IT and/or Cybersecurity provider, stay the course! There's a lot of work to do and this will take a concerted private-public partnership to succeed.

This presentation is for informational purposes only

- Not legal advice
- Local governments should consult with their legal counsel and technology vendors to ensure compliance
- DPS and AOS will be releasing additional guidance and instructions on compliance before the effective date.

WHO MUST COMPLY & WHEN

- Applies to all political subdivisions:
- "Political subdivision" means 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.
- Auditor of State Compliance Timeline for Cyber Program
  - Counties and Cities should have a program in place by **January 1, 2026.**
  - For all other entities, the deadline will be **July 1, 2026.**
- Compliance Timeline to begin Reporting to DPS and Auditor of State
  - **September 30, 2025**

CYBER PROGRAM

- **Local Governments Must:**

  Establish a cybersecurity program that:

  - Safeguards data, IT, and IT resources
  - Ensures availability, confidentiality, and integrity
  - Follows best practices like:
    - **NIST Cybersecurity Framework (CSF)**
    - **Center for Internet Security (CIS)** controls

PROGRAM COMPONENTS

Depending on the size and complexity of an organization, a compliant cybersecurity program should:

- **Identify critical functions** and risks
- **Assess** the potential **impact of breaches**
- **Implement** threat **detection mechanisms**
- **Establish incident response procedures**
- **Plan** for **recovery and continuity**
- Define **employee training requirements**

RANSOMWARE PAYMENT RESTRICTIONS

New Requirement

Local governments **may not pay or comply** with ransomware demands **unless**:

- A formal **resolution or ordinance** is passed
- The resolution **must justify** why payment is in the best interest of the jurisdiction

(B) 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.

DEFINITION OF RANSOMWARE INCIDENT

Ransomware Incident =

Malicious software that:

- Gains unauthorized access
- Encrypts, modifies, or disables data
- Demands payment to restore access or prevent data release

(3) "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.

DEFINITION OF REPORTABLE INCIDENTS

Cybersecurity Incident Includes:

- Loss of data confidentiality, integrity, or availability
- Operational disruption
- Business continuity failure
- Unauthorized access due to:
  - Third-party or supply chain compromise

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

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

information system or network;

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

and processes;

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

(d) Unauthorized access to an entity's information system or network, or nonpublic

information contained therein, that is facilitated through or is caused by:

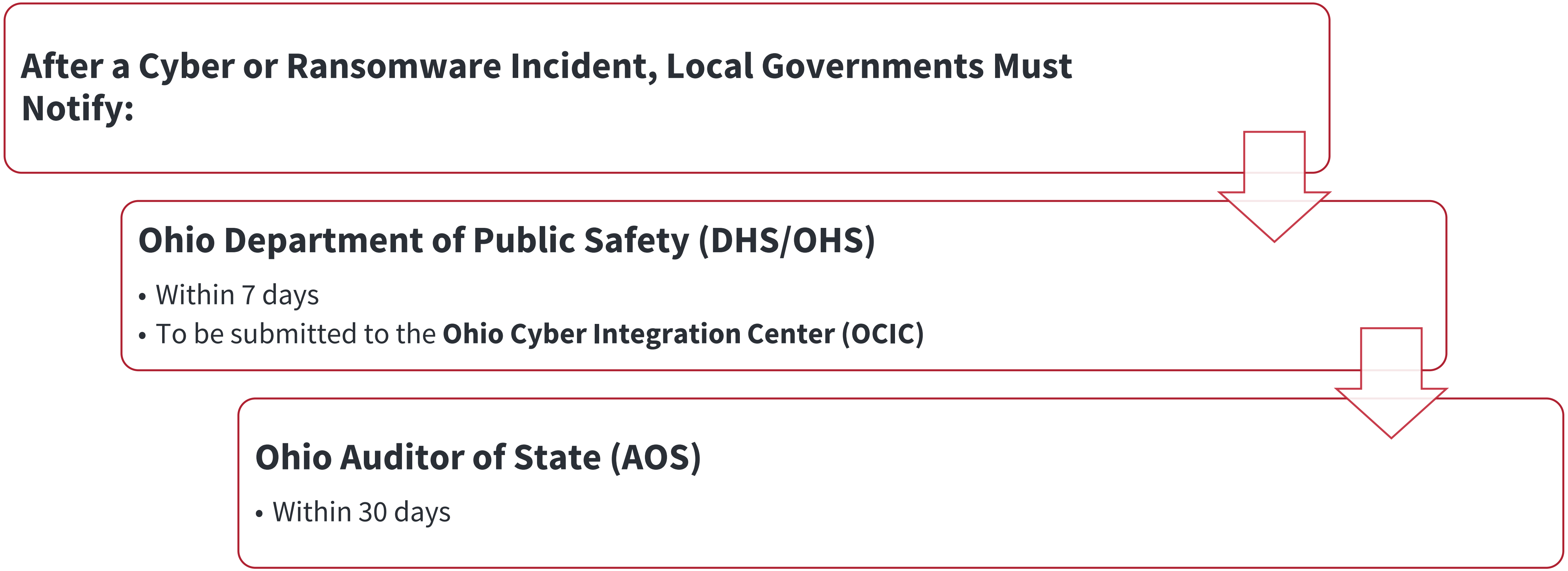
(i) A compromise of a cloud service provider, managed service provider, or other third-party

data hosting provider; or

(ii) 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 United States, state, local, tribal, or territorial government entity.

CYBER INCIDENT REPORTING REQUIREMENTS



After a Cyber or Ransomware Incident, Local Governments Must Notify:

Ohio Department of Public Safety (DHS/OHS)

- Within 7 days
- To be submitted to the **Ohio Cyber Integration Center (OCIC)**

Ohio Auditor of State (AOS)

- Within 30 days

Reporting procedures to be issued soon

OCIC INCIDENT REPORTING PROCESS

- **Within 7 Days of Incident:**

  1. Affected entity contacts OCIC
     - Intake form completed (under NDA)
     - Case number generated, stakeholders notified
  2. Initial Coordination Call Setup:
     - DAS OISP, DPS IT/LEADS, SoS (election), FBI, DHS, CISA
     - Ohio Cyber Reserve & ONG (if requested, VOCO required)
  3. OCIC facilitates response coordination & tracking
     - Case management system used for tracking & documentation
  4. Follow-up Calls (as needed):
     - Forensics, mitigative actions, TTPs/IOCs, reconnection, AAR
  5. OCIC shares final disposition & anonymized lessons learned

INCIDENT INFORMATION REQUIREMENTS

- **Organization Details & Contact Info:**
- • Name, Address, County, Phone, Org Type
- • POC: Name, Title, Phone, Email

Security Team Details:

• Device count, PPI presence, state connected device?

• Last backup date

Incident Specifics:

• Date/Time of incident or suspicious activity

• Type of incident, mitigation steps taken prior to reporting

• Affected devices removed/turned off?

• Cyber insurance status & provider contacted?

• Others contacted regarding incident?

OHIO CYBER INTEGRATION CENTER

To Report a Cybersecurity Incident or Request Resources:

- ➢Phone: 614-387-1089
- ➢Email: OCIC@dps.ohio.gov
- ➢Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center

CYBERSECURITY TRAINING

Annual Training

- Tailored to job duties
- May be provided by the State of Ohio
- LGEs are encouraged to utilize existing capabilities provided by their MSPs.
- Free training offered by:
  - **Ohio Persistent Cyber Initiative (O-PCI)**
  - **Ohio Cyber Reserve**

O-PCI

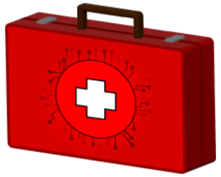
Free Cybersecurity Training for Local Government Entities

- Whole-of-organization training
- Tailored to the roles of employees (Executive/IT/General)
- Includes online modules, creation of plans/policies/procedures, cyber exercises, and vulnerability assessments

OHIO PERSISTENT CYBER IMPROVEMENT

ohiocyberrangeinstitute.org/opci

9,000+ public employees have completed 8,000+ hours of training in counties, cities, libraries, schools, and health districts across Ohio.



BONUS Resource: Cyber Frontline First Aid Kit (CFFAK)

ohiocyberrangeinstitute.org/cffak

TECH CRED: TECHCRED.OHIO.GOV

TechCred helps Ohioans learn new skills and helps employers build a stronger workforce with the skills needed in a technology-infused economy.

Many of these trainings can be completed online!

These technology-focused credentials take a year or less to complete and prepare current and future employees for the technology jobs Ohio employers need.

Application and Reimbursement Process

- Employer applies for funding during application period
- The Ohio Department of Development scores application and awards funding
- Employer sponsors current or prospective employees to complete an eligible credential program
- Current or prospective employee successfully completes the program and receives approved credential
- Employer submits a copy of the credential earned, an invoice which clearly identifies the per person cost of the credential, and proof of payment.

- Many Cyber and IoT Certifications Available
- https://techcred.ohio.gov/about/credential-list

Employer Eligibility

Employers of all sizes and in all industries are encouraged to apply. Only one application will be accepted per employer per application period. Agencies of the State of Ohio are not eligible to receive reimbursement. Additionally, training providers are not eligible to receive reimbursement for employees trained in-house. If a training provider wishes to utilize TechCred to upskill their employees, they must use an outside training provider.

PUBLIC RECORDS EXEMPTION

Records related to:

- Cybersecurity programs
- Incident reports and procurement documents are **not public records** under R.C. §149.43

This protects the confidentiality of sensitive systems and responses.

KEY TAKEAWAYS

- All local governments must implement cybersecurity programs
- Annual employee training is highly recommended to meet the program requirement
- Ransom payments require formal approval
- Cyber incidents must be reported within specific timeframes
- Free support is available from several state programs
- If you have an existing private-sector IT and/or Cybersecurity Partner, stay the course!

This presentation is for informational purposes only

- Not legal advice
- Local governments should consult with their legal counsel to ensure compliance

STATE SUPPORT PATHWAYS

CyberOhio & State of Ohio Capabilities to Support Compliance

The following state-led programs are available to assist local governments in meeting some of the cybersecurity requirements of HB 96:

- **Ohio Cyber Integration Center (OCIC)**
- **Ohio Persistent Cyber Initiative (O-PCI)**
- **Ohio Cyber Reserves**

Each offers a defined pathway for risk assessment, training, incident response planning, and long-term cyber maturity.

Look for future deeper dive webinars on each capability.

QUESTIONS & SUPPORT

- **Need Assistance?**
- Contact CyberOhio at Cyber.Ohio.gov
- Contact the Auditor of State at https://ohioauditor.gov/contact.html
- We’re here to help you meet the new cybersecurity requirements.