CyberOhio

CyberOhio

CCAO/CEAO Winter Conference

December 4th, 2025

Kirk Herath
Cybersecurity Strategic Advisor to Governor DeWine
Chair, CyberOhio

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

BUILDING A CYBER PROGRAM

The legislative authority of a political subdivision shall adopt a cybersecurity program that:

1. Safeguards the entity's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.
2. The program shall be consistent with generally accepted best practices for cybersecurity, such as,
   - **National Institute of Standards and Technology (NIST) cybersecurity framework** and
   - **Center for Internet Security (CIS)** cybersecurity best practices.

As stated on the next slides, if you are currently complying with the AOS Financial Statement Audit, you are already significantly on your way to having a cyber program in accordance with NIST CSF and CIS.

- The program **MAY** include, but is not limited to the following:
  - 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
    - Training from Ohio Persistent Cyber Initiative (O-PCI) could satisfy this requirement.

AUDITOR OF STATE BULLETIN 2024-003

- Ohio governments are increasingly falling victim to cybercrimes in the form of payment “re-direct” and business email compromise schemes.
- In 2023, the Auditor of State issued an Advisory alerting Ohio governments to an increase in cybercrime and providing guidance on what to look for and how to prevent attacks.
- This bulletin sets clear standards and expectations for Ohio governments and public employees regarding the handling of requests for payment re-directs.
- AOS has issued FFRs against fiscal officers for failing to follow protocols that resulted in the local government falling victim to cybercrimes.
    - Example: changing employee or vendor bank accounts to route payments to the bad actor's account.

Financial Statement Audit

- Currently, AOS audits for IT controls in financial audits.
- What IT controls do auditors look for currently?
  - IT Strategy – (IT planning and IT training)
  - Change Management (maintaining support, patches, upgrades)
  - Security Management (policies such as IT policies such as cyber policies and cyber awareness training programs)
  - System Level Access Controls (multi-factor, password controls, remote access, firewall)
  - Application Level Access Controls (multi-factor, role-based access, least privileged access)
  - Contracts with Vendors
  - Physical Security (contract, locked room, environmentally safe, access protection)
  - System Admin & Maintenance (vulnerability checks and monitoring up-time)
  - Backup (backups SHOULD BE TESTED and disconnected/offline)
  - Disaster recovery & business continuity (plan for what happens in a disaster, should have a copy off-site)

Financial Statement Audit

- **Currently, AOS audits for IT controls in financial audits.**
- **In other words, the following program elements are already audited by AOS and should be in place now.**
- **With these elements in place, your entity has already made significant strides toward a cyber program.**

Program Element (already audited by AOS)	Relevant NIST Cybersecurity Framework (CSF) Function(s)	Relevant CIS Controls v8 (IG1) Reference
IT Strategy (planning, IT training)	**Govern (GV)** – establish strategy, assign roles. **Protect (PR.AT)** – awareness & training.	**CIS Control 14** – Security Awareness & Skills Training. **CIS Control 17** – Incident Response Management (basic planning).
Change Management (patches, upgrades, support)	**Protect (PR.MA, PR.IP)** – maintenance and secure configuration. **Identify (ID.AM)** – asset inventory.	**CIS Control 7** – Continuous Vulnerability Management. **CIS Control 4** – Secure Configuration of Enterprise Assets & Software.
Security Management (policies, cyber awareness training)	**Govern (GV)** – policies, oversight. **Protect (PR.AT)** – training.	**CIS Control 14** – Security Awareness & Skills Training. **CIS Control 2** – Inventory & Control of Software Assets (via policies).
System-Level Access Controls (MFA, passwords, remote access, firewall)	**Protect (PR.AC)** – identity management, authentication, network access.	**CIS Control 5** – Account Management. **CIS Control 6** – Access Control Management. **CIS Control 12** – Network Infrastructure Management.
Application-Level Access Controls (MFA, role-based access, least privilege)	**Protect (PR.AC)** – application access, least privilege.	**CIS Control 5** – Account Management. **CIS Control 6** – Access Control Management.
Contracts with Vendors	**Govern (GV.SC)** – supply chain risk management.	**CIS Control 15** – Service Provider Management.
Physical Security (locked rooms, contracts, environmental safety)	**Protect (PR.PH)** – physical security & environmental protections.	**CIS Control 16** – Application Software Security (partial). **CIS Control 12** – Network Infrastructure (physical protections).
System Admin & Maintenance (vulnerability checks, uptime monitoring)	**Protect (PR.MA)** – maintenance. **Detect (DE.CM)** – monitoring.	**CIS Control 7** – Continuous Vulnerability Management. **CIS Control 8** – Audit Log Management.
Backup (tested, disconnected/offline)	**Protect (PR.DS)** – data security. **Recover (RC.RP)** – recovery planning.	**CIS Control 11** – Data Recovery.
Disaster Recovery & Business Continuity (off-site copy, recovery planning)	**Recover (RC.RP, RC.IM)** – recovery planning, improvements.	**CIS Control 11** – Data Recovery. **CIS Control 17** – Incident Response Management (continuity).

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

WHO SHOULD BE INVOLVED?

- Developing a strong cybersecurity program for any local government, particularly counties, requires a **collaborative, cross-functional team** that brings together technical, administrative, and educational expertise.

County Leadership	**County Commissioners**: Approve policies, budgets, and risk management strategies related to cybersecurity.
	Agency and Office Leadership: Provide strategic direction, allocate resources, and ensure cybersecurity is prioritized at the highest level.
	Treasurer, Auditor, Sheriff & Related Personnel: Duty to safeguard and protect financial information. Should work closely with Commissioners and staff.
	Data Board: Where it exists, work closely with the Board to ensure continuity of policies and strategy.
IT and Cybersecurity Personnel	**Chief Information Officer (CIO)**: Leads the technical planning and implementation of cybersecurity measures.
	Network and Systems Administrators: Manage firewalls, endpoint protection, access controls, and monitoring systems.
	Information Security Officer (if available): Oversees risk assessments, incident response, and compliance with data protection laws.

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.

Section 121.22 (F)– Emergency meeting can be called with less than 24 hours notice and still be in compliance with Open Meetings

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 RC 9.64(A)(1)

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

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)

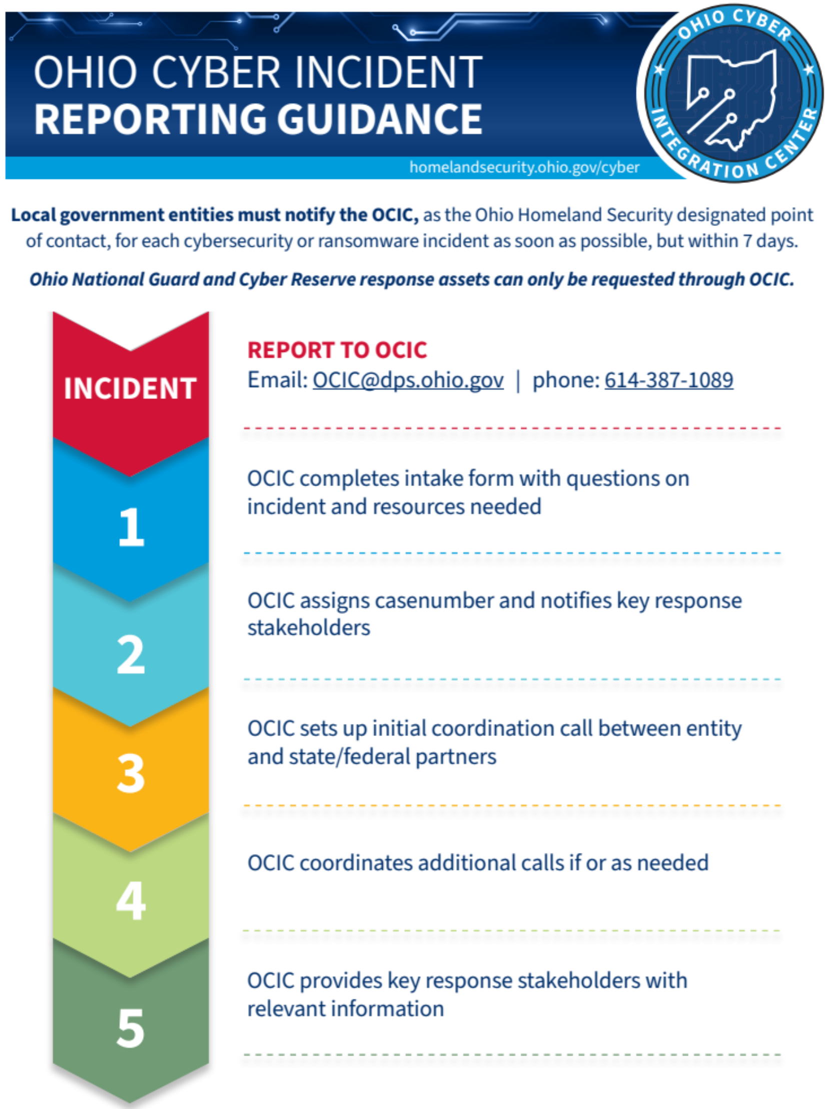
3. OCIC facilitates response coordination & tracking

  - 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



OHIO CYBER INCIDENT REPORTING GUIDANCE

homelandsecurity.ohio.gov/cyber

OHIO CYBER INTEGRATION CENTER

Local government entities must notify the OCIC, as the Ohio Homeland Security designated point of contact, for each cybersecurity or ransomware incident as soon as possible, but within 7 days.

Ohio National Guard and Cyber Reserve response assets can only be requested through OCIC.

INCIDENT — **REPORT TO OCIC**
Email: OCIC@dps.ohio.gov | phone: 614-387-1089

1 — OCIC completes intake form with questions on incident and resources needed

2 — OCIC assigns casenumber and notifies key response stakeholders

3 — OCIC sets up initial coordination call between entity and state/federal partners

4 — OCIC coordinates additional calls if or as needed

5 — OCIC provides key response stakeholders with relevant information

CONTACT INFO TO REPORT:

- **Ohio Cyber Integration Center**
  - Phone: 614-387-1089
  - Email: OCIC@dps.ohio.gov
  - Website: https://homelandsecurity.ohio.gov/ohio-cyber-integration-center
- **Ohio Auditor of State**
  - Phone: 866-FRAUD-OH
  - Reporting Form: ohioauditor.gov/fraud/docs/CybersecurityReportingForm.pdf
  - Email: cyber@ohioauditor.gov
  - Website: www.ohioauditor.gov

INCIDENT INFORMATION REQUIREMENTS

Ohio Cyber Integration Center (DPS)

Organization Details & Contact Info:

- Name, Address, County, Phone, Org Type
- POC: Name, Title, Phone, Email

Security Team Details:

- Device count, PPI, 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?

Auditor of State

- Report as soon as possible, but no later than 30 days upon discovery of an incident

Questions on AOS Report Form include:

- POC: name, title, email, phone
- Government entity type
- Date/time of incident and type of incident
- Was any data compromised?
- Was there a loss of funds? If yes, how much?
- Was ransom demanded? If so, was it paid?
- If ransom was paid, what is the ordinance or resolution approving payment?
- Were policies and procedures in place at the time of the event?

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.

CYBERSECURITY TRAINING: O-PCI

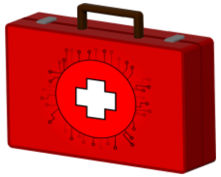
Free Cybersecurity Training for Local Government Entities

- 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
- 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.

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

WATER & WASTEWATER CYBER THREATS

- Water and wastewater systems are some of the most targeted entities for cyber attacks.
- Assistance for water entities through the Ohio Cyber Reserve is available.
  - Free cyber assessments
  - Guidance on mitigation as well as
  - Guidance on cyber program development
- The Ohio Cyber Reserve is actively reaching out to water and wastewater systems to offer support.
- https://ohcr.ohio.gov/

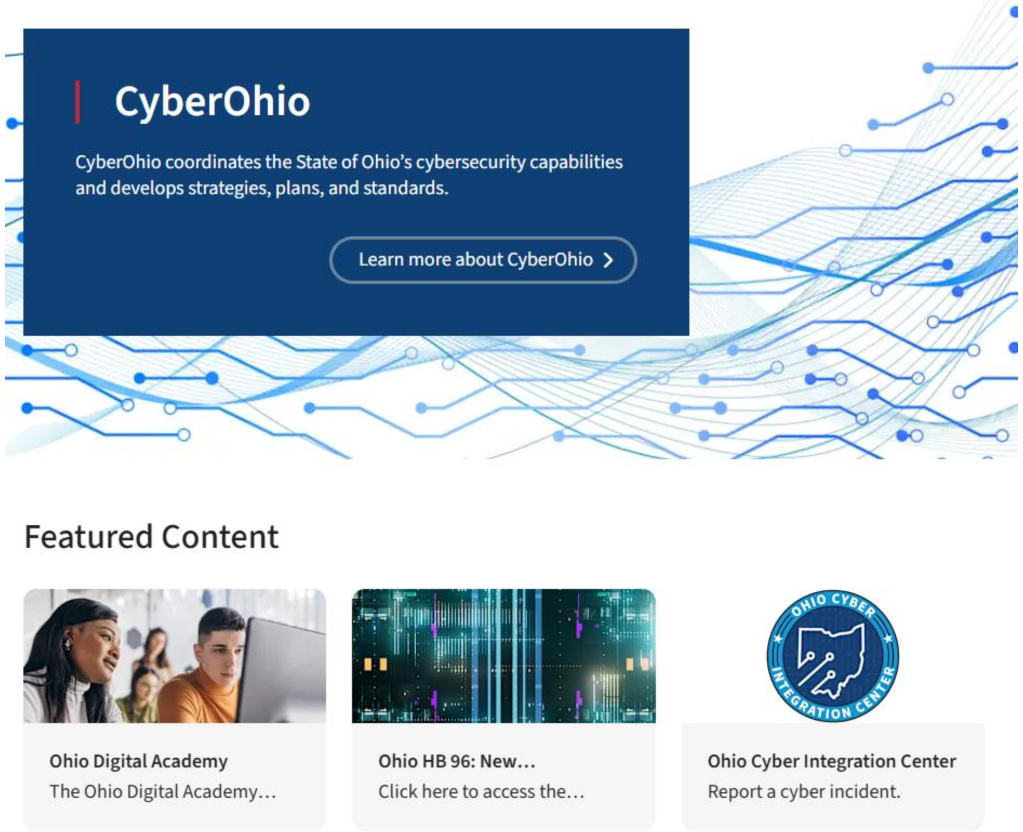
HOW TO USE COLLECTIVE DEFENSE

- Local governments don’t have to do this in isolation. There are ways to reduce duplication and share expertise:
- **Shared Threat Intel:** Participate in MS-ISAC and OCIC alerts—this gives MSPs and local IT staff common early warning.
- **Shared Playbooks:** Use state-provided templates for IR plans, ransomware runbooks, and board resolutions.
- **Regional Partnerships:** Pool with nearby counties/municipalities for joint tabletops, exercises, or staff training—what matters is demonstrating that your program is “reasonable and appropriate,” not that it’s identical everywhere.
- **Using Aggregate Purchasing Pathways**
- **Cooperative Purchasing:**
  - Buy endpoint protection, secure email, backup/DR, or monitoring tools at statewide rates.
  - This lowers cost for small jurisdictions and ensures products meet state baseline standards.
- **Shared MSP Services:** Some councils of governments, county IT departments, or regional planning commissions already contract MSPs and can extend services to member LGEs.
- **Training & Awareness:** Utilize aggregate networks like the O-PCI and CFFAK.

<u>Putting it Together: Division of Roles</u>

- **Board/Council:** Adopt program, approve policies, sign off on annual CSF profile and any ransom decision.
- **Local Executive (Mayor, Administrator, Superintendent, Director):** Designated accountable official.
- **MSP:** Operates day-to-day technical controls, monitoring, patching, backups, and provides reporting.
- **Collective Defense & Cooperative Purchasing:** Supply playbooks, templates, shared intelligence, and discounted procurement.

REGISTER FOR UPCOMING EVENTS AT CYBER.OHIO.GOV



CyberOhio

CyberOhio coordinates the State of Ohio's cybersecurity capabilities and develops strategies, plans, and standards.

Featured Content

Ohio Digital Academy
The Ohio Digital Academy…

Ohio HB 96: New…
Click here to access the…

Ohio Cyber Integration Center
Report a cyber incident.

REGISTER FOR THE CYBEROHIO WEBINAR SERIES – EVERY 2 WEEKS

JOIN THE CYBEROHIO NEWSLETTER

FIND ADDITIONAL HB 96 RESOURCES, VIDEOS, SLIDES

QUESTIONS?

OHIO.ORG