CyberOhio Newsletter **June 2026**

Collective Defense Whitepaper

Collective Defense: Strengthening Cybersecurity Across Ohio

Ohio communities are stronger together. As public entities work to meet the requirements of Ohio's new cybersecurity law, CyberOhio's latest whitepaper highlights how a collective defense approach can help organizations build and strengthen cyber programs collaboratively—reducing costly siloed efforts while expanding access to shared intelligence, resources, and expertise.

By working together, Ohio can improve resilience statewide, support long-term compliance, and better protect the critical services and communities that rely on them.

Read the full whitepaper below.

Whitepaper

CyberOhio Webinar Recap

A Deep Dive with Ohio Persistent Cyber Improvement (O-PCI) from April 29th

The latest CyberOhio webinar offered an in-depth look at the Ohio Persistent Cyber Improvement (O-PCI) program, a free cybersecurity support resource for Ohio's local governments and public entities. Participants learned how O-PCI guides

organizations through a structured, multi-level framework designed to help them build and sustain resilient cybersecurity programs.

Attendees also gained insight into how the program supports compliance with cybersecurity expectations under HB 96 (ORC 9.64) while providing practical, scalable tools that local governments, schools, and public entities can integrate into their existing operations.

O-PCI offers scalable, no-cost tools for local governments, schools, and public entities looking to build a resilient, sustainable cybersecurity program.

To watch the full webinar, click below.

Watch Here

Ohio Cyber Integration Center (OCIC)

OCIC & Ohio Rev. Code § 9.64 (HB 96)

Under Ohio's new cybersecurity law, political subdivisions are required to report cybersecurity incidents to both the Ohio Cyber Integration Center (OCIC) and the Ohio Auditor of State. Cyber incidents must be reported to OCIC as soon as possible, but no later than seven (7) days after discovery, and to the Auditor of State within thirty (30) days. Public entities are strongly encouraged to connect with OCIC and subscribe to their products and notifications to stay informed on the evolving threat landscape.

Report a Cyber Incident to OCIC

Email: OCIC@dps.ohio.gov
Phone: 614-387-1089

Cyber incidents should also be reported to the Ohio Auditor of State in accordance with ORC 9.64.

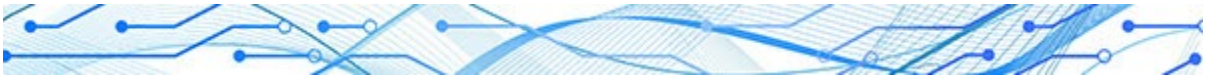
Need Help Building Your Cyber Program?

Access all of the assistance available from CyberOhio and our partner programs.

- Ohio Cyber Integration Center:About OCIC | Ohio Homeland Security
- CyberOhio Cyber Program resources
- Ohio Auditor of State Guidance
    - See the Auditor of State Bulletin 2025-007: Adoption of Cybersecurity Program
    - See the Auditor of State 2026 Compliance Supplement Manual pages 78-81 for more information on what the Auditor of State will be looking for in cybersecurity programs.
- The Ohio Cyber Reserve Ready-Made Security Program
- Ohio Cyber Reserve Assist Missions
- The Ohio Persistent Cyber Improvement Program (O-PCI)
- The Ohio Cyber Range Institute Cyber Frontline First Aid Kit
- Watch CyberOhio Webinars

Best-Practice Frameworks mentioned in Ohio Rev. Code § 9.64:

- NIST Cybersecurity Framework
- Center for Internet Security Critical Security Controls



CyberOhio coordinates and evolves Ohio's cybersecurity practices in partnership with state, local, and critical infrastructure entities.

Cyber.Ohio.gov

CyberOhio@Governor.Ohio.gov