

CYBERSECURITY PROGRAM

Finance and Audit Committee

April 10, 2026

ACTION REQUESTED

Recommend this item to the Executive Committee for placement on the June 2026 Board of Directors agenda:

- Authorize the agency to develop and adopt a cybersecurity program that complies with the requirements of Ohio Revised Code (ORC) § 9.64

PREVIOUS ACTION

No prior action

BACKGROUND

ORC 9.64 – *Political subdivision cybersecurity*

- Effective September 30, 2025
- Requires that the “legislative authority of a political subdivision shall adopt a cybersecurity program that safeguards the political subdivision's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.”

BACKGROUND

Minimum requirements, per ORC 9.64, the cybersecurity program must:

1. Identify and address critical functions and cybersecurity risks
2. Identify the potential impacts of a cybersecurity breach
3. Specify mechanisms to detect potential threats and events
4. Specify procedures for communication, analysis, and containment of incidents
5. Establish procedures for recovery and post-incident prevention
6. Establish cybersecurity training requirements for all employees

BACKGROUND

Other program requirements:

- Prohibits payment of or compliance with a ransomware demand without a Board authorization that specifically states why compliance with the ransom demand is in the best interest of the organization
- Outlines required notification procedures following a cybersecurity or ransomware incident
- Specifies that cybersecurity program-related documents are not subject to disclosure under Ohio Public Records Law

BACKGROUND

Ohio Auditor of State Bulletin 2025-007, *Adoption of Cybersecurity Program*

- Provides further details on the requirements of ORC 9.64
- Establishes deadlines for compliance for different types of political subdivisions
 - County – January 1, 2026
 - City – January 1, 2026
 - All other entity types – July 1, 2026

BACKGROUND

Current state of Information Security at NOACA

- Hardware and applications
- Managed service provider (MSP)
- Disaster Recovery Plan
- Employee training

BACKGROUND

Future State of Information Security at NOACA

- **Engaging consultant On Technology Partners**
 - Assessment of network, hardware, applications, policies, procedures, managed services, and employee training
 - Development of recommendations toward compliance with ORC 9.64 and improving NOACA's information security environment
- **“Tabletop” exercise for information security incident**
 - Convene key agency positions and run-through of procedures

FINANCIAL IMPACTS

- **No direct financial impact from this item**
- **Consulting engagement with On Technology Partners is \$14,000**

NEXT STEPS

- **Commence work on program with Consultant**
 - Anticipated completion within 2 months
- **Refer item to Executive Committee for placement on June 2026 Board meeting agenda**

ACTION

Recommend this item to the Executive Committee for placement on the June 2026 Board of Directors agenda:

- Authorize the Agency to develop and adopt a cybersecurity program that complies with the requirements of Ohio Revised Code (ORC) § 9.64



**Motion
Second
Discussion
Put the Question**





NOACA

Northeast Ohio Areawide Coordinating Agency

NOACA will **strengthen** regional cohesion, **preserve** existing infrastructure, and **build** a sustainable multimodal transportation system to **support** economic development and **enhance** quality of life in Northeast Ohio.