OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

H.B. 475
136th General Assembly

Bill Analysis

Version: As Introduced

Primary Sponsors: Reps. Mohamed and E. White

Daniel DeSantis, Research Analyst

SUMMARY

- Requires the assessment of municipal corporation cybersecurity infrastructure.
- Allows the Cybersecurity Strategic Advisor to certify and contract with private cybersecurity firms.
- Establishes a toll-free secure line to the Ohio Cyber Reserve.

DETAILED ANALYSIS

Background

On April 25, 2022, Governor Mike DeWine signed Executive Order 2022-07D[1] calling for the appointment of a State Cybersecurity Strategic Advisor to serve in the Administration and specified that the advisor must coordinate the state's efforts to protect state's information technology infrastructure and data, develop and exercise a cyber-response plan, establish uniform reporting standards, conduct outreach, and support collaboration for all state agencies, counties, and local governments, academic institutions, and critical infrastructure partners.

The Executive Order further required the Adjutant General's Office, the Department of Administrative Services, and the Department of Public Safety to support the Strategic Advisor, and required Ohio's state cabinet agencies, boards, and commissions to work collaboratively with the Strategic Advisor.

Assessment of cybersecurity infrastructure

The bill requires that the State Cybersecurity Strategic Advisor, with the assistance of the Executive Director of the Emergency Management Agency, and the Chief Information Security

[1] Available on the Governor's Executive Order's website: governor.ohio.gov/media/executive-orders.

Officer, to annually assess the cybersecurity infrastructure of municipal corporations in Ohio and to prepare and submit a report of the assessment to the Governor, Adjutant General, and General Assembly.[2]

Use of private cybersecurity firms

The bill authorizes the State Cybersecurity Strategic Advisor to certify Ohio-based private cybersecurity firms and to contract with certified firms to do the following:

1. Assist the Strategic Advisor in the assessment of municipal corporation cybersecurity infrastructure under the supervision of the Strategic Advisor and in accordance with established assessment standards; and

2. Respond, in coordination with the Ohio Cyber Reserve, to a cybersecurity incident.[3]

The bill expressly authorizes the Ohio Cyber Reserve to coordinate with or deploy a private cybersecurity firm that has been certified by, and is under contract with, the Strategic Advisor to provide specialized support in response to a cyberattack.[4]

Requirements of private cybersecurity contracts

Under the contract or certification, the private cybersecurity firm must do all of the following:

- Register in Ohio and be in good standing with the Secretary of State;
- Provide proof of insurance coverage including cybersecurity liability coverage;
- Employ staff with relevant certifications, at least one of whom must possess certification from at least one of the following: the Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Global Information Assurance Certification (GIAC), Offensive Security Certified Professional (OSCP), Service Organization Control (SOC) 2, or an equivalent;
- Demonstrate proficiency in cybersecurity frameworks such as any of the following: the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), National Institute of Standards and Technology (NIST) 800-53, Center for Internet Security (CIS) Controls, or International Organization for Standardization (ISO) 27001;
- Provide a documented history of providing cybersecurity risk assessments, incident response, or municipal information technology support and have the ability to respond within 48 hours to a municipal corporation incident or request;
- Subject key personnel to background checks or attestations of trustworthiness;

[2] R.C. 5502.282(A) and 125.18(C)(2).

[3] R.C. 5502.282(B).

[4] R.C. 5922.08(C).

- Complete a state-offered orientation or partnership workshop to ensure alignment with government protocols and expectations;
- Adhere to a standardized code of ethics, including transparency;
- Agree to provisions prohibiting the retention of data;
- Agree to provisions prohibiting the disclosure of client data;
- Agree to provisions specifying the requirements of reports that must be provided to the Strategic Advisor by the private cybersecurity firm.[5]

Cybersecurity emergency reporting telephone line

The bill requires the Adjutant General to establish a toll-free telephone number that may be used by a state, county, or local government entity to report a cyberattack and to request immediate support by the Ohio Cyber Reserve. The telephone number must be staffed by live personnel 24 hours a day at its answering point. The telephone line must be protected by security measures to prevent eavesdropping or interception.

The bill requires that the Adjutant General establish adequate rules and procedures to facilitate an immediate response to a request for support by a state, county, or local government entity, including the procedure for contacting the Governor's office to request that the Governor order individuals or units of the Ohio Cyber Reserve to state active duty, and requires that the Reserve, when so ordered, respond within 48 hours.[6]

The bill also requires that a countywide emergency management agency, a regional authority for emergency management, or a program for emergency management within a political subdivision incorporate utilization of the secure toll-free cyber attack telephone line into the entity's emergency plan.[7]

HISTORY

Action	Date
Introduced	09-29-25

ANHB0475IN-136/ts

[5] R.C. 5502.282(B).

[6] R.C. 5922.08(B) and 5922.09.

[7] R.C. 5502.283.