OHIO LEGISLATIVE SERVICE COMMISSION

www.lsc.ohio.gov

Office of Research and Drafting

Legislative Budget Office

S.B. 203
136th General Assembly

Fiscal Note & Local Impact Statement

Click here for S.B. 203's Bill Analysis

Version: As Introduced

Primary Sponsor: Sen. Schaffer

Local Impact Statement Procedure Required: Yes

Jared Cape, Budget Analyst

Highlights

- Political subdivisions will incur additional costs to adopt a cybersecurity program that meets certain requirements. The cost to each political subdivision will vary based on their existing cybersecurity program, any short-term improvements needed to comply with the new requirements, and any recurring costs to meet higher security standards.

Detailed Analysis

Cybersecurity program

Under the bill, political subdivisions will incur additional costs to adopt a cybersecurity program that meets certain requirements, which are described in the bill analysis. The cost to each political subdivision will vary based on their existing cybersecurity program, any short-term improvements needed to comply with the new requirements, and any recurring costs to meet higher security standards. These additional costs could include new personnel, training, hardware, software, and consulting services.

Political subdivisions may choose to collaborate with CyberOhio, located in the Governor's Office, to improve their cybersecurity. Employee training costs could be minimized by attending the free Ohio Persistent Cyber Improvement (O-PCI) training program, which is developed and delivered by the Ohio Cyber Range Institute (OCRI) and funded through the U.S. Cybersecurity and Infrastructure Security Agency and the state of Ohio. For more information on the O-PCI program, see the OCRI website: ohiocyberrangeinstitute.org/government-training.

Ransomware and cybersecurity incidents

Under the bill, political subdivisions would incur minimal additional costs for staff time when responding to a ransomware or cybersecurity incident. Specifically, the bill prohibits a political subdivision experiencing a ransomware incident from paying or otherwise complying

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. Additionally, the bill requires the legislative authority of a political subdivision, following each cybersecurity incident or ransomware incident, to notify both (1) the Executive Director of the Division of Homeland Security within the Department of Public Safety, and (2) the Auditor of State.

Public records exemption

The bill specifies that any records, documents, or reports related to the cybersecurity program and framework, and the reports of a cybersecurity incident or ransomware incident, are not public records, and are not subject to the disclosure requirements of the Ohio Public Records Law. The state and political subdivisions likely would not incur any new costs to adhere to exemptions under the Ohio Public Records Law.

FNSB0203IN-136/lb