OHIO AUDITOR OF STATE
KEITH FABER

Senate Financial Institutions, Insurance and Technology Committee

Alexis Davis
Senate Bill 203
June 17, 2025

Chair Wilson, Vice-Chair Lang, Ranking Member Craig and members of the Senate Financial Institutions, Insurance and Technology Committee, my name is Alexis Davis and I am Deputy Director of Policy and Legislative Affairs for Auditor of State Keith Faber. Thank you for the opportunity to testify in support of Senate Bill 203.

This legislation was crafted in response to a question – is it proper public purpose for a political subdivision to pay a ransomware demand using taxpayer dollars? The resulting bill, which included repeated conversations with local government associations, has three key components that I will briefly discuss.

First, Senate Bill 203 bans political subdivisions from paying or otherwise complying with a ransomware demand. That said, this provision has significantly changed from the original concept of a complete ban after concerns were raised by interested parties. For instance, what if a ransom demand is small enough that payment is the best route forward? Senate Bill 203 now includes a compromise which allows the legislative authority to pay a cybersecurity ransom if the local authority adopts a resolution explaining why payment or compliance is in the public interest. The intent of this provision is to give local elected officials the ability to pay a ransom while also ensuring that the public is informed about such a decision.

It is worth noting that we found at least twelve states that have addressed ransomware in law, with Florida and North Carolina being two specific examples. Those two states stood out because they passed a total ban on ransomware payments, which is something that this legislation does not do.

Second, Senate Bill 203 requires each political subdivision to adopt a cybersecurity program that is appropriate for their needs. As cyber-attacks and cybersecurity incidents are inevitable, local governments need to take preventative measures to keep their systems and residents' information safe. Having a policy or program in place is a commonsense step that will allow a local government who falls victim to a cyber-attack to respond quickly, effectively, and with minimal loss.

The bill provides a list of six items that **may** be included in a cybersecurity program:

1. Identify and address the critical functions and cybersecurity risks of the political subdivision
2. Identify the potential impacts of a cybersecurity breach
3. Specify mechanisms to detect potential threats and cybersecurity events
4. Specify procedures for the political subdivision to establish communication channels, analyze incidents, and take actions to contain cybersecurity incidents
5. Establish procedures for the repair of infrastructure impacted by a cybersecurity incident, and the maintenance of security after the incident
6. Establish cybersecurity training requirements for all employees of the political subdivision; the frequency, duration, and detail of which shall correspond to the duties of each employee. This also clarifies that annual cybersecurity training provided by the state, and training provided for local governments by the Ohio persistent cyber initiative program, satisfy this requirement.

The Auditor of State's (AOS) office recognizes that a one-size-fits all policy is not an appropriate approach for the thousands of local governments across the state of Ohio. This is why Senate Bill 203 allows local officials to design a program that best fits their needs; AOS staff will simply audit to that policy.

Third, this legislation requires that local governments who fall victim to a cyber-attack must notify the Ohio Department of Public Safety (DPS) and the Auditor of

State's office within a set period. Incidents must be reported to DPS within seven days and to the Auditor of State within thirty days.

The reason for the reporting requirements and their differing time periods is specific to each agency and their role in the recovery process. DPS is the far more crucial call in the immediate aftermath of a cyberattack. The Department has cybersecurity resources that can be of immediate assistance, and we believe that the state should do everything it can to help local governments who fall victim to these attacks. This provision is an effort to connect local governments to those resources so that relief can be obtained as quickly as possible.

Additionally, our agency needs to be aware of cybersecurity losses when conducting an audit. That is why Senate Bill 203 asks that AOS be notified within a month of an incident's occurrence. This provision is necessary because current law does not require local governments to report a theft to AOS and we often find out about such incidents either much later during an audit, or more concerningly, in the news media.

Lastly, it is important to note that Senate Bill 203 exempts records, documents, or reports related to a cybersecurity program as well as reports of cybersecurity incidents or ransomware to DPS and AOS from public records law. The exemption also includes procurement of cybersecurity-related software, hardware, goods, and services. This exemption is included to protect the local governments from public records requests that could be a cybersecurity risk.

Over the past year our office has been made aware of several other cyber incidents such as business email compromises, vendor redirect schemes, and fraudulent checks. Since January 2023, there have been at least 221 occurrences with nearly $11.2 million in losses reported. Of this amount, approximately $3.4 million was recovered or stopped, leaving a loss of $7.8 million in public dollars.

These numbers are based on reports made to our Special Investigations Unit; however, the actual losses could be higher as this data only covers reported incidents. As I mentioned earlier, AOS may learn of an incident during an audit. However, it is important to emphasize that discovering an incident would only happen if a payment is material to the audit. For an incident to be material, the payment would need to be large enough that it is individually significant enough to

test, or if it appears in a year-to-year comparison. If such a payment is not large enough to stand out, we are reliant upon the client to share that information with us. It is also important to note that AOS audits in arrears and a cybersecurity incident may have occurred, and the money already been paid, by the time we discover the issue.

In conclusion, the Auditor of State is striving to educate local elected officials on how to best prevent cybersecurity breaches. Senate Bill 203 is an important step in this process as it will ensure that cybersecurity programs are in place and that there is required reporting to the appropriate agencies. That said, AOS recognizes the importance of local control, and we are happy to support a version of this legislation which protects local authorities' ability to have the final say on how this policy is implemented.

Thank you again for the opportunity to testify and thank you to Senator Schaffer for introducing this legislation.

I am happy to take any questions from the committee.