State and Local Cybersecurity Changes

HB 7055 and HB 7057

2022 Legislative Session

New Requirements for Local Governments

- ***Training:*** Annual training required for all local government employees with access to the government's network. An advanced training will be required for employees with access to highly sensitive information. All employees must participate in the training within 30 days of employment and annually thereafter. The Florida Digital Service is responsible for establishing and providing the training but may contract with another entity to execute the program.
- ***Standards:*** Local governments will now be required to adopt cybersecurity standards that safeguard data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. The bill specifies that those standards must be consistent with NIST generally acceptable best practices (National Institute of Standards and Technology).
    - Timeline: Counties with less than 75,000 in population and cities with less than 25,000 in population must be compliant by January 1, 2025.
    - Counties with a population of 75,000 or more and cities with a population of 25,000 or more must be compliant by January 1, 2024.
- ***Reporting:*** Local governments must provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of FDLE, and the sheriff who has jurisdiction over the local government. The bill points to levels of severity established by the National Cyber Incident Plan of the U.S. Department of Homeland Security. Incidents of severity levels 3, 4, and 5 must be reported. Reporting of incidents levels 1 and 2 are optional.
    - Timeline: Severe incidents must be reported as soon as possible but no later than 48 hours after discovery and no later than 12 hours after discovery of a ransomware incident.
    - An after-action report must be submitted to the Florida Digital Service within 1 week of remediation of a cybersecurity incident or ransomware incident.

Additional Policy Changes

- Local governments are prohibited from paying or otherwise complying with a ransom demand.

- Expands the role of the Florida Cybersecurity Advisory Council to advise local governments on cybersecurity threats, trends, and best practices.

Cybersecurity Public Record Exemptions Expanded to Include Local Governments

The bill makes confidential and exempt from public record requirements:

- Cybersecurity insurance coverage limits and deductible self-insurance amounts
- Information related to a local government's critical infrastructure
- Cybersecurity incident information
- Network schematics, hardware and software configurations, or encryption information
- Response practices for cybersecurity incidents if disclosure of such information would facilitate unauthorized access to the network

*The bill also provides that any portion of a meeting that might reveal information exempt under this act are exempt from public meeting requirements.

Funding Opportunities

- ***State:*** The Legislature allocated $30 million to create a local government cybersecurity grant program for fiscal year 2022-2023. The Florida Digital Service which is housed in the Department of Management Services is responsible for creating and executing the grant program. Please visit the funding page for more information.