FLC

FLORIDA LEAGUE OF CITIES

Understanding the Local Government Cybersecurity Act

Tara Taggart
Palm Beach County League of Cities
October 26, 2022

State Cybersecurity Changes

- 2020 – HB 1391 created the Florida Digital Service
- 2021 – HB 1297 designated FDS the lead entity on cybersecurity for the state. Tasked the office with creating innovative solutions that securely modernize state government.
- 2022 – HB 7055 enacted the Local Government Cybersecurity Act & HB 7057 enacted Exempting Public Records for Local Agencies

New Cybersecurity Requirements for Local Governments

Training

- Annual training required for all local government employees with access to the government's network
- Advanced training required for employees with access to "highly sensitive information"
- Completed within 30 days of employment and annually thereafter
- $30 million appropriated to USF's Florida Center for Cybersecurity – "Cyber Florida"
  - $7 million to perform a comprehensive risk assessment of critical infrastructure

Standards

Local governments will be required to adopt cybersecurity standards consistent with NIST (National Institute of Standards and Technology) principles.

- Standards must be “appropriate for the size of the organization”
- Standards must safeguard data, IT resources and infrastructure, and ensure the availability, integrity, and confidentiality of data
- Cities < 25,000 in population must comply by January 1, 2025
- Cities > 25,000 in population must comply by January 1, 2024

Reporting

Local governments must provide notification of severe cybersecurity incidents and ransomware attacks to the Cybersecurity Operations Center, Cybercrime Office of FDLE, and the sheriff who has jurisdiction over the local government.

- Levels of incident severity are established by the National Cyber Incident Plan of the U.S. Dept. of Homeland Security
  - Incident levels 3, 4 and 5 must be reported
  - Reporting of incident levels 1 and 2 is optional

National Cyber Incident Response Plan

	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

	Observed Actions	Intended Consequence[1]
	Effect	Cause physical consequence
		Damage computer and networking hardware
	Presence	Corrupt or destroy data
		Deny availability to a key system or service
	Engagement	Steal sensitive information
		Commit a financial crime
	Preparation	Nuisance DoS or defacement

Additional Policy Changes

Timeline for Incident Response

- Severe incidents: as soon as possible but no later than 48 hours after discovery
- Ransomware attacks within 12 hours of discovery
- After-action report must be submitted to FDS within 1 week of remediation of an incident.

Policy Changes

- Paying ransomware or "otherwise complying" with a ransom demand is now prohibited
- Role of the Florida Cybersecurity Advisory Council expanded to advise local governments

Public Records Exemptions – HB 7057

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 also exempt from public meeting requirements.

$$ Funding $$

State

- The legislature allocated $30 million to launch a competitive grant program to fund cybersecurity initiatives in cities and counties
- $5.6 million to FDS to administer federal grant funds

Federal

The Department of Homeland Security has allocated $1 billion for a State and Local Cybersecurity Grant Program over five years.

- Florida's first tranche of funding ~$5.6 million
- 80% must go to local entities

Questions?

Contact:
Tara Taggart
Ttaggart@flcities.com
850-701-3603