John A. Carey
Inspector General

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

TIPS AND TRENDS #2022-0003

JULY 2022

Inspector General
Accredited

LOCAL GOVERNMENT CYBERSECURITY ACT

Are you ready for the Local Government Cybersecurity Act?

On June 24, 2022, the Governor signed Florida House Bill 7055, "Cybersecurity," into law (Chapter 2022-220, Laws of Florida). Effective July 1, 2022, the bill:

- Created section 282.3185, Florida Statutes (F.S.), known as the "Local Government Cybersecurity Act," and section 282.3186, F.S.
- Updated the definition of "incident" and added a definition of "ransomware" in section 282.0041, F.S., to include counties and municipalities;
- Updated section 282.318, F.S., to define the level of severity of and reporting process for a ransomware or cybersecurity incident; and
- Created section 815.062, F.S., to establish penalties and fines for certain ransomware offenses against a government entity.

Prior to the passage of Florida House Bill 7055, only the heads of state agencies were required to meet certain requirements to enhance the cybersecurity of state agencies. The updated law requires counties and municipalities to:

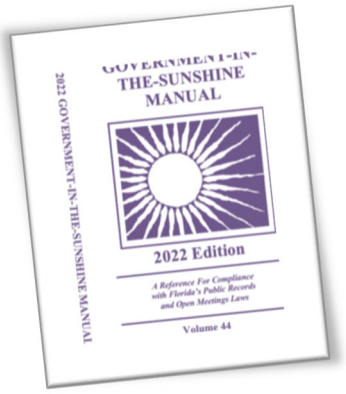
- Provide basic cybersecurity training[1] to all employees with access to the local government's network within 30 days of employment and annually thereafter.
- Provide advanced cybersecurity training[1] to technology professionals and employees with access to highly sensitive information within 30 days of employment and annually thereafter.

[1] Cybersecurity training will be developed by the Florida Digital Service, an organization created by the State of Florida in 2020 to leverage data and deploy technology to better serve Floridians.

PO Box 16568, West Palm Beach, FL 33416-6568
Email: inspector@pbcgov.org Website: http://www.pbcgov.com/oig/
Office: (561) 233-2350 Hotline: (877) 283-7068 Fax: (561) 233-2370

- Adopt cybersecurity standards to safeguard data, Information Technology (IT), and IT resources to ensure availability, confidentiality, and integrity.[2]
- Notify the Cybersecurity Operations Center, Cybercrime Office of the Florida Department of Law Enforcement (www.fdle.state.fl.us), and the local sheriff (www.pbso.org) of a cybersecurity or ransomware incident.[3]
- Provide the Florida Digital Service (www.digital.fl.gov) with an after-action report summarizing a cybersecurity or ransomware incident, the incident's resolution, and any insights gained as a result of the incident.
- Cease making ransom payments or otherwise complying with a ransom demand.

Corresponding Florida House Bill 7057, "Public Records and Meetings/Cybersecurity," was also signed into law (Chapter 2022-221, Laws of Florida) on June 24, 2022. The bill, which became effective July 1, 2022, created section 119.0725, F.S., defines terms related to cybersecurity information and makes confidential and exempt from public disclosure certain local government cybersecurity-related information, including:[4]



- Ransomware insurance coverage,
- Critical infrastructure information,
- Network schematics,
- Hardware and software configurations,
- Encryption information,
- Cybersecurity incident information, and
- The recording and transcript of portions of a meeting[5] that would reveal the above information.

Suggestions

We recommend that the County and municipalities review the requirements outlined in the Local Government Cybersecurity Act, sections 282.3185 and 282.3186, F.S., and corresponding update to public records exemptions in section 119.0725, F.S., and establish or update policies and procedures accordingly.

For further information, including Cybersecurity Resources, please visit the State of Florida's Cybersecurity Advisory Council website at https://www.dms.myflorida.com/other_programs/cybersecurity_advisory_council.

[2] The standards must be adopted by January 1, 2024 for counties with a population of 75,000 or more and municipalities with a population of 25,000 or more. January 1, 2025 is the deadline for County's with populations of less than 75,000 and municipalities with a population of less than 25,000.

[3] All ransomware incidents and any cybersecurity incidents determined by the local government to be of severity level 3, 4, or 5 as provided in section 282.318(3)(c), F.S., must be reported as soon as possible, but no later than 48 hours after discovery of the cybersecurity incident and no later than 12 hours after discovery of the ransomware incident.

[4] The public records exemptions apply to information held by an agency before, on, or after July 1, 2022.

[5] Any portion of a meeting that would reveal information made confidential and exempt under section 119.0725(2), F.S. is exempt from public meetings requirements in s. 286.011 and s. 24(b), Art. I of the State Constitution. An exempt portion of a meeting may not be off the record and must be recorded and transcribed.