Cybersecurity Legislative Update

FACT Risk Management Conference

Jeff Scala
FAC Associate Director of Public Policy

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

2021 Legislation

- HB 1297
  - Florida Digital Service assigned as lead state entity
    - Assess state agency cybersecurity risks
    - Determine appropriate security measures
  - Created/amended new cybersecurity duties and responsibilities previously assigned to DMS
  - s. 282.0051, Florida Statutes
    - Florida Digital Service; powers, duties, & functions

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Digital Service

- Establish standards and processes consistent with best practices for IT security, including the NIST cybersecurity framework.
- Adopt rules to mitigate risk, support a security governance framework, and safeguard state agency digital assets, data, information, and IT resources to ensure availability, confidentiality, and integrity.
- Designate a chief information security officer (CISO)
- Develop/annually update a statewide cybersecurity plan

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Digital Service

- Develop a cybersecurity governance framework to use when procuring IT commodities and services
- Track agencies' implementation remediation plans.
- Provide cybersecurity training to all state agency technology professionals
- Operate and maintain a Cybersecurity Operations Center led by the CISO
  - clearinghouse for threat information
  - coordinated with FDLE for incidents response
- Lead an Emergency Support Function under the state comprehensive emergency management plan.
  - ESF-20

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

2021 Legislation

- Created the Florida Cybersecurity Advisory Council within DMS.
  - Assist state agencies in protecting IT resources from cyber threats and incidents. The council will
  - Assist FDS in implementing best cybersecurity practices, taking into consideration the final recommendations of the Florida Cybersecurity Task Force.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

2022 Legislation

- Two bills—FAC Supported & **PASSED**
  - HB 7055—Cybersecurity Reporting, Standards, and Training for Local Governments
    - s. 282.3185, Florida Statutes
  - HB 7057—Public Records Exemption for Critical Infrastructure and Cybersecurity Information
    - s. 119.0725, Florida Statutes

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

2022 Legislation

- HB 7057—Public Records & Meetings/Cybersecurity
  - Representative Giallombardo and others
  - General public record exemption or public meeting exemption related to state or local government cybersecurity information

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7057—Pub. Rec. Exemptions

- Exemption includes:
  - Coverage limits and deductible or self-insurance amounts of insurance or other risk mitigation coverages acquired for the protection of IT systems, operational technology systems, or data of an agency.
  - Information relating to critical infrastructure.
  - Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents.
  - Cybersecurity incident information reported pursuant to Sections 282.318 or 282.3185, F.S.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7057—Pub. Rec. Exemptions

- Exemption includes:
  - The bill also creates a public meeting exemption for any portion of a meeting that would reveal the confidential and exempt information; however, any portion of an exempt meeting must be recorded and transcribed. The recording and transcript are confidential and exempt from public record requirements.

  - The bill provides for release of the confidential and exempt information in certain instances and authorizes agencies to report information about cybersecurity incidents in an aggregate format.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7057—Pub. Rec. Exemptions

- Public Necessity statement:
  - Release of such information could place an agency at greater risk of breaches, cybersecurity incidents, and ransomware attacks.
  - If information related to the coverage limits and deductible or self-insurance amounts of cybersecurity insurance were disclosed, it could give cybercriminals an understanding of the monetary sum an agency can afford or may be willing to pay as a result of a ransomware attack at the expense of the taxpayer.
  - Vital component of public safety and could aid in the planning of, training for, and execution of cyberattacks, increasing the ability of bad actors to harm individuals in this state.
  - Could be used by criminals to identify vulnerabilities that existed in cybersecurity systems or protocols

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7057—Pub. Rec. Exemptions

- Public Necessity statement:
  - Network schematics, hardware and software configurations, or encryption information or information that identifies detection, investigation, or response practices for suspected or confirmed cybersecurity incidents, including suspected or confirmed breaches, would facilitate unauthorized access to or the unauthorized modification, disclosure, or destruction of data or information, whether physical or virtual, or information technology resources.
  - Such information also includes proprietary information about the security of an agency's system.
  - The disclosure of such information could compromise the integrity of an agency's data, information, or information technology resources, which would significantly impair the administration of vital governmental programs. Therefore, this information should be made confidential and exempt in order to protect the agency's data, information, and information technology resources.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

2022 Legislation

- HB 7055—Cybersecurity
  - Representative Giallombardo and Stevenson
  - Reporting, Standards, and Training for State & Local Governments
    - Compliance intended to be uniform across state
  - Mandate
    - Rare *FUNDED* mandate
    - Grants to local governments (more on that later)

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Ransomware Incident Definition:
  - a malicious cybersecurity incident in which a person or entity introduces software that gains unauthorized access to or encrypts, modifies, or otherwise renders unavailable a state agency's, county's, or municipality's data and thereafter the person or entity demands a ransom to prevent the publication of the data, restore access to the data, or otherwise remediate the impact of the software.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Ransomware Payment Prohibition
  - State agencies, local governments experiencing a ransomware incident may not pay or otherwise comply with a ransom demand

- Ransomware offense
  - Establishes “offenses against governmental entities” felony of the first degree

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Incident/Ransomware Reporting Summary info
  - (1) summary of the facts
  - (2) date of most recent back up, other back up info
  - (3) types of data compromised
  - (4) estimated fiscal impact
  - (5) if ransom, details of ransom

- Local Governments must also provide:
  - (6) A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the sheriff who has jurisdiction over the local government

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Notification process
  - Ransomware/incidents of levels 3, 4, or 5 reported to Cybersecurity Operations center, FDLE cybercrime office asap but not later than 48 others after incident; 12 hours after ransomware
    - Cybersecurity Operations office will notify FL House/Senate
    - Additional reporting for levels 1 and 2
    - Provide for additional consolidated report

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Cyber Incident Tier Severity

- Defined by the National Cyber Incident Response Plan of the US Department of Homeland Security as follows:
  - Level 5—emergency-level incident
  - Level 4—severe-level incident
  - Level 3—high-level incident
  - Level 2—medium-level incident
  - Level 1—low-level incident

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

Description	Disaster Level	Cyber Incident Severity	Description
Due to its severity, size, location, actual or potential impact on public health, welfare, and infrastructure it requires an extreme amount of federal assistance for response and recovery efforts for which the capabilities to support do not exist at any level of government.	Level 1	Level 5 *Emergency*	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government security, or the lives of US citizens.
Requires elevated coordination among federal and SLTT governments due to moderate levels and breadth of damage. Significant involvement of FEMA and other federal agencies.	Level 2	Level 4 *Severe*	Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
		Level 3 *High*	Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Requires coordination among federal and SLTT governments due to minor to average levels and breadth of damage. Typically, this is primarily a recovery effort with minimal response requirements.	Level 3	Level 2 *Medium*	May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
		Level 1 *Low*	Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT

Risk Management

HB 7055—Cybersecurity

- Local Government Incident Notification
  - A local government shall provide notification of a cybersecurity incident or ransomware incident to the Cybersecurity Operations Center, Cybercrime Office of the Department of Law Enforcement, and sheriff

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- After Action Reports
  - FL_DS will develop and publish process for after-action reports for cybersecurity or ransomware incidents by 12/1/22
  - A local government must submit to the Florida Digital Service, within 1 week after the remediation of a cybersecurity incident or ransomware incident, an after action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Annual Training Requirements
  - Annual cyber training for all employees with access to highly sensitive information
  - Training must include the identification of each cybersecurity incident severity level

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Cybersecurity Training
  - FL_DS shall develop a basic cybersecurity training curriculum for local government employees.
  - All local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Cybersecurity Training
  - Develop an advanced cybersecurity training curriculum for local governments which is consistent with the cybersecurity training required under s. 282.318(3)(g) Severity levels.
  - All local government technology professionals and employees with access to highly sensitive information must complete the advanced cybersecurity training within 30 days after commencing employment and annually thereafter.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Cybersecurity Standards
  - Each local government shall adopt cybersecurity standards that safeguard its data, information technology, and information technology resources to ensure availability, confidentiality, and integrity.
  - The cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity Standards

- DMS adopted Rules in August
  - 60GG-2.001 through 60GG-2.006
- Modeled after the NIST Standards
- Applies to state agencies
  - Local governments must adopt standards
  - Roadmap for standards

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

HB 7055—Cybersecurity

- Local Cybersecurity Standards
  - Each county with a population of 75,000 or more must adopt the cybersecurity standards required by this subsection by **January 1, 2024.**
  - Each county with a population of less than 75,000 must adopt the cybersecurity standards required by this subsection by **January 1, 2025.**
  - Local governments must notify FL_DS when in compliance

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

State Cybersecurity Grants

- FY 2022-23 budget allocated $30 million to create a local government cybersecurity technical assistance grants
  - DMS/Florida Digital Service is responsible for creating and executing the grant program.
  - FL_DS will develop the criteria and process for awarding assistance funds

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

State Cybersecurity Grants

- FY 2022-23 budget allocated $30 million to conduct cybersecurity training for state and local government executive, managerial, technical, and general staff
  - Developed by the Florida Center for Cybersecurity at the University of South Florida

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Federal Cybersecurity Grants

- State and Local Cybersecurity Grant Program (SLCGP)
  - funded by the Bipartisan Infrastructure Law (BIL)
  - Program through U.S. DHS and FEMA
  - Recently announced NOFO on September 16

- The SLGCP provides a total of $1 billion in funding over the next four years
  - $185 million available for Fiscal Year (FY) 2022
  - Support state and local efforts to address cyber risks to their information systems
  - $5.9 million for Florida in FY 22
  - 80% of funds must be sub-allocated to local governments and rural areas

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Federal Cybersecurity Grants

- Applicants are required to demonstrate how their efforts will achieve the following SLCGP program objectives:
  - Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations
  - Understand their current cybersecurity posture and areas for improvement based on continuous testing, evaluation, and structured assessments
  - Implement security protections commensurate with risk
  - Ensure organization personnel are appropriately trained in cybersecurity, commensurate with responsibility

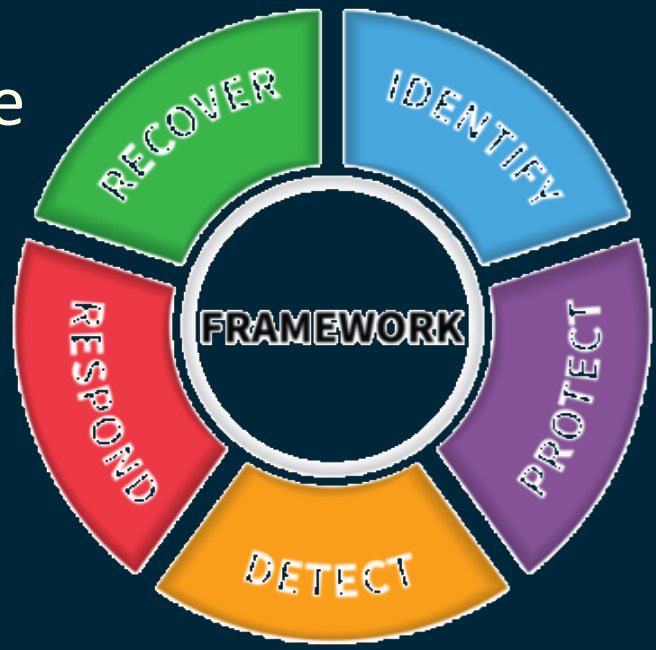
FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

NIST Framework Attributes

Principles of Current and Future Versions of the Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors and uses
- Risk-based
- Based on international standards
- Living document
- Guided by many perspectives – private sector, academia, public sector



FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT
Risk Management

Florida Cybersecurity/NIST Standards

- Identify
  - Determining what your county has, what is most important, and what are the biggest threats to what you have
  - Identify your county's assets
    - Hardware, software, network infrastructure
  - Policies, vulnerabilities, threats, legal and regulatory requirements

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT
Risk Management

Florida Cybersecurity/NIST Standards

- Identify
  - Asset Management
  - Business Environment
  - Governance
  - Risk Assessment
  - Risk Management Strategy
  - Supply Chain Risk Management

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Protect
  - All the technology, people, and processes that protect the county's assets
  - Safeguards (technology, policies, and training) that are put in place to limit or contain a potential cyber event

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Protect
  - Identity Management, Authentication, and Access Control
  - Awareness and Training
  - Data Security
  - Information Protection Processes and Procedures
  - Maintenance
  - Protective Technology

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Detect
  - Anomalies and Events
  - Security Continuous Monitoring
  - Detection Processes

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Respond
  - Making sure all leaders, technical staff, and employees know what to do if someone accesses the county's assets, then they do it.
  - A plan and set of activities to take action on a detected cyber event to contain and mitigate the potential impact

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Respond
  - Response Planning
  - Communications
  - Analysis
  - Mitigation
  - Improvements

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Recover
  - Activities to get the county's assets back, protected, and then get back to normal operations
  - Activities to restore all functions, capabilities, and services impacted by the cybersecurity event

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Cybersecurity/NIST Standards

- Recover
  - Recovery Planning
  - Improvements
  - Communications

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Cybersecurity Best Practices

- Multi-Factor Authentication (MFA) user accounts
- End Point Security and Host Based Firewalls
- Regularly Update your Software
- Regular and Robust Back up Programs
- Limiting Administrative Accounts
- Lock Devices
- Zero-Trust Security
- Strong Password Policies
- Phishing Training
- Least Privilege Access

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

CYBER SECURE FLORIDA

Welcome to the CyberSecureFlorida initiative, a first-of-its-kind effort to assess the cybersecurity strengths and weaknesses of Florida's collective critical infrastructure. The information gathered through this effort will be critical to helping Florida's elected leaders determine how best to allocate resources and enact appropriate legislation to create a more secure Sunshine State!

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT

Risk Management

Cyber Secure Florida

- Led by Cyber Florida in consultation with the Florida Cybersecurity Advisory Council

- Establish a baseline of current critical infrastructure cybersecurity protections
- Provide actionable solutions to increase the state's preparedness and resilience to cyberattacks
- Reduce the vulnerabilities of critical systems, assets, and networks
- Increase resiliency and security to protect the people, property, and prosperity of Florida
- CyberSecureFlorida is open to all public- and private-sector critical infrastructure entities
- https://cyberflorida.org/cybersecureflorida/

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Cybersecurity Legislative Update

Jeff Scala
FAC Associate Director of Public Policy

jscala@fl-counties.com
(727) 637-4081

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Hurricane Ian Timeline and Updates

- The State Emergency Operations Center (EOC) activated to a Level 2 partial activation on September 24 and Level 1 full activation on September 25
- On September 23, the governor issued Executive Order 22-218 (2022-09-23) and EO 22-219 (2022-09-24) declaring a state of emergency for all sixty-seven counties. (https://www.floridadisaster.org/info/)
- On September 28, Hurricane Ian made landfall on Cayo Costa, on the southwestern coast of Florida, as a strong Category 4 hurricane
- A storm surge of 12 to 18 feet above ground level was reported along the southwestern Florida coast, and the city of Fort Myers itself was hit particularly hard with a 7.26 foot surge—a record high.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

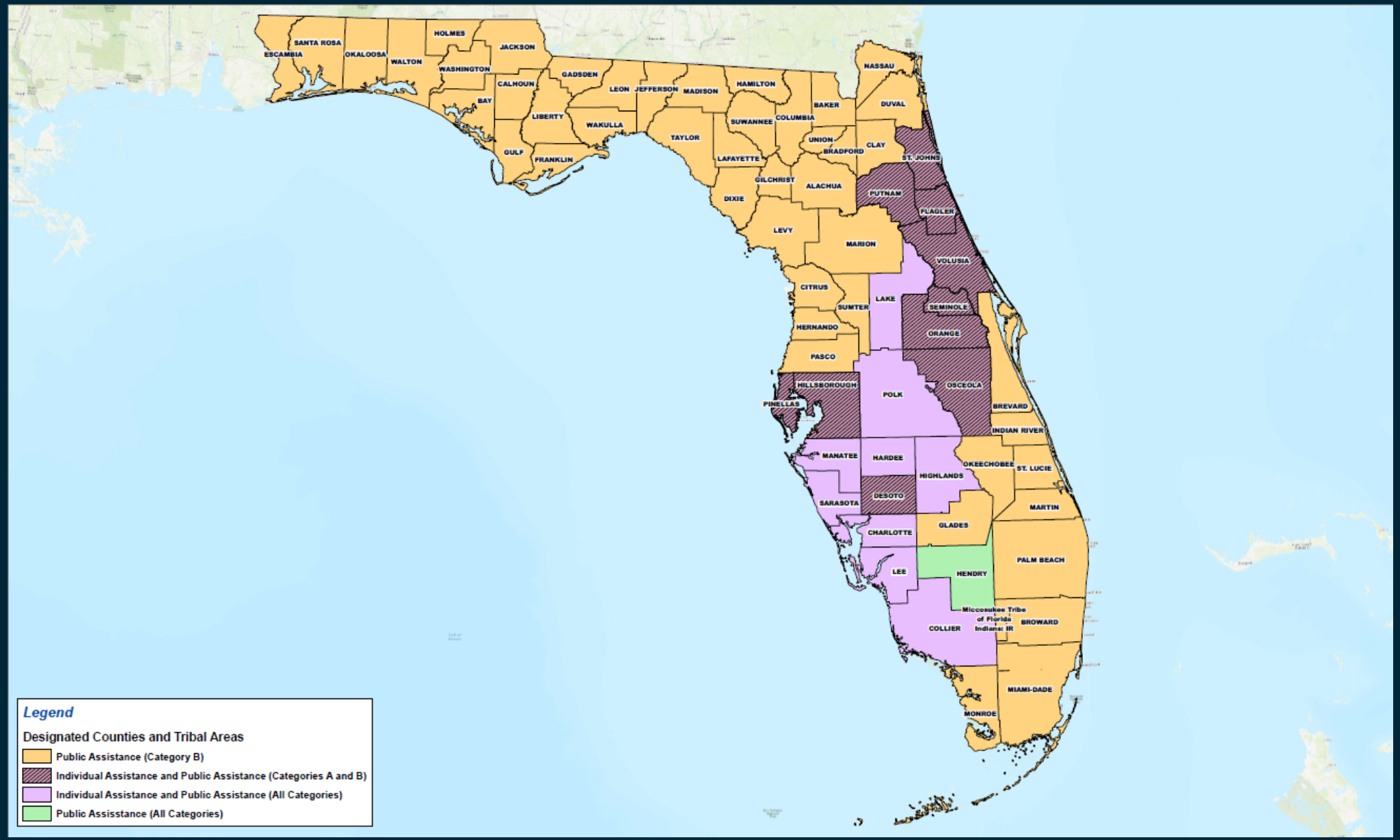
Hurricane Ian Timeline and Updates

- Ian was downgraded to a tropical storm on Sept. 29 as it tracked inland, crossing over the Florida peninsula. However, as it did so, extreme rainfall became particularly destructive, producing 1-in-1000-year amounts in some places.
- The storm knocked out power to more than four million customers in Florida
- FEMA issued federal disaster declaration, DR-4673-FL, on September 29th
- Rescue crews have visited about 45,000 homes and businesses in affected areas
- Individuals, communities, and businesses may apply for assistance at https://www.disasterassistance.gov/

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management

Florida Disaster Declaration as of 10/4/22



FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT

Risk Management

FEMA Assistance: Eligible Counties

- Individual Assistance: Charlotte, Collier, DeSoto, Flagler, Hardee, Highlands, Hillsborough, Lake, Lee, Manatee, Orange, Osceola, Pinellas, Polk, Putnam, Sarasota, Seminole, St. Johns and Volusia Counties.

- Public Assistance Category A (Debris): Charlotte, Collier, DeSoto, Flagler, Hardee, Hendry, Highlands, Hillsborough, Lake, Lee, Manatee, Orange, Osceola, Pinellas, Polk, Putnam, Sarasota, Seminole, St. Johns, and Volusia.

- Public Assistance Category B (Emergency Protective Measures, including direct federal assistance): All 67 Counties and the Miccosukee Tribe of Indians of Florida and the Seminole Tribe of Florida for a period of 30 days from the start of the incident period.

- Public Assistance Permanent Work (Categories C-G): Charlotte, Collier, Hardee, Hendry, Highlands, Lake, Lee, Manatee, Polk and Sarasota Counties.

FACT
FLORIDA ASSOCIATION OF COUNTIES TRUST

2022 FACT Risk Management