Summer 2022

Preferred News

Special Edition

Member Recognition Awards & Return of Member Education Day!

Inside This Issue:

The Property Data You Need for Hurricane Season

By Melvin P. Ngayan, Director of Appraisal Services, East - AssetWorks, LLC

Atlantic Hurricane Season officially starts June 1. However, in recent years storms have been known to start kicking up their heels off the coast as early as May, getting a speedy start to their meteorological mayhem.

It's never too early for you to make sure your properties' COPE data is complete and up-to-date. When used in conjunction with a catastrophe modeling tool like AIR or RMS, thorough COPE data can help ensure you have the right coverage whenever a severe weather event pays you a visit.

When you're talking about the data that insurers and reinsurers need in the case of a hurricane risk event, this mainly concerns the "E" in secondary COPE data. In Risk Management, COPE is an acronym for "Construction Occupancy Protection and Exposure."

COPE data comes in two categories: primary and secondary COPE data. Primary COPE data details a property's square footage, its construction materials, any fire protection, and its location. Secondary COPE data drills down within those categories, detailing building structure and how it might behave under adverse weather conditions.

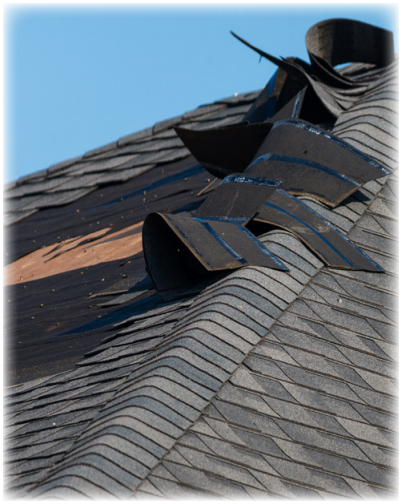
If you are in an area where hurricanes are prevalent, having accurate exposure details becomes a priority. Note that wind and flood insurance are separate policies from standard property insurance.

Your insurance rates are partially based on how well your property can withstand powerful inland winds and storm surges, as well as factors like your geography, the area's weather history and the Federal Emergency Management Agency's (FEMA) information. That involves collecting data related to the features of your property that protect against — and can be affected by — high winds and flooding.

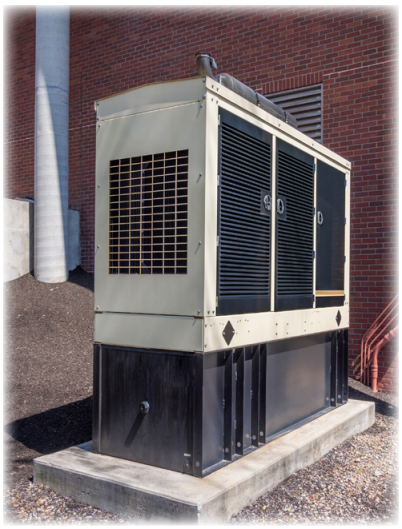
Secondary COPE Data Related to Wind

When it comes to the wind exposure associated with hurricanes and convective storms, there is a wide array of secondary COPE details that can be important to track for your Property Statement of Values. They include but are not limited to:

CONTINUED ON PAGE 2



- **Wind Resistance of Windows:** Windows with poor wind resistance are less likely to withstand powerful winds and flying debris, their damage potentially resulting in additional damage to building interiors from both wind impact and precipitation.
- **Sheltered or Unsheltered Windows:** Whether or not a window is sheltered can be another factor of note, particularly in high wind conditions where airborne objects can easily become missiles.
- **Roof Framing:** The type of framing material used for the roof can affect the roof's ability to remain safely in place during hurricane-force winds.
- **Roof Anchors:** The type and effectiveness of the connections used to secure the roof support systems to the walls can affect your risk for property damage. Different types can be more effective in areas where hurricanes are prevalent.
- **Roof Covering:** The type of materials used to cover a roof – for instance, clay tiles versus standard shingles — can affect the severity of damage to a building during a hurricane.
- **Roof Geometry:** The shape of a roof can be a factor when wind load is a concern. A high steepled roof, for example, will have more wind uplift than a flat roof.
- **Roof Parapets and Chimneys:** Parapets or chimneys are additions to a building structure that can be subject to damage in high winds. Knowing the number of chimneys and parapets a building has and the height in feet of each can be valuable data to keep on hand.
- **Roof Age and Condition:** An older roof can become brittle and might not endure the extremely high winds of a hurricane the way a newer, more flexible roof would. It's good to know the life of the roof for each of your buildings and how well each is holding up.
- **Wind Zone:** Based on information from FEMA, the Wind Zone indicates the tiers of vulnerability a particular area has for natural risk events involving high winds like hurricanes or tornadoes.



- **Mechanical/Electrical Equipment Bracing:** The way items like generators and HVAC are braced and connected to the building exterior can have an impact on how much damage occurs to a property during high winds.
- **Wind Missiles:** Some items can become missiles during the high winds of a hurricane. It's important to document these items and their distance from your property.
- **Contents' Vulnerability Due to Wind:** Describes the vulnerability of damage due to wind.
- **Cladding Type:** Cladding is the final layer on an exterior of a building. In the case of hurricanes, it can help prevent weather damage to the frame.
- **Door Resistance:** How powerfully can the property's doors resist wind and pressure? A door blown in by hurricane wind is the beginning of potential interior and structural damage.

These are just a few of the wind-related details you may wish to document to help create a more accurate picture of your property for your insurance provider. Your agent or provider can provide you with more details to collect specific to your locations and their needs.

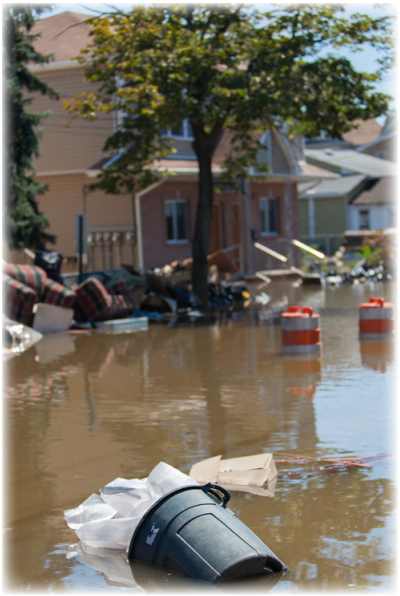
CONTINUED ON PAGE 3

Secondary COPE Data Related to Flooding

Analyzing and updating the COPE data related to flood protection can be a great way to align your property with best practices for your area as hurricane season approaches. With forethought and — if necessary – remediation, you can help avoid worst case scenarios and potentially secure better insurance rates in the process. The recommended best practices for flood protection can vary by location so be sure to contact your underwriter for the information they use to assess your flood risk. You can also check out the Flood Zone materials on FEMA's website for even more information.

Important secondary COPE details regarding flooding to incorporate into your Statement of Values might include:

- **Flood Zone:** Based on information from FEMA, the Flood Zone indicates the tiers of vulnerability that a particular area has for natural risk events involving flooding.
- **Flood Protection:** This describes the compliance of the building with flood zone requirements in design and construction.
- **Base Flood Elevation:** In a flood zone, a building may be elevated to stand on piles or have high retaining walls to ensure the lowest floor is above the Base Flood Elevation (also called BFE). Structures in flood zones with basements or non-elevated lowest floor living space built prior to current code requirements may prompt worst case scenario insurance ratings.
- **Basement:** Detailing whether a structure has a basement and, if so, its level of flood protection can be an important point to include on your SOV, particularly in a hurricane-prone region.
- **Contents' Vulnerability Due to Water:** Insurers may want to know just how vulnerable the contents of your property would be, if exposed to flooding.



While the items above are common COPE data points for flooding, make sure to check with your insurance provider for the full list of data needed for your policy and your region.

It's Not Just Bluster

Having the right COPE details on hand for your property, specific to wind and flood protection, can be a major help once hurricane season blows in. With a little forethought and a data collection plan, you can make sure your insurance coverage is complete and your ratings aren't gone with the wind.

In conjunction with AssetWorks, Preferred offers free, comprehensive property appraisals to all members that purchase their property insurance from Preferred.

Mr. Ngayan is the Regional Director with AssetWorks LLC and has been serving clients since 1997. His tenure at AssetWorks LLC has included the planning, management, and execution of numerous capital asset cost accounting studies and property appraisal projects for municipalities, county governments, and other public sector entities. As a lead valuation consultant, Mr. Ngayan's responsibilities included the training and management of appraisal staff in the Eastern Region as well as the task of managing large and complex projects.

Mr. Ngayan possesses significant technical expertise in the procedures and methodologies used to value machinery & equipment, buildings & building services, infrastructure, land improvements, and land parcels. He possesses a practical knowledge and understanding of Generally Accepted Accounting Principles (GAAP); Government Accounting, Auditing, and Financial Reporting (GAAFR); Governmental Accounting Standards Board Statement 34 (GASB 34); and various other audit concerns related to capital asset reporting. Mr. Ngayan is also experienced in providing insurance replacement and proof-of-loss information to our clients to assist in addressing their insurance reporting needs. Mr. Ngayan also has significant experience appraising architecturally unique and historical buildings.

Cybersecurity and Florida Local Government

By John M. Janousek, Esquire - Roper, P.A.

CS/HB 7055 ("Cybersecurity Bill" or "Bill") is a recent Florida bill passed by both the Florida House and Senate unanimously, which will become effective July 1, 2022, subject to the Governor's veto powers.

Among other things, the Bill creates Section 282.3185, Florida Statutes, titled "Local Government Cybersecurity Act", which imposes several requirements on Florida counties and municipalities in responding to cybersecurity and ransomware incidents.

This article provides a summary of certain of those requirements.

Prohibition on Paying/Complying with Ransomware Demands

First, the Act creates Section 282.3186, Florida Statutes, which states: "A state agency as defined in s. 282.318(2), a county, or a municipality experiencing a ransomware incident may not pay or otherwise comply with a ransom demand."[1]

As such, in the event a Florida county or municipality experiences a ransomware incident, the Act prohibits such entity from paying or otherwise complying with the ransom demanded.

Incident Notification

The Act also imposes upon local governments certain reporting requirements regarding cybersecurity and ransomware incidents. Specifically, a local government shall *report all ransomware incidents* and *certain cybersecurity incidents* to (1) the Cybersecurity Operations Center, (2) the Cybercrime Office of the Department of Law Enforcement, *and* (3) the sheriff having jurisdiction over the local government. Such report must be made as soon as possible but no later than 48 hours after discovery of a cybersecurity incident and no later than 12 hours after discovery or a ransomware incident.

Regarding cybersecurity incidents, a local government is required to report any cybersecurity incident it deems to be of severity level 3, 4, or 5, as provided in FLA. STAT. § 282.318(3)(c), which is itself significantly revised the Cybersecurity Bill. Specifically, the newly revised Section 282.318(3)(c) sets forth five (5) levels of severity for a cybersecurity incident. Such levels are defined by the National Cyber Incident Response Plan of the U.S. Department of Homeland Security, as follows:

- **Level 1** is a low-level incident that is unlikely to impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence;
- **Level 2** is a medium-level incident that may impact public health or safety; national, state, or local security; economic security; civil liberties; or public confidence;
- **Level 3** is a high-level incident that is likely to result in demonstrable impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; civil liberties; or public confidence;
- **Level 4** is a severe-level incident that is likely to result in a significant impact in the affected jurisdiction to public health or safety; national, state, or local security; economic security; or civil liberties; and
- **Level 5** is an emergency-level incident within the specified jurisdiction that poses an immediate threat to the provision of wide-scale critical infrastructure services; national, state, or local government security; or the lives of the country's, state's, or local government's residents.

CONTINUED ON PAGE 5

As noted, pursuant to the Act, a local government *is required to report* any *cybersecurity incident* it deems to be of *severity level 3, 4, or 5*. A local government *may report* a cybersecurity incident that it determines to be of *severity level 1 or 2*.

For any report by a local government of a ransomware or cybersecurity incident, the local government must include, at a *minimum*, the following:

1. A summary of the facts surrounding the cybersecurity incident or ransomware incident;
2. The date on which the local government most recently backed up its data, the physical location of the backup (if the backup was affected), and if the backup was created using cloud computing;
3. The types of data compromised by the cybersecurity or ransomware incident;
4. The estimated fiscal impact of the cybersecurity or ransomware incident;
5. The details of the ransom demanded, in the case of a ransomware incident; and
6. A statement requesting or declining assistance from the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, or the local sheriff.

Finally, the Act also imposes an "after-action report" requirement, such that the local government must submit to the Florida Digital Service,[2] within 1 week after the remediation of a cybersecurity or ransomware incident, a report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident.

The Florida Digital Service shall establish guidelines and processes for submission of these reports by December 1, 2022.

Training

The Act also requires *all local government employees with access to the local government's network* to complete certain basic cybersecurity training within thirty (30) days after commencing employment and annually thereafter.

Similarly, it requires *all local government technology professionals and employees* with access to *highly sensitive information* to complete an advanced cybersecurity training within thirty (30) days after commencing employment and annually thereafter.

Both the basic cybersecurity training and the advanced cybersecurity training are to be developed by the Florida Digital Service.

CONTINUED ON PAGE 6

Cybersecurity Standards

The Act also requires each local government to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources to ensure availability, confidentiality, and integrity. Such standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

Each county with a population of 75,000 or more, and each municipality with a population of 25,000 or more, must adopt such cybersecurity standards by January 1, 2024. Each county with a population of less than 75,000, and each municipality with a population of less than 25,000, must adopt such cybersecurity standards by January 1, 2025. Each local government must notify the Florida Digital Service once it has complied with this adoption requirement.

Given these requirements, counties and municipalities should work with their respective I.T. professionals on adopting appropriate cybersecurity standards, so as to comply with the Act.

Criminal Penalties

Finally, the Bill creates Section 815.062, Florida States, which criminalizes certain ransomware incidents. Specifically, a person who willfully, knowingly, and without authorization engages in a ransomware incident against a governmental entity, including a county or municipality, commits a first degree felony.

An employee or contractor of a governmental entity with access to the governmental entity's network who willfully and knowingly aids or abets another in the commission of such ransomware incident also commits a first degree felony.

In addition to other penalties, a person convicted of any of the above offenses must pay a fine equal to twice the amount of the ransom demand. Said funds are deposited into the General Revenue Fund.

[1] The Bill defines the term "ransomware incident" as "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."

[2] A The Florida Digital Service is a service within the Florida Department of Management Services whose purposes include, *inter alia*, providing operational management and oversight of the state data center, including developing and implementing a process for detecting, reporting, and responding to cybersecurity incidents, breaches, and threats, in collaboration with the Department of Law Enforcement.

John Janousek was admitted to the Florida Bar in 2012 and is admitted to practice before the United States District Courts for the Middle and Southern Districts of Florida, and the United States Court of Appeals for the Eleventh Circuit. Mr. Janousek received his Bachelor of Arts, majoring in Philosophy, cum laude, from the University of Florida in 2008 and his J.D., cum laude, from the University of Florida Levin College of Law in 2012. While in law school, Mr. Janousek served as the Senior Research Editor for the Florida Law Review. He was awarded the Outstanding Candidate Award and the Outstanding Associate Editor Award. He also earned book awards for both Law Review and Antitrust. Prior to joining Roper, P.A., Mr. Janousek served as a law clerk to the Honorable Maurice M. Paul, Senior United States District Judge, in the United States District Court for the Northern District of Florida. He also worked in private practice, defending clients in federal and state civil matters in such areas as products liability, personal injury, and malpractice liability.

Mr. Janousek practices primarily in the areas of civil rights, employment law, public entity law, and insurance coverage.

For more information regarding the Cybersecurity Bill and its requirements, please do not hesitate to contact the undersigned counsel.

John M. Janousek, Esq. - Roper, P.A. | 2707 East Jefferson Street Orlando, FL 32803 |Ph: 407-897-5150 | Email: jjanousek@roperpa.com

Cybersecurity Services & Support for Preferred Members

Local governments face significant financial loss when a cyber attack occurs. In recent years there has been a sharp increase in the number of reported cyber attacks that target local governments using stolen logins and passwords.

Cybercriminals often rely on human error such as employees failing to install software upgrades or clicking on malicious links to gain access to computer systems. Once access is gained, the absence of proper backup systems for data can cause an organization to become paralyzed.

Best practices to avoid the devastating effects of a cyber attack include:

- Safely manage your password and email account.
- Secure your computer and mobile devices - institute Multi-factor Authentication (MFA).
- Avoid risky online behavior - operate on a known, safe and secure network.
- Protect your data - utilize adequate backup systems.
- Equip yourself with the knowledge of cybersecurity guidelines, policies, and procedures.

To assist our members with their cybersecurity exposures, Preferred offers the following services and support to Members at no cost:

PREFERRED RISK MANAGEMENT RESOURCE CENTER

Preferred Loss Control's Preferred Risk Management Resource Center is available to Members that have their EPLI coverages with Preferred and provides the following cybersecurity resources at no cost:

- Unlimited access to cybersecurity experts via phone and email.
- Breach HealthCheck - Measurable data breach exposure and protection through instant feedback.
- Robust privacy and security templates, including a customizable incident response plan (IRP).
- Resources for keeping staff up to date on a range of issues related to privacy, data security and compliance.
- Latest news and events regarding data breaches, regulations, class-action lawsuits, cyber threats and protective technologies.

VECTOR SOLUTIONS ONLINE TRAINING

Vector Solutions online cybersecurity resources feature several courses with up-to-date lessons for browser, email, and password security to improve cybersecurity awareness amongst employees and mitigate risks to your organization. Courses offered at no cost to Preferred Members include the following:

- Cybersecurity Awareness for Employees: Classifying and Safeguarding Data for Corporate and Personal Use
- Cybersecurity Awareness for Employees: End-User Best Practices
- Cybersecurity Awareness for Employees: Security Awareness Essentials
- Cybersecurity Awareness for Employees: Social Engineering

For questions or to request additional information on Cybersecurity related services and support please contact your Regional Loss Control Consultant.

2022 Preferred Safety & Risk Management Award Recipients

The Preferred Safety and Risk Management Award Program provides recognition to Members and Risk Management Professionals that have fostered/promoted safety & health as well as advanced the profession of risk management to protect personnel/property.

Preferred presents two awards per Loss Control territory annually as follows:

Risk Management Professional of the Year Award

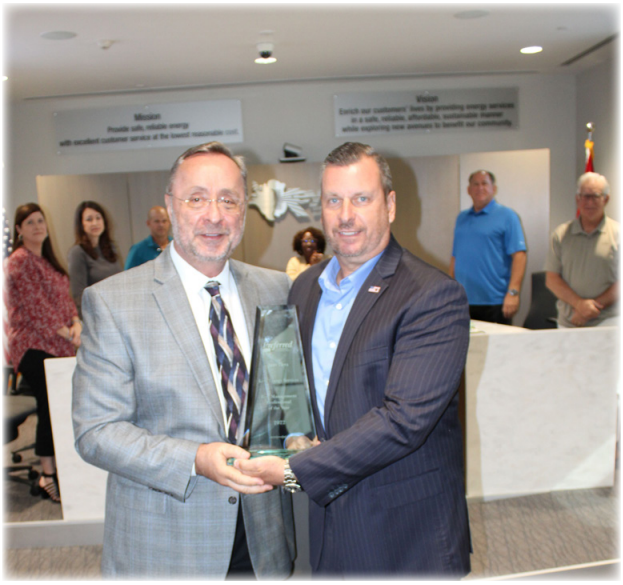
Awarded to a Risk Management Professional that has demonstrated outstanding performance in the practice of risk management for their entity as well as the risk management profession.

Safety & Risk Management Member of the Year Award

Awarded to a Member that has demonstrated continuous improvement through sound risk management practices as measured primarily by the performance of their organization's insurance program.

Preferred Members recognized for 2022 include the following:

Risk Management Professional of the Year - 2022	Safety and Risk Management Member of the Year - 2022
Juan Llera - Keys Energy Services	City of Greenacres
Jeff Hoyle - Cedar Hammock Fire Rescue	Southern Manatee Fire & Rescue
Christina Maguire - City of Ormond Beach	Marion County BOCC



Juan Llera, Risk Manager - Keys Energy Services
Risk Management Professional of the Year

Juan's accomplishments are numerous and include establishing an effective Safety Committee, developing safety-conscious policies and procedures, as well as posturing claims to achieve positive outcomes.

Juan has conducted thorough accident investigations to determine cause and corrective action to prevent reoccurrence, provided safety training to staff, performed safety inspections, and continues to promote the advancement of Risk Management to protect personnel and property for Keys Energy Services.

Pictured: (L to R) Chris Kittleson, Director of Loss Control Technical Services - Public Risk Underwriters of Florida, Inc.; Juan Llera, Risk Manager - Keys Energy Services

CONTINUED ON PAGE 9

Jeff Hoyle, Fire Chief - Cedar Hammock Fire Rescue

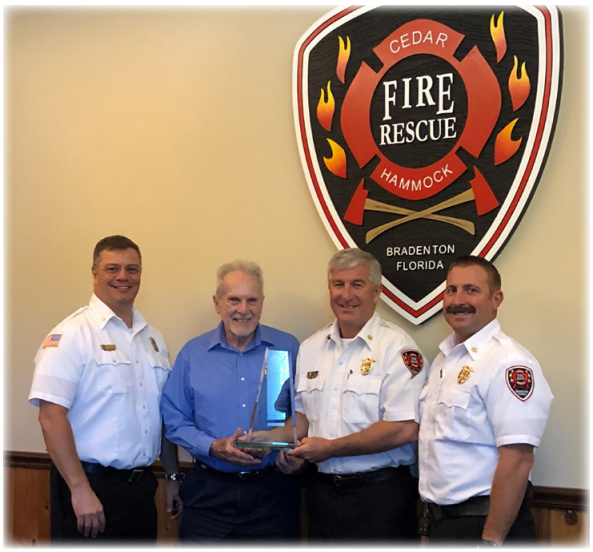
Risk Management Professional of the Year

When Chief Hoyle began his tenure with Cedar Hammock, they were plagued with workers' compensation claims frequency and severity issues.

Working closely with Preferred Loss Control, the Chief instituted a light duty program, internal claims management procedures and regular claims reviews.

The Chief appointed a training officer. They extensively utilize Vector Solutions online training for many of their training needs, including those courses needed for certification.

Pictured: (L to R) Kyle Bradshaw, Deputy Chief; Art Eversole, Boyd Insurance & Investment Services; Jeff Hoyle, Fire Chief; Joe Falcone, Deputy Chief - Cedar Hammock Fire Rescue



Christina Maguire, Risk Manager - City of Ormond Beach

Risk Management Professional of the Year

Christina is actively engaged in leading safety activities and aggressively pursues claims for positive outcomes. In no small part due to Christina's contributions, Ormond Beach's loss ratios have remained in the single digits for the last five years.

She takes advantage of the full complement of resources available to her as a Preferred member and has an excellent working relationship with Preferred Loss Control. Christina is also a mentor to RM and HR professionals at peer organizations.

Pictured: (L to R) Christina Maguire, Risk Manager - City of Ormond Beach; Mike Marinan, Director of Member Services - Public Risk Underwriters of Florida, Inc.

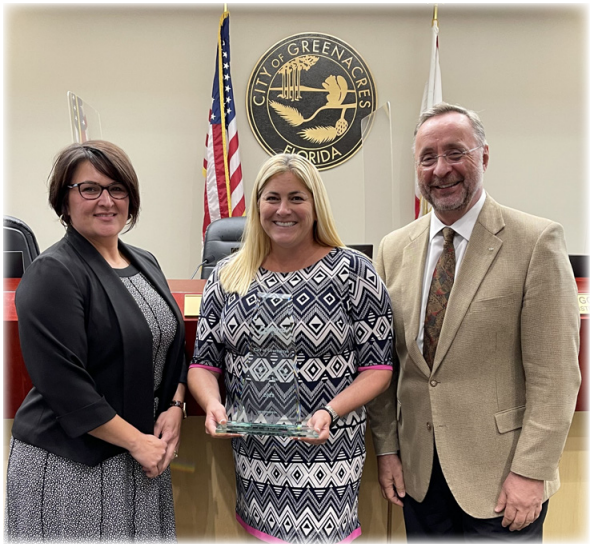
City of Greenacres

Safety and Risk Management Member of the Year

Led by Suzanne Skidmore, HR Director, the Member has established an effective Safety Committee, developed safety-conscious policies and procedures, aggressively pursued claims to achieve positive outcomes, conducted thorough accident investigations to determine cause and corrective action to prevent reoccurrence as well as provided safety training to keep staff up to date on safe work methods.

Ms. Skidmore and her team are always receptive to working with Preferred.

Pictured: (L to R) Andrea McCue, City Manager; Suzanne Skidmore, Human Resources Director - City of Greenacres; Chris Kittleson, Director of Loss Control Technical Services - Public Risk Underwriters of Florida, Inc



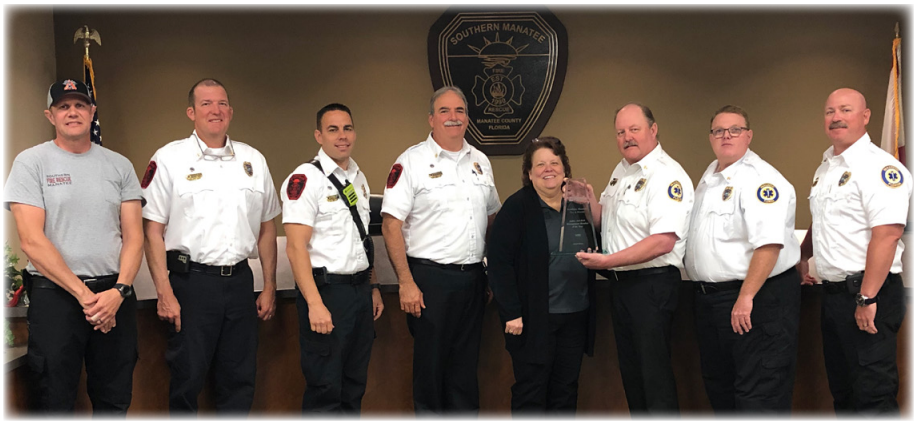
CONTINUED ON PAGE 10

Southern Manatee Fire & Rescue - Safety and Risk Management Member of the Year

SMFR has innovatively rolled their wellness program into their already effective safety committee, believing that employee safety is tied into both mental and physical health.

They extensively utilize Vector Solutions online training.

Their internal claims management has strong elements of employee communication and creative light duty assignments.



Pictured: (L to R) Steve Hodges, Lieutenant; Adam Chevalier, Logistics Officer; Adam Perry, Battalion Chief; Rick Blanco, Assistant Chief; Debbie Tuckerman, Executive Management Assistant; Robert Bounds, Fire Chief; Bobby Thayer, Training Chief; Dan Anderson, EMS Officer - Southern Manatee Fire & Rescue

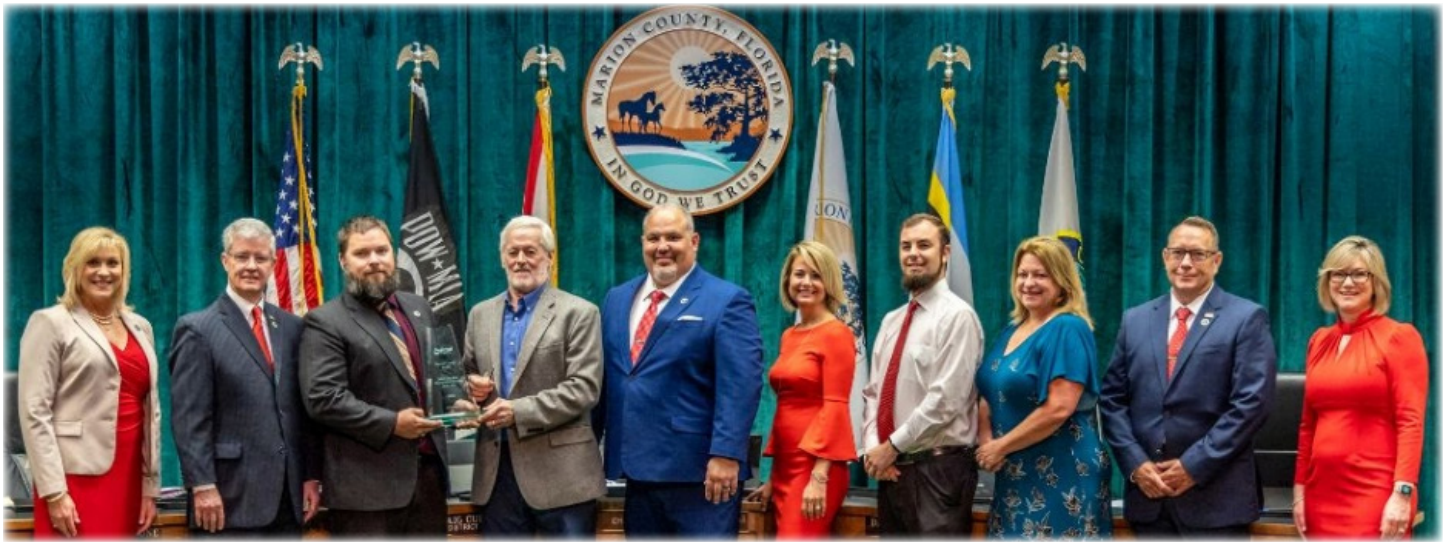
Marion County BOCC - Safety and Risk Management Member of the Year

Marion County self-insures a substantial portion of their insurance.

Led by Thomas Futch, they have a comprehensive and effective program to decrease preventable accidents and bring attention to the safety needs of the County.

They have instituted required monthly training, a recognition program for participants and have created safety liaisons within each department to encourage ownership. Employee accidents have decreased steadily over the last ten years.

Marion County extensively utilizes full complement of the resources that are made available to them as members of Preferred.



Pictured: (L to R) Michelle Stone, Commissioner [District 5]; Craig Curry, Commissioner [District 1]; Thomas Futch, Risk Liability Asset Analyst; Mike Marinan, Director of Member Services - Public Risk Underwriters of Florida, Inc.; Carl Zalak, III, Commissioner [District 4]; Amanda Tart, Executive Director of Administrative Services; Michael Rittenhouse, Safety Training & Compliance Manager; Sheri Wiley, Risk & Benefits Manager; Jeff Gold, Commissioner [District 3]; Kathy Bryant, Commissioner [District 2] - Marion County BOCC

Back by Popular Demand!

Preferred
PGIT GOVERNMENTAL INSURANCE TRUST

Member Education Day

Wednesday - February 1, 2023

Orlando World Center Marriott

SAVE THE DATE!

Preferred would like to welcome the following new members:

Children's Services Council of Leon County

Coleman Ridge CDD

Village CDD #14

KEY STAFF CONTACTS:

Marketing:
marketing@publicrisk.com
321-832-1455
Kurt Heyman

Operations:
sfugate@publicrisk.com
321-832-1451
Sarah Fugate

Loss Control:
losscontrol@publicrisk.com
321-832-1658
Mike Stephens

Claims:
fred.tucker@pgcs-tpa.com
321-832-1401
Fred Tucker

Preferred®
PGIT GOVERNMENTAL INSURANCE TRUST

P. O. BOX 958455 - Lake Mary, FL 32795-8455

PRESORTED
STANDARD
U.S. POSTAGE
PAID
ORLANDO, FL
PERMIT 1058

Preferred