2025 NEWSLETTER THIRD QUARTER

PEP ON POINT

Building Stronger Communities Together

IN THIS ISSUE

RISK SERVICES

Abolish Qualified Immunity? pg. 2-3

Security Cameras for Public Entities pg. 6

Fire Evacuation Planning pg. 8-9

FEATURE ARTICLE

Ohio House Bill 96 Cybersecurity Compliance pg. 4-5

PEP BENEFITS

PEP+ Grant Recipients and What Members are Saying pg. 7

CYBER RISK SERVICES

Top Five Cyber Threats Targeting Public Entities pg. 10-11

MEMBER SPOTLIGHT AND BOARD OF DIRECTORS

Hartford Independent Agricultural Society and PEP Board of Directors pg. 12

PHOTO COURTESY OF:
COLUMBUS & FRANKLIN COUNTY METROPOLITAN PARK DISTRICT

ABOLISH QUALIFIED IMMUNITY?

OHIO'S PROPOSED CONSTITUTIONAL AMENDMENT

BY THOMAS SPYKER, ESQ., REMINGER LAW

The **Ohio Coalition to End Qualified Immunity (OCEQI)**, is a group proclaiming to "end qualified immunity" throughout the state of Ohio by proposing a state constitutional amendment. Although OCEQI calls their proposal a narrow, corrective reform, it is actually an unprecedented expansion of governmental liability that goes beyond eliminating governmental immunities and would be ruinous to local governments. Ohio municipal leaders should be informed on this issue so that voters are aware of the impact this proposal could have on local governments.

First, let's clarify what OCEQI's proposed amendment language means. OCEQI claims the amendment abolishes qualified immunity, a defense used in federal civil rights lawsuits. In reality, however, the proposal side-steps the immunity issue by creating a new state-level claim for violations of the Ohio Constitution. Here are the ways the proposal seeks to expand liability against public sector employees and their employers:

- **Creating a Strict Liability Standard:** A claim under the proposal only requires proving a government actor caused a state-constitutional violation by a **preponderance of evidence**. In other words, a person can succeed on these claims just by proving that a municipal employee made any simple mistake in the performance of their duties.
- **Unlimited Damages and Attorney Fees:** Plaintiffs can claim, and recover, uncapped economic and non-economic damages, plus attorney fees, fueling frivolous lawsuits.
- **Vicarious Liability:** Taxpayers foot the bill for employees' conduct, even if the municipality had no role in the incident and even if the municipality disciplines the employee while correcting the issue.
- **No Right to a Jury for the public employees and municipalities:** Plaintiffs alone pick judge or jury trials, denying defendants their constitutional right to a jury.
- **Elimination of All Immunities:** The amendment prevents courts from using a qualified immunity-like analysis on these new claims. But it also wipes sovereign, prosecutorial, judicial, and legislative immunity, long-standing doctrines with completely different functions in our society.
- **Six-Year Statute of Limitations:** Claims can linger for six years, triple Ohio's two-year personal injury limit.

Second, let's consider the harmful ramifications of OCEQI's new state claim against public sector employees and their employers.

- **The Strict Liability Standard will lead to an Unprecedented Rise in Frivolous Lawsuits Against All Public Sector Employees:** The amendment's strict liability standard is a disaster nobody's talking about. It's simple and devastating: No government actor shall deprive anyone of a constitutional right. **Anyone claiming a violation can sue. No need to prove negligence or intent—they just show the act happened.**

Combining the strict liability with the broad scope of Ohio's constitution turns utterly frivolous lawsuits into viable claims that could bankrupt local governments. Consider these examples:

- **Typo Trouble:** A teacher emails student records to the wrong parent due to an auto-fill error. Ohio's Constitution (Article I, Section 1) protects student privacy. The typo violates it. The parents sue for unlimited damages and must win under this amendment. The parents may not get much money for damages, but the attorneys representing them will submit six-figure legal bills that the municipality will be forced to pay.
- **Bee Sting Mishap:** A park cleanup volunteer misses bees near a trash can. Moving it stirs the bees, stinging bystanders. Ohio's right to be free from harm (Article I, Section 1) is violated. The bystanders sue.

These examples are just the beginning because lawyers are incentivized to litigate any trivial mistake since their fees are paid on the success of the claim—not the value of it.

- **The Unlimited Damages and Vicarious Liability Components Would Drain Tax Coffers Defending and Paying Out These Lawsuits:** There is a real impact to every Ohioan. Unlimited damages and uncapped attorney fees combined with vicarious liability spell financial ruin for governments. **Plaintiffs can claim millions for emotional distress over inconveniences, and even if they do not get it, their attorneys will get six figure pay days on every case, regardless of outcome.** Public entity insurers will withdraw from the state and the legal fees accrued in defending these claims will force service cuts and tax hikes.
- **The Six-Year Statute of Limitations Creates a Long Lawsuit Window:** The six-year statute of limitations triples Ohio's two-year personal injury limit. Plaintiffs can wait years to sue, when evidence is gone and memories fade. A teacher's 2025 typo could spark a 2031 lawsuit.

Although it is unlikely OCEQI will succeed in collecting enough signatures to allow the proposal to appear on the November 2025 ballot, they will continue to pursue this proposal for future ballots. **Local governments and the public should remain aware of the effects.**

For more information on qualified immunity, contact your PEP Risk Services Specialist at (866) 907-3776.

WHAT LOCAL GOVERNMENTS NEED TO KNOW

OHIO HOUSE BILL 96 CYBERSECURITY COMPLIANCE

BY PEP CYBER RISK SERVICES TEAM

Ohio House Bill 96 (HB96) has introduced mandatory cybersecurity requirements for all local government entities. This bill was signed into law by Governor DeWine on June 30, 2025. The bill includes various provisions with different effective dates. The biennial state budget appropriations took effect on **July 1, 2025**. Most other provisions, including cybersecurity requirements, go into effect on **September 29, 2025**. This article outlines the key compliance areas and how PEP supports its Members.

CYBERSECURITY PROGRAM REQUIREMENTS

PEP provides cyber assessment support in the following areas:

- Cybersecurity assessment program that safeguards data and IT resources
- Alignment with National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
- Alignment with Center for Internet Security (CIS) controls
- Identification of critical functions and cyber risks
- Incident response and containment templates, guidance, and training
- Annual cybersecurity training tailored to employee roles

PEP Member internal or external IT support is required for:

- Threat detection mechanisms
- Drafting of incident response plans; PEP's Cyber Risk Services team can review the final draft using our vCISO services
- Infrastructure repair and post-incident security unless it's covered by insurance

TRAINING REQUIREMENTS

PEP provides annual cybersecurity training. However, HB96 may require training to be delivered by:

- Ohio Persistent Cyber Initiative (O-PCI)
- Ohio Cyber Range Institute

RANSOMWARE PAYMENT RESTRICTIONS

Members must not pay or comply with ransom demands unless:

- A formal resolution or ordinance is passed by the Ohio legislative authority
- The action is justified as in the public interest

INCIDENT REPORTING REQUIREMENTS

Cybersecurity incidents must be reported to:

- Ohio Department of Public Safety's Division of Homeland Security within 7 days
- Ohio Auditor of State within 30 days

PEP Claims will handle reporting if the incident is covered by insurance. Otherwise, the Member's internal or external IT support is responsible for handling reporting.

Reportable incidents include:

- Substantial loss of data confidentiality, integrity, or availability
- Disruption of operations
- Unauthorized access via third-party providers or supply chain compromises

ADDITIONAL REQUIREMENTS

HB96 applies to all local government entities, including:

- Counties, municipalities, public entities
- School districts, libraries, utilities, and health departments

Please reach out to PEP's Cyber IT Risk Consultant, Eric Adonteng, by email: Eric.Adonteng@Persopool.com or by phone at (240) 808-9278 to schedule a cyber risk visit.

In the event a PEP Member has a cyber breach claim, the Member should immediately reach out to Public Entity Risk Services of Ohio (PERSO), the PEP Claims Service Provider, at (866) 907-3776.

PEP CYBER SUPPORT

PEP provides support for:

- Annual cyber risk assessments
- Providing incident response plan templates and training with the Member responsible for drafting the incident response plan
- Cyber risk assessment reviews of access, backups, and logging controls

Drafting of incident response plans must be completed by the Member's internal or external IT support.

THE BENEFITS OF SECURITY CAMERAS FOR PUBLIC ENTITIES

BY PEP RISK SERVICES TEAM

Security cameras have been a topic of debate for decades. Their introduction in 1949 has led to significant advancements, making it easier for businesses, organizations, and entities to adopt them.

Concerns about cameras in public spaces, such as cost, effectiveness, potential misuse, and public perception, exist. However, like most technology, competition in the market has driven down investment costs, improved quality, and added features like remote access from secure cellular devices, eliminating the need for late-night trips to the office.

Cameras provide accurate and detailed footage, deterring vandalism in areas like local parks. To address misuse concerns, public entities should implement comprehensive policies and procedures defining access and circumstances. Studies show that the public doesn't perceive security cameras in public spaces as an invasion of privacy. In fact, they expect their presence in highly frequented areas.

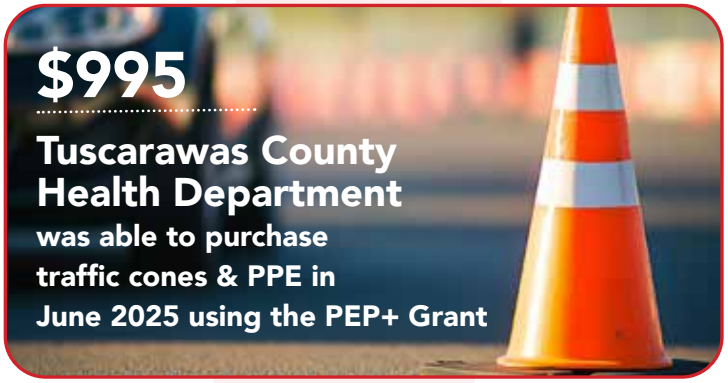
The benefits of security cameras are undeniable. Numerous entities have reported reduced vandalism after installing them. The added peace of mind they provide benefits both the public and staff. In today's staffing challenges, cameras have become increasingly valuable. Additionally, they enhance emergency operations plans by providing real-time footage, leading to quicker and more informed decision-making.

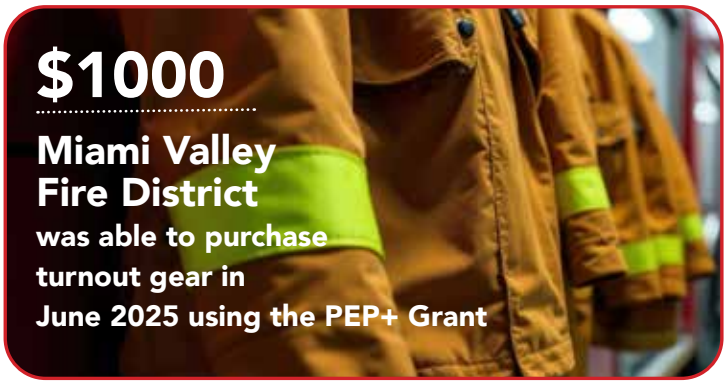
Initial hesitation about security cameras may exist, but the experience with body cameras in law enforcement demonstrates their protection of public institutions far outweighs any potential drawbacks.

Security cameras are eligible for the PEP+ grant.

'MEMBER-FOCUSED'
PEP BENEFITS

PEP+ GRANT RECIPIENTS





Apply for up to $1,000 in grant money to help fund safety items that will aid in risk control or risk management efforts. Each applicant must be a PEP Member both at the time of submission and issuance of the **PEP+ Grant Program** funds. Approved funds will be issued once membership is verified. Only qualified expenses will be considered for **PEP+ Grant Program** funds; qualified expenses include safety items wherein the primary purpose of the item is the prevention or reduction of liability claims or property losses, as well as risk control training.

QUALIFIED EXPENSES MAY INCLUDE:

- Playground Safety Material
- Safety Signage
- **Safety Cones** or other Hazard Warning Items
- Automatic External Defibrillators (AEDs)
- Fire Extinguishers
- Warning Sirens
- Reflective Materials
- Firefighter and Police Training
- Personal Protective Equipment (PPE)
- **Security Cameras**
- Driver's Training
- Fleet Management Assistance
- Compliance-related Security Software and Training Tools

WHAT MEMBERS ARE SAYING ABOUT THE RISK SERVICES TEAM

Diana Woolf provided an overview of current and pending lawsuits, vehicle crashes, driving records of employees, and potential training opportunities. I appreciate the effort to help us stay safe and save money - two important issues.

~ City of Whitehall

Nick Leach provided an update to the areas we needed to address or improve on that may have not been an issue in our last visit with him. We were provided other tools as well that will better equip our elected officials and employees. The company and representative do an excellent job for the Village of Clinton. I refer PEP to other municipalities as well.

~ Village of Clinton

FIRE EVACUATION PLANNING

BY PEP RISK SERVICES TEAM

Have you ever attended a conference, workshop, or workplace event where the speaker begins by pointing out the fire exits and explaining where to assemble if the alarm sounds? **There's a vital reason behind it; fire evacuation plans save lives.**

Every workplace, especially public buildings, must have a fire evacuation plan. Public employers are responsible for ensuring the safety of both employees and visitors. A comprehensive plan must account for everyone in the building, including individuals with disabilities and those who speak different languages. It should consider mobility, sensory, cognitive impairments, and temporary conditions that may hinder a person's ability to evacuate quickly.

KEY COMPONENTS OF A FIRE EVACUATION PLAN

- **Clear Evacuation Procedures:** Instructions on what to do when an alarm sounds, how to exit the building, and where to go once outside.
- **Designated Escape Routes:** Primary and secondary routes should be clearly marked to provide multiple exit options during an emergency.
- **Assembly Points:** Safe, designated locations outside the building where occupants can gather for accountability.
- **Communication Plan:** A strategy to alert occupants, notify emergency services, and communicate when it's safe to return.
- **Documentation:** A written plan helps educate employees, update emergency contacts, and outline specific procedures. It should also include how to alert others during an emergency.
- **Training and Practice:** Sharing the plan with employees and conducting regular drills builds confidence and reduces panic. Trained employees can assist visitors who may be unfamiliar with the evacuation process.

STEPS TO CREATE A FIRE EMERGENCY EVACUATION PLAN

1. Assess the Building: Identify hazards and determine the safest evacuation routes.
2. Develop Procedures and Maps: Include who to notify, how to alert occupants, and how to evacuate.
3. Designate Roles: Assign responsibilities such as assisting individuals with disabilities, guiding people to assembly points, and ensuring accountability.
4. Train Staff: Employees must understand the plan and their roles to effectively assist visitors to the building during an emergency.
5. Review and Update Annually: Update the plan to reflect changes in building layout, personnel, and contact information.

ADDITIONAL FIRE SAFETY TIPS

- Ensure fire extinguishers are inspected annually.
- Train employees in proper extinguisher use.
- Keep exits unlocked and pathways clear.
- Use stairs, not elevators, during an evacuation.
- Leave personal belongings behind and do not spend time powering down workstation computers; exit immediately.
- Do not reenter the building until cleared by the fire department.
- Plan for individuals who may need assistance after evacuating.
- Require participation in training and drills.

If your building does not yet have a fire or emergency evacuation plan, please contact your Risk Services Consultant for support in developing one at (866) 907-3776.

More trainings and resources covering fire evacuation planning can be found on the Guide at poolingguide.com/explore

the GUIDE

TOP FIVE CYBER THREATS

TARGETING PUBLIC ENTITIES

BY PEP RISK CYBER SERVICES TEAM

Cyberattacks continue to escalate in frequency, sophistication, and impact on public entities. Agencies face mounting pressure to defend their systems against an evolving landscape of threats. The most concerning cybersecurity risks stem from advanced persistent threats, supply chain vulnerabilities, and the increasing use of artificial intelligence by malicious actors.

1. RANSOMWARE-AS-A-SERVICE (RAAS) AND TARGETED EXTORTION

Ransomware remains one of the most dangerous threats to public entities. In 2025, attackers have professionalized their operations through RAAS, allowing even low-skill criminals to launch devastating attacks. Public entities are particularly vulnerable due to limited IT budgets and outdated infrastructure. Attackers increasingly use double extortion tactics, encrypting data while also threatening to leak sensitive citizen information unless a ransom is paid.

2. AI-POWERED PHISHING AND SOCIAL ENGINEERING

Artificial intelligence is now being weaponized to craft highly personalized and convincing phishing emails. AI can scrape public data about officials and employees to generate tailored lures that are difficult to detect. Voice cloning and deepfake video tools are also being used to impersonate executives or trusted contacts, tricking employees into making unauthorized transfers or disclosing sensitive information.

PEP offers cyber risk assessments, training, incident response plans, tabletop exercises, external vulnerability testing, and more. Please reach out to PEP's Cyber IT Risk Consultant, Eric Adonteng, by email: Eric.Adonteng@Persopool.com or by phone at (240) 808-9278 to schedule a cyber risk visit.

3. SUPPLY CHAIN INFILTRATION

Public sector systems often rely on a patchwork of third-party vendors and service providers. In 2025, attackers are increasingly exploiting these supply chain relationships to gain indirect access to critical infrastructure. A compromise in a single vendor's software or hardware can serve as a backdoor into dozens, or hundreds, of interconnected networks.

4. INTERNET OF THINGS (IOT) AND SMART CITY VULNERABILITIES

As cities and counties adopt smart technologies to improve efficiency, from traffic systems to utility grids, they also expose themselves to new attack surfaces. Many IoT devices lack robust security and cannot be easily patched, making them easy entry points for attackers looking to disrupt essential services or cause physical damage.

5. INSIDER THREATS AND CREDENTIAL ABUSE

Whether intentional or accidental, insider threats continue to pose a major challenge. In 2025, compromised credentials are a leading cause of breaches. Threat actors often purchase or harvest login information from dark web marketplaces or phishing campaigns, then use them to access government systems undetected. The lack of multi-factor authentication (MFA) across many public sector platforms exacerbates the risk.

Proactive measures are critical to defend against these threats. Public entities must prioritize basic cybersecurity hygiene: enforce MFA, segment networks, implement immutable backups, and provide regular employee training. Threat detection tools using AI and anomaly detection should be adopted where possible, and public-private partnerships can help share threat intelligence and bolster defenses.

MEMBER SPOTLIGHT

HARTFORD INDEPENDENT AGRICULTURAL SOCIETY

Hartford Independent Agricultural Society was able to obtain new playground equipment for their fairgrounds. This playground is being used as an expo for the manufacturer of the equipment. The equipment manufacturer is completing all maintenance on the playground and performing regular inspections of the equipment.

PEP BOARD OF DIRECTORS

HOWARD POSTON
Chairman
Representing Greene County Park District

DAVID MALINOWSKI
Vice Chairman
City of Mentor

JAMES L. CAPLINGER
Secretary
Representing Village of Mechanicsburg

GREG DIXON
Treasurer
Representing City of Middletown

SAL TALARICO
Representing City of Oberlin

SUSAN JAGERS
Association of Ohio Health Commissioners, Inc.

KENT SCARRETT
Ohio Municipal League

KEVIN SMITH
City of Columbiana