




---

---

---

---

---

---

---

---

**Overview**

- **Ohio Persistent Cyber Improvement (O-PCI) Purpose**
  - Supporting local government entities and their staff in all of Ohio's 88 counties in building and sustaining their capacity to anticipate, adapt, withstand and, when necessary, recover from cyber aggression.
- **Delivered at no cost to Ohio-based Local Government Entities (LGE)**
  - Funded through the Cybersecurity and Infrastructure Security Agency (CISA) and the State of Ohio.
- **Persistent Cyber Improvement Model**
  - Includes a blend of online, hybrid, and in-person modules that are tailored to local government entities of all sizes as well as to the range of organizations that have a strong cybersecurity posture and those that are actively developing in this critical space.

[cyber.rangeginstitute.org/opci](http://cyber.rangeginstitute.org/opci)

---

---

---

---

---

---

---

---

**Background**

- **US Congress passes Infrastructure Bill in 2021**
  - Cyber and Information Security Agency (CISA) disburses funds through State and Local Cyber Grant Program (SLCGP).
  - State of Ohio made a strategic decision to leverage these funds to create a statewide offering through OCRI.
- **Executed by the Ohio Cyber Range Institute (OCRI)**
  - Budget allocated to leverage talent and expertise across 26 Ohio institutions to scale delivery.
  - Example: Partnering with UD to create Cyber Mindfulness curriculum.
- **Ohio Counties (88) as lead partners**
  - All local government entities are eligible to partner.

[cyber.rangeginstitute.org/opci](http://cyber.rangeginstitute.org/opci)

---

---

---

---

---


---

---

---

OHIO PERSISTENT CYBER IMPROVEMENT

OHIO CYBER RANGE INSTITUTE



### Compliance vs. Persistence

- CISA calls for "forward-leaning action-oriented collaboration" that detects and mitigates "before" vulnerability exploitation.
- Training that not only covers how to defend, but how to anticipate. Not just "box-checking" but "continuous improvement."
- Deliverables include co-creating operating documents and guidance on organizational structure that supports persistence.
- Incremental, tailored, and sustainable.
  - General Staff, IT, Managers, Executives

[cyber.rangerangeinstitute.org/opci](http://cyber.rangerangeinstitute.org/opci)

---

---

---

---

---

---

---

---

OHIO PERSISTENT CYBER IMPROVEMENT

OHIO CYBER RANGE INSTITUTE

### A Compliance Approach

- Defend
- Attacks; Hacks; Incidents
- React/Respond
- Incident Response Plan
- Cyber Awareness
- NIST as objective/end state
- Box-checking
- "Best Practice" Adoption

### An Initiative Persistence Approach

- Defend Forward (temporal)
- Cyber Campaigns
- Anticipate/Anticipatory Resilience
- Anticipation and Resilience Plan
- Cyber Mindfulness
- NIST as a means to reduce insecurity
- Continuous improvement
- Better Practice Integration

[cyber.rangerangeinstitute.org/opci](http://cyber.rangerangeinstitute.org/opci)

---

---

---

---

---

---

---

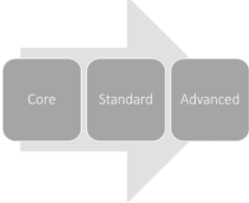
---

OHIO PERSISTENT CYBER IMPROVEMENT

OHIO CYBER RANGE INSTITUTE

### 3 Levels of Training: Gateways

- Gateway 1
  - **Core** – Understanding Concepts and National Standards
- Gateway 2
  - **Standard** – Put it into Practice with Behavior Change
- Gateway 3
  - **Advanced** – Drilling your Plans and Procedures



[cyber.rangerangeinstitute.org/opci](http://cyber.rangerangeinstitute.org/opci)

---

---

---


---

---

---

---

---



## Gateway One: Core Overview

- Sensing Engagement (In Person - 2.5 Hours)
- Cyber Mindfulness (3 Hours)
- Cybersecurity 101 (3 Hours)
- Cybersecurity Frameworks Introduction (2 Hours)
- Risk Management (2.5 Hours)
- Vulnerability Management (5 Hours)
- Organizational Leadership & Third Party Security (2.5 Hours)
- Network Control Systems (5 Hours)

- **25 Hours of training content included in Gateway 1**
- **Overall time commitment will vary by role**
  - General, IT Staff, Management, Executive/Elected
- **One Month for all staff to complete**
  - Local government entities will be onboarded into Gateway One on a rolling basis once training has commenced for the county government

[cyber.angainstitute.org/opci](http://cyber.angainstitute.org/opci)

---

---

---


---

---

---

---

---



## Sensing Engagement (2.5 Hours) \*in person\*

- **For IT Leadership, Management, Executives**
  - Gaming out an abbreviated cyber incident scenario in real-time with key stakeholders from the organization.
- **Outcome**
  - Engage leadership and key stakeholders to encourage buy-in across organization
  - Opportunity to request any additional information prior to launch of online educational modules

[cyber.angainstitute.org/opci](http://cyber.angainstitute.org/opci)

---

---

---


---

---

---

---

---



## Cyber Mindfulness (3 Hours)

- **For All Employees**
  - Basic cybersecurity best practices. Overview of cyber mindfulness and how to practice it in daily digital activities such as emailing, web browsing, and social media. How to recognize and avoid cyber threats such as phishing, malware, and ransomware.
- **Learning Outcome**
  - Apply cyber mindfulness techniques to online behavior and habits to identify vulnerabilities and prevent common cyber attacks.
  - Course offers guide to security breach response.

[cyber.angainstitute.org/opci](http://cyber.angainstitute.org/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## Cybersecurity 101 (3 Hours)

- **For IT Staff**
  - Introduction to the principles and concepts applied to cybersecurity. Provides a deeper technical understanding of cybersecurity threats and challenges facing local governments. Explores the fundamental security services, mechanisms, and principles used to establish standards and best practices for cyber persistence.
- **Learning Outcome**
  - Understand key cybersecurity concepts and principles to apply a persistent cyber strategy in the organization.
  - Course offers communication methods for greater alliance.

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## Cybersecurity Frameworks Intro (2 Hours)

- **For IT Staff, Management, Executive**
  - Introduction to core concepts and applied practices of Cybersecurity Frameworks (CSF), a set of voluntary guidelines and standards for improving cybersecurity and managing cyber risks. Tailored to the specific needs and challenges of local governments. Includes an optional module focused understanding and applying the National Institute of Standards and Technology (NIST) frameworks.
- **Learning Outcome**
  - Understand the benefits of implementing Cybersecurity Frameworks to implement a persistent cyber defense and mindful workforce.
  - Course offers methods to improve cybersecurity.

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## Risk Management (2-5 Hours, varies by role)

- **For IT Staff, Management, Executive**
  - Introduction to core concepts and applied practices of Cybersecurity Frameworks (CSF), a set of voluntary guidelines and standards for improving cybersecurity and managing cyber risks. Tailored to the specific needs and challenges of local governments. Includes an optional module focused understanding and applying the National Institute of Standards and Technology (NIST) frameworks.
- **Learning Outcome**
  - Understand the benefits of implementing Cybersecurity Frameworks to implement a persistent cyber defense and mindful workforce.
  - Course offers methods to improve cybersecurity.

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---


---

---


---

---


---



**OHIO PERSISTENT  
CYBER IMPROVEMENT**



**OHIO CYBER  
RANGE  
INSTITUTE**




---

## Vulnerability Management (5 Hours)

- **For IT Staff**
  - Deep technical dive into the types of vulnerabilities and attack vectors that threat actors can exploit to compromise systems and data. Provides techniques and tools for conducting automated and manual scans to identify and assess cyber vulnerabilities.
- **Learning Outcome**
  - Develop and maintain a network system vulnerability management plan.
  - Course offers creation of a network vulnerability plan.

[cyber.rangemaster.com/opci](http://cyber.rangemaster.com/opci)

---

---

---

---

---

---

---

---



**OHIO PERSISTENT  
CYBER IMPROVEMENT**



**OHIO CYBER  
RANGE  
INSTITUTE**




---

## Organizational & Third-Party Security (2-5 Hours, varies by role)

- **For IT Leadership, Management, Executive**
  - Equips local government officials and managers with the knowledge and skills needed to protect information and infrastructure from cyber threats. Protect the confidentiality, integrity, and availability of personal, private, and sensitive information (PPSI) collected, stored, processed and shared by the organization.
- **Learning Outcome**
  - Assess and manage cybersecurity risks posed by third-parties.
  - Course offers development of a cybersecurity policy.

[cyber.rangemaster.com/opci](http://cyber.rangemaster.com/opci)

---

---

---


---

---


---

---


---



**OHIO PERSISTENT  
CYBER IMPROVEMENT**



**OHIO CYBER  
RANGE  
INSTITUTE**




---

## Network Control Systems (5 Hours)

- **For IT Staff**
  - Concepts and techniques of network systems controls and security design. Technical implementation of various network security mechanisms will be explored. Learn to analyze and prioritize security controls to design a security architecture that aligns with critical business systems, policies, and best practices.
- **Learning Outcome**
  - Design and plan network systems architecture and topology, security controls, and solutions.
  - Course offers details of how to map and analyze data flow.

[cyber.rangemaster.com/opci](http://cyber.rangemaster.com/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## Gateway Two: Standard / Three: Advanced

- **In development**
  - Plan to pilot Gateway Two in Summer 2024; pilot Gateway Three in Fall 2024
  - Gateways completed in sequence, but will be tailored to each entities needs and positioning
- **Gateway Two: Standard**
  - Put training into practice with behavior change
  - Two months for all staff to complete; 29 hours of training provided, varies by role
- **Gateway Three: Advanced**
  - Drilling plans and procedures
  - Two months for all staff to complete; 46 hours of training provided, varies by role

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## Current Timeline

- **Pilot - Spring 2024**
  - Onboarding two counties and sub-county local government entities to start training in April 2024.
  - Collecting user feedback and iterating through the pilot
- **Launch Gateway One: Core - Summer 2024**
  - Counties and local government entities will be onboarded as capacity allows.
  - Currently 20+ counties interested in participating.

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---

---

---

---

---

---



OHIO PERSISTENT  
CYBER IMPROVEMENT



OHIO CYBER  
RANGE  
INSTITUTE



## How to Participate

1. Register at: <https://www.ohio cyberangeinstitute.org/opci>
2. County leadership will meet with OCRI staff to initiate the onboarding process, including review of training requirements, timeline, and review of Memorandum of Understanding (MOU), Non-Disclosure Agreement (NDA), and other required documentation.
3. Interested local government entities within a county will be onboarded into O-PCI through a combination of outreach by county leadership and OCRI staff to establish county-based cohorts of training participants.
4. Training begins on a mutually agreed upon start date once a cohort of local government entities are onboarded, MOU and NDA agreements are completed, and dependent on OCRI capacity.

[cyberangeinstitute.org/opci](http://cyberangeinstitute.org/opci)

---

---

---


---

---


---

---

---



**OHIO PERSISTENT  
CYBER IMPROVEMENT**



**OHIO CYBER  
RANGE  
INSTITUTE**

**More Information**

- Visit [ohiocyberrangeinstitute.org/opci](http://ohiocyberrangeinstitute.org/opci)
- All handouts are available on the site
- 30 Minute webinar from December 2023 posted with FAQs
- **Reach out to your county government officials**
- Interest from: Hocking, Jackson, Mercer, Fairfield, Holmes, Portage, Tuscarawas, Miami, Hamilton, Morrow, Lake, Ashtabula, Summit, Scioto, Cuyahoga, Lucas, Mahoning, Knox, Henry, Union, Washington
- **Connect with Us!**
- [linkedin.com/company/ohio-cyber-range-institute/](https://www.linkedin.com/company/ohio-cyber-range-institute/)

cyberangeinstitute.org/opci

---

---

---

---

---

---

---

---



**OHIO PERSISTENT  
CYBER IMPROVEMENT**

[ohiocyberrangeinstitute.org/opci](http://ohiocyberrangeinstitute.org/opci)



**Peter Koback**  
Associate Director  
Ohio Persistent  
Cyber Improvement  
[peter.koback@uc.edu](mailto:peter.koback@uc.edu)  
(513) 556 - 8138



**Amanda O'Mara**  
Cyber Training Program Coordinator  
Ohio Persistent  
Cyber Improvement  
[omaraaj@uc.edu](mailto:omaraaj@uc.edu)  
513-556-9903



**OHIO CYBER  
RANGE  
INSTITUTE**

---

---

---

---

---

---

---

---