CyberOhio

CyberOhio

Governor DeWine's Cyber Ohio Program

Kirk Herath
Cybersecurity Strategic Advisor to Governor DeWine

CCAO
Winter Conference
December 4, 2024

WHY CYBERSECURITY MATTERS FOR GOVERNMENTS

NBC NEWS

U.S. NEWS

Hackers have taken down dozens of 911 centers. Why is it so hard to stop them?

Cyberattacks on state and local governments rose in 2023, says CIS report

New survey results from the Center for Internet Security found that all types of attacks against government agencies increased in frequency last year.

The New York Times

China Is Targeting U.S. Infrastructure and Could 'Wreak Chaos,' F.B.I. Says

In testimony before Congress, Christopher A. Wray, the agency's director, said Beijing was preparing to sow chaos if disputes with the United States flared into conflict.

CNN Business Markets Tech Media Calculators Videos

Alabama state and city governments grapple with pair of cyber incidents

Local governments in Colorado, Pennsylvania and Missouri dealing with ransomware

CYBERSECURITY

Medicaid, SNAP Could Become Key Cyber Attack Targets

A new report predicts cyber attackers may increasingly target federal services that support residents' basic needs, aiming to disrupt U.S. society, spark panic and foment distrust in government.

CYBERSECURITY INFRASTRUCTURE SECURITY

U.S. County Files Disaster Declaration in Wake of a Devastating Ransomware Attack

10 WJAR

New Bedford Police Department hit with ransomware attack

by NBC 10 NEWS

mware attack

abc NEWS

Emergency services a likely target for cyberattacks, warns DHS

Ransomware attacks in particular threaten to disrupt services.

OHIO CYBER CAPABILITIES

Mike DeWine, Governor

Jon Husted, Lt. Governor

Cybersecurity Strategic Advisor (CSA), CyberOhio

Ohio Comprehensive Cybersecurity Plan (OCCP), EO 2022- 07D

Public Safety (ODPS)

Homeland Security
SAIC Cyber
Critical Infra. Office

State Highway Patrol
Computer Crimes Unit

Emergency Mgmt Agency
Planning, Training Exercise

Adjutant General

Ohio Cyber Integration Center (OCIC)

Statewide Terrorism Analysis & Crime Center (STACC)

CyberOhio Local Gov Grants

Ohio Persistent Cyber Improvement (OPCI)

Ohio Cyber Reserve (OhCR)

Ohio Cyber Collaboration Committee (OC3)

Ohio National Guard Cyber Force

Ohio Air National Guard Cyber Warfare Wing

Higher Education

Ohio Cyber Range Institute (OCRI)

Cybersecurity and Information Technology curriculum for adult education

OARNet

Education (ODEW)

Cybersecurity and Information Technology Curriculum for K-12

Cyber Academy Pilot

Career Tech School Cyber Program Support

Management Councils
Information Tech. Centers

Administrative Services (DAS)

Innovate Ohio Platform
OHID

Office of Information Security and Privacy
Enterprise Security Incident & Response (SIRT)
Engineering
Governance Risk & Compliance (GRC)
Information Security Officers (ISO)
Cloud Architecture Team
Privacy Team

Ohio EPA

Water & Wastewater Security

Dept. of Development

Small Business Training - CMMC

OSU – SBA Small Business Training

Inter-Agency Coordination & Outreach

CyberOhio Advisory Board

Cyber Risk Committee

Homeland Security Advisory Committee – Cyber
SLCGP Management

CyberOhio Speakers Bureau

Ohio Digital Academy

Federal Partners

FBI

DHS - CISA

DHS - HSI

USSS

Constitutional Offices

Secretary of State
Cyber Defense Team

Attorney General
Bureau of Criminal Investigation
Cyber Crimes Unit

Auditor of State

CURRENT OHIO COMPREHENSIVE CYBERSECURITY PLAN GOALS

Improve cyber intelligence sharing across local, state and federal organizations

Expand Ohio Persistent Cyber Improvement (OPCI) – 3 levels of training, cyber assessments and table-top exercises for local governments

Whole-of-State cyber capabilities and resiliency

Improve cybersecurity across state agencies

Update and test the Ohio Cyber Incident Response Emergency Operations Plan with state and local governments

WHOLE-OF-STATE APPROACH

Ohio Persistent Cyber Improvement Program (OPCI)

- Local government cybersecurity training and assessment program. Operated through the University of Cincinnati Ohio Cyber Range Institute.

Ohio Cyber Integration Center (OCIC)

- The OCIC is a fusion center that shares cyber intelligence and coordinates incident response for local governments.

Local Government Cybersecurity Software Grants

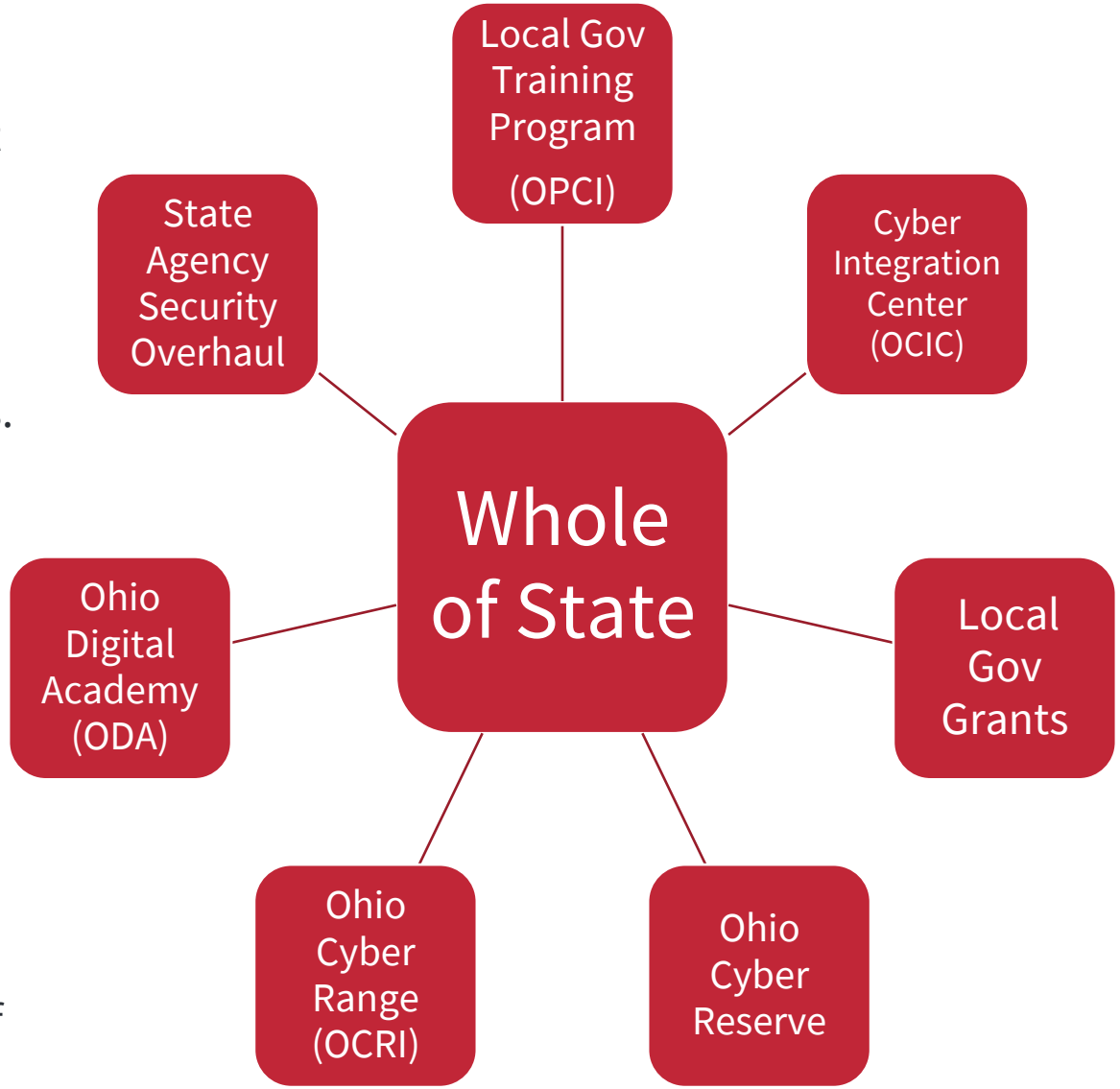
- Our $7 million grant program recently closed. Awards to be announced.
- Highly encouraging "collective defense" communities.

Ohio Cyber Reserve

- Currently, 177 reservists. We expect 200 reservists by the end of the year.

Ohio Cyber Range Institute

- Training platform for cybersecurity students and professionals, like a law enforcement training range.
- Trained 28k+ Ohioans through its statewide ecosystem of 19 regional programming centers (generally, higher ed institutions).



COLLECTIVE DEFENSE

What is Collective Defense in Cybersecurity?

Collective defense is a cybersecurity strategy where multiple organizations work together to protect against common threats. In the context of local governments, it involves sharing resources, intelligence, and best practices to build a stronger and more unified defense against cyber attacks.

- By adopting a collective defense model, local governments can significantly enhance their cybersecurity posture and build a more resilient digital infrastructure.
- CyberOhio Offers a variety of resources to help you implement this model.

Key Components of Collective Defense

Coordinated Response: By collaborating, local governments can coordinate responses to incidents, ensuring faster and more effective containment and recovery.

Shared Threat Intelligence: Participating entities exchange information on emerging threats, attack patterns, and vulnerabilities, enabling proactive defenses.

Unified Security Policies: Collective defense encourages the adoption of standardized security policies and protocols, enhancing consistency across different jurisdictions

Resource Pooling: Municipalities share cybersecurity tools, expertise, and training, optimizing resource usage and expanding capabilities.

Benefits of Collective Defense

Enhanced Protection: By sharing knowledge and resources, local governments are better equipped to detect, prevent, and respond to cyber threats.

Cost Savings: Pooling resources reduces individual costs, making advanced cybersecurity measures more affordable.

Greater Resilience: Together, local governments create a stronger and more resilient cybersecurity network.

BEST PRACTICES & ACTION PLAN

Complete a Cybersecurity Assessment

- Understanding what your vulnerabilities are is crucial to charting a way forward.
- Coordinate with your county to get an assessment done through the O-PCI program.

Close gaps with training and resources

- Use the OPCI program to learn and train for preventing cyber-attacks.
- Apply for grant dollars through the Local Government Cybersecurity Grant program to fill any gaps found.

Create a response plan for a cyber-attack

- What processes do you need to have in place to function?
- Reference the State Cyber Emergency Response plan.
- Coordinate with your county EMA to create a plan specific to you

Test your plan with a tabletop exercise

- Participate in a tabletop exercise with your county through OPCI or CISA.
- Identify further areas for improvement
- Repeat!

LOCAL GOVERNMENT CYBER GRANTS

The Infrastructure Investment and Jobs Act (IIJA) included provisions for SLCGP (State and Local Cybersecurity Grant Program) to address cyber risks and threats to the information systems of state, local, or tribal governments. State of Ohio is matching with over $10 million in-kind contributions.

Round 1: $7million – Closed in September

Round 2: Estimated $5 million – Spring 2025
Helping local governments purchase cybersecurity software, transition to a Dot Gov, and targeting collective defense arrangements

Local government cybersecurity grants (Helps Defend and Recover)

Local government Dot Gov Domain Transition (Protects Websites and Prevents Fraud)

DEEP DIVE : OHIO PERSISTENT CYBER IMPROVEMENT (OPCI)

LOCAL GOVERNMENT CYBERSECURITY ASSESSMENT & TRAINING

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.

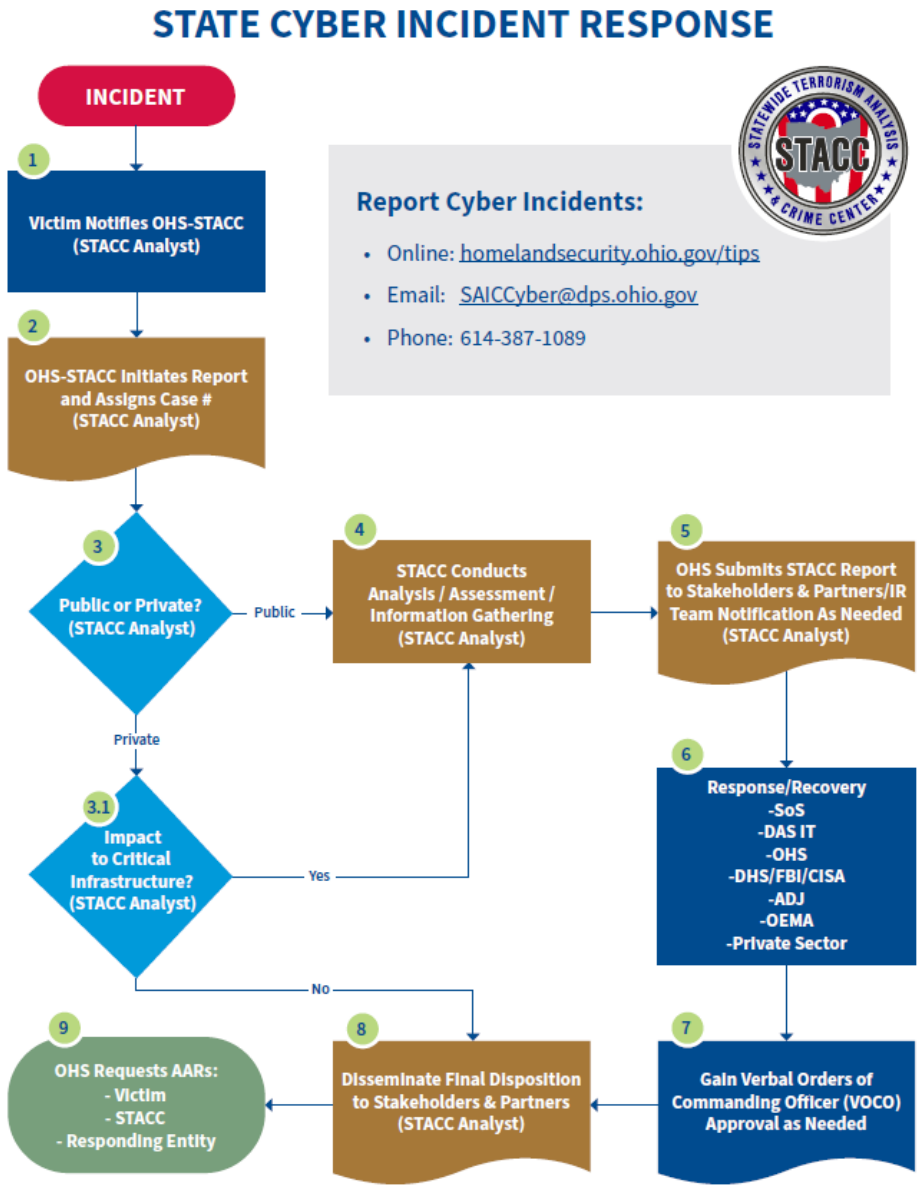
Persistent Cyber Improvement Model Includes a blend of online, hybrid, and in-person modules that are tailored to local government entities of all sizes as well as to the range of organizations that have a strong cybersecurity posture and those that are actively developing in this critical space.

- **Over 1,797 local public employees** currently receiving training in 5 counties.
- **25 hours of training content** created.
- **42 Local Gov. Entities (25 counties) in the pipeline** (40k employees serving 5.5+ million Ohioans)
- Future: Recruiting counties and seeking additional funding through biennial budget process.

2024	2025	
Hocking (Live)	Summit	Lake
Jackson (Live)	Knox	Morrow
Morrow (Live)	Henry	Medina
Tuscarawas (Live)	Union	Ross
Miami (Live)	Washington	Stark
Lucas	Butler	Mercer
City of Akron	Athens	Geauga
	Cuyahoga	Fairfield
	Hamilton	Holmes
	Mahoning	Portage
	Clermont	Ashtabula
		Scioto

CYBER INCIDENT RESPONSE

- Cyber Incident Response for local government entities and critical infrastructure is now coordinated through the "new" Ohio Cyber Integration Center.
- Internal Cyber Incidents are coordinated with the Office of Information Security and Privacy.
- Staffing for the OCIC is in process:
  - Four hired employees from Ohio Homeland Security
  - One hired from the Adjutant General's Office.
  - A manager hire is in process and three more Cyber Analysts to be hired by Ohio Homeland Security
  - Total staff will be 10 by this time next year.
- The Ohio Cyber Integration Center formally opens in 2025, but it is being built and run today.



CRITICAL INFRASTRUCTURE

Water and Wastewater Systems

- Coordinating with Ohio EPA on surveying licensees and grants.
- Coordinating with Cyber Reserve on assessments.
- Education and outreach to water and wastewater associations.
- Submitted Cybersecurity water action to the White House Director of Critical Cyber Infrastructure.

Energy

- Working with the Ohio Electric Cooperatives to build shared cybersecurity services and a self-assessment model.
- Coordinating with the DPS critical infrastructure office to build out assessment capability.

Critical Communications & Emergency Services

- Initiated first (and free) cybersecurity assessment of 6 Next Gen 911 operators.
- Working with DAS MARCS and 911 to secure systems.

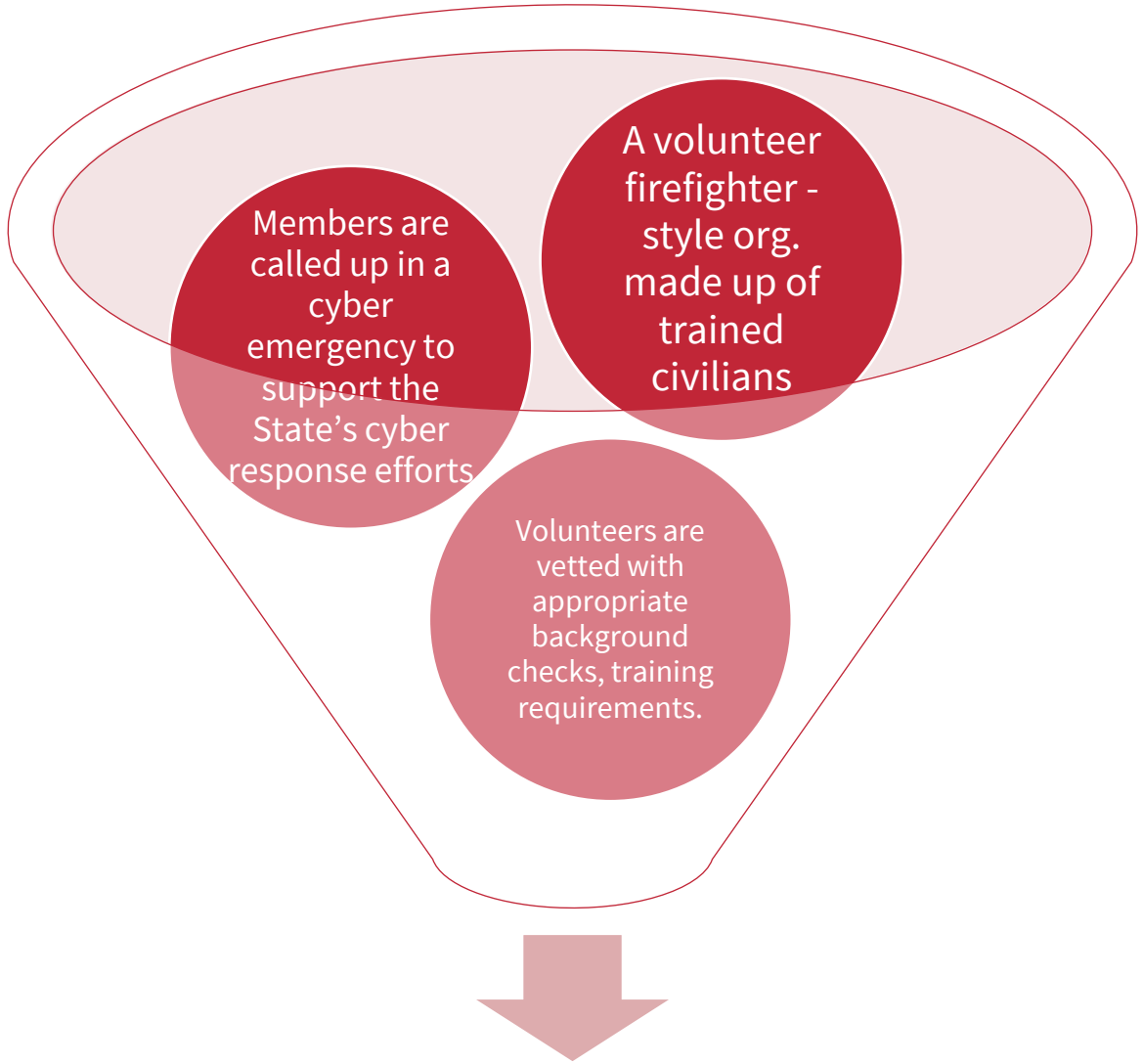
Elections

- Created a formal pre-election cybersecurity coordination network.
- Group includes Secretary of State, U.S. Cybersecurity, Infrastructure and Security Agency, and several State of Ohio agencies, such as DAS.

- Building a regular assessment mechanism of the most vulnerable critical infrastructure sectors.
- Creating a mechanism for state-level breach reporting.

THE OHIO CYBER RESERVE

- The Cyber Reserve is on track to have 200 members by the end of the year.
- Like a fire department, it's important to involve the Cyber Reserve quickly, if they are needed.
- The Cyber Reserve is not formulated to be the first line of defense.
- It's important that you have your "smoke alarms," "fire extinguishers," and "fire hydrants".



The Cyber Reserve's regional teams are available to support you in a cyber emergency.

CYBER.OHIO.GOV: RESOURCES ARE AVAILABLE

CyberOhio exists to connect you to resources and help you navigate the cybersecurity world.

Several State of Ohio Agencies have resources and support available:

Ohio Department of Public Safety, Department of Homeland Security

Ohio Adjutant General's Office, Cyber Reserve and Ohio Cyber Range Institute

Connect with us at: CyberOhio@Governor.ohio.gov