



MID-OHIO REGIONAL  
**MORPC**  
PLANNING COMMISSION

111 Liberty Street, Suite 100  
Columbus, Ohio 43215  
morpc.org

T. 614. 228.2663  
TTY. 1.800.750.0750  
info@morpc.org

**NOTICE OF A MEETING  
LOCAL GOVERNMENT RESOURCES WORKING GROUP**

MID-OHIO REGIONAL PLANNING COMMISSION  
111 LIBERTY STREET, SUITE 100 COLUMBUS, OH 43215

*OLENTANGY CONFERENCE ROOM  
(MICROSOFT TEAMS LINK IN CALENDAR INVITATION)*

November 14, 2022 | 3:00 PM

**AGENDA**

- 1. Welcome / Overview – *Christina Drummond, Chair***
- 2. Staff Report – *Jennifer Noll, MORPC***
- 3. Priority Resources Updates & Report-Out**
  - i. Cybersecurity
    - a. Doug: Items 1 – 5
    - b. Andrew: Items 6 – 10
  - ii. Public Records
    - a. Christina: Items 1 – 6
- 4. Work Plan and Schedule for the Remainder of 2022**
- 5. Refining the 2023 Working Group Objectives**
  - i. How to make the resource library self-sustaining?
- 6. Other Business**
- 7. Adjourn**

**Please notify Lynn Kaufman at 614-233-4189 or [LKaufman@morpc.org](mailto:LKaufman@morpc.org) to confirm your attendance for this meeting or if you require special assistance.**

The Date and Time of the Next Meeting of the  
Local Government Resources Working Group is  
**3:00 pm Monday, December 12 at MORPC**

## **Priority Domains & Sub-Domains/Categories**

### **Cybersecurity - Cybersecurity policies and guidance**

1. Cybersecurity Plan & Controls (Assessment, prioritization, plan and security controls architecture for protecting data and systems)
2. Cyberliability (Insurance coverage for system breach response, claim defense, affected persons notification, ransom, and recovery)
3. Data & System Risk Assessment (Data and system sensitivity, criticality and risk assessment and compensating controls)
4. Compliance Management (Management of HIPAA, PCI, CJIS, FTI, 1347 and other security compliance regulations)
5. Employee Cybersecurity (Employee security training and awareness)
6. Cloud & Vendor Cybersecurity (Security assessment, terms and conditions for using cloud and vendor services)
7. Data Sharing Cybersecurity (Security assessment, terms and conditions for sharing data)
8. Smart Devices Cybersecurity (Security assessment, controls and 2 configuration for using smart and connected devices)
9. Remote Access Cybersecurity (Security assessment, controls, and terms for permitting employee and vendor remote access to devices and systems)
10. Incident Response (Communications, responsibilities, actions and custody I the event of a cybersecurity event)

### **Public Records**

1. A policy that describes routine ways to respond to requests.
2. A policy that describes how metadata is to automatically accompany a response for data, where appropriate.
3. A policy that describes how people can request records on a website or through some other convenient communication.
4. A policy that explicitly determines what resources are needed to provision public records.
5. A policy that describes how to log requests and responses to requests.
6. A policy that describes how to anticipate what public records might be requested.