**MCRCSIP Cyber Security Pre-Review Questionnaire**

In advance of your road commission’s cyber security review, answer as many questions as you can. If you do not know the answer to a question, leave it blank.

**County Name** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Completed by** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_ **Date** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Person to contact to schedule on-site visit** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Virus and Malware:**

1. Do you have a centralized anti-virus program? [ ] Yes [ ] No
2. Which Anti-virus program do you use? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Do you check your anti-virus for updates weekly? [ ] Yes [ ] No
4. Do you perform weekly full scans? [ ] Yes [ ] No
5. Do you have a log of viruses you get? [ ] Yes [ ] No

**Windows and Active Directory:**

1. Are employees required to regularly reset their Windows password? [ ] Yes [ ] No
2. If so, how often? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Do you use Active Directory for user and password management? [ ] Yes [ ] No
4. Do you use 2-Factor Authentication? [ ] Yes [ ] No
5. Do you have a maintenance plan for patch management? [ ] Yes [ ] No
6. Do you have any operating systems that are XP or older? [ ] Yes [ ] No
7. Do you have mapped drives? (Drives you can connect to that are not part of your local PC) [ ] Yes [ ] No
	1. Can you open up any and all files on your mapped drives? [ ] Yes [ ] No
8. How does your network or system administrators keep and maintain a log of changes made? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
9. Do your Windows desktops automatically lock out after a period of inactivity?
 [ ] Yes [ ] No

**Policies:**

Do you have any of the following policies?

1. Internet usage policies for all employees who access the Internet? [ ] Yes [ ] No
2. Remote access policies for all users who access your network from home or another office? [ ] Yes [ ] No
3. Phone policies for users connecting to mail and other secure networks?
 [ ] Yes [ ] No
4. Bring your own device policies? [ ] Yes [x] No
5. Password policies? [ ] Yes [ ] No
6. Locked desktop policies? [ ] Yes [ ] No
7. Do you have a disaster recovery (DR) plan? [ ] Yes [ ] No
8. Does your DR plan include DDOS attacks and data breaches? [ ] Yes [ ] No
9. Does your DR plan include how to respond to and address ransomware?
[ ] Yes [ ] No
10. Does it include down time for disaster levels such as a destroyed building?
[ ] Yes [ ] No

**Remote access:**

* + 1. Describe how remote access is authorized and monitored.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Describe the type of authentication used for remote access.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. Are remote users required to have anti-virus on their devices? [ ] Yes [ ] No
1. Do you allow users to access your network through public networks such as a coffee shop, etc? [ ] Yes [ ] No

**Servers:**

1. How often do you have to reset your server password? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Is it required or optional? [ ] Required [ ] Optional
2. Do you use two factor authentication on your servers? [ ] Yes [ ] No
3. Do you have a maintenance plan for patching your server? [ ] Yes [ ] No
4. Do you have any operating systems that are Windows 2003 or older? [ ] Yes [ ] No
5. Are your servers or computers recording logins? [ ] Yes [ ] No
	1. Are the logs being stored on the server? [ ] Yes [ ] No
6. Describe how network and system administrators keep and maintain a log of changes made on servers. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
7. Does your server lock out after a period of inactivity? [ ] Yes [ ] No
8. Does your server have anti-virus? [ ] Yes [ ] No

**Road Commission Software (e.g. Precision)**

1. Do you run on a SQL server? [ ] Yes [ ] No
2. Is the SA password for your SQL server non-default? [ ] Yes [ ] No
3. Does your SQL server use Windows authentication or SQL logins? [ ] Yes [ ] No
4. Are non-required tables within the SQL database locked down? [ ] Yes [ ] No
5. Can someone access all data with standard user accounts? [ ] Yes [ ] No
6. Do you run a maintenance plan on your SQL database? [ ] Yes [ ] No
	1. Do you get notification if there is corruption? [ ] Yes [ ] No
	2. Do you get notification of certain table access? [ ] Yes [ ] No
7. What version of SQL server is Precision running on? [ ] Yes [ ] No
8. Describe how a new user/account is generated? How many people can create users?
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Network**

1. Describe how security events are logged.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Describe how responses to security events are initiated, implemented, and reported.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Do you have a separate firewall on your network and what kind? [ ] Yes [ ] No
	1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. Does the Firewall have intrusion detection and prevention?
	[ ] Yes [ ] No
	3. Do you have any monitoring in place on your firewall or network?
	[ ] Yes [ ] No
	4. Are log files kept and backed up on your firewall?
	[ ] Yes [ ] No
4. Do you port forward any ports on your firewall? [ ] Yes [ ] No
Which ports? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please return to your completed survey to Wayne via email (wjoubert@mcrcsip.org) or snail mail (417 Seymour, Suite 2, Lansing, MI 48933) by August 10

Thank you!