Request for Proposal for Comprehensive Cybersecurity Assessment for Meramec Regional Planning Commission
Proposals must be received by: February 2, 2026, by Noon

Objective

Meramec Regional Planning Commission (hereafter known as "MRPC") is requesting proposals for a comprehensive cybersecurity assessment that will assess current status and make suggestions on enhancements to MRPC's cybersecurity protocols and data safety.

1. Map MRPC Assets
2. Identify Security Threats & Vulnerabilities
3. Determine & Prioritize Risks
4. Analyze & Develop Security Controls
5. Document Results from Risk Assessment in a Detailed Report
6. Create a Action Plan to Reduce Risks

MRPC is a regional planning commission serving Crawford, Dent, Gasconade, Maries, Osage, Phelps, Pulaski and Washington counties with various federal and state planning activities, grant administration, economic and community development programs, administration of the HUD Choice Voucher program and other grant funded activities. Because of this, MRPC serves as a hub of information concerning the cities and counties in our eight-county region and must take our cybersecurity seriously to prevent any breaches. Currently, MRPC operates a staff of 24. This requires 20+ Dell Desktop computers and two MAC systems, 28 VOIP phones, 24 Microsoft 365 work accounts that include emails attached to the meramecregion.org domain and an onsite server that has a double redundancy with cloud backup. Our internal network is maintained by a third-party IT company. MRPC also maintains three websites meramecregion.org, naturallymeramec.org and Ozarkrivers.org (the Ozark Rivers Solid Waste Management District's site that MRPC is the current administrator for the district). The company also has social accounts on Facebook for MRPC, Naturally Meramec and Ozark Rivers, as well as, an MRPC account on X, YouTube and LinkedIn.

Scope of Work

Asset Identification and Classification:

- Detailed inventory of all critical information assets (systems, applications, data, intellectual property) with categorization based on sensitivity and business impact.
- Assessment of asset locations, access controls, and data flow.

Threat Identification and Analysis:

- Evaluation of current threat landscape, including internal and external threats (malware, phishing, social engineering, insider threats, etc.).
- Analysis of potential threat vectors and likelihood of occurrence.

Vulnerability Assessment:

- Comprehensive vulnerability scanning of all network devices, systems, and applications.
- Identification of critical vulnerabilities and potential exploitation pathways.
- Prioritization of vulnerabilities based on severity and risk.

Impact Analysis:

- Assessment of potential impact of identified vulnerabilities on business operations, reputation, financial stability, and compliance.
- Calculation of potential financial loss and data breach consequences.

Risk Assessment and Prioritization:

- Calculation of risk scores by considering threat likelihood and impact severity for each identified vulnerability.

- Development of a prioritized list of cyber risks based on risk potential and business criticality.

Security Control Evaluation:

- Review of existing security controls and their effectiveness in mitigating identified cyber risks.
- Assessment of security policies, procedures, and compliance with industry standards (e.g., NIST, PCI DSS, HIPAA).

Reporting and Action Plan:

- Detailed report outlining identified risks, prioritized mitigation strategies, and action plan.
- Recommendations for security control improvements, including technology upgrades, policy updates, and training programs.
- Provide a detailed assessment report including risks and recommendations for future improvements including prioritization and budget estimates for recommended improvements in order to ensure a secure cyber and data environment. Recommendations must be structured as projects/action items for ease of execution, including a prioritization of the action items into high, medium and low categories based on the needs assessment.

Deliverable: Detailed report (4 hard-copy and one electronic) detailing above findings and action items.

Funding for this project is provided through the Missouri Department of Public Safety State and Local Cybersecurity Grant Program that aims to assist state, local, and territorial governments with managing and reducing systemic cyber risk. MRPC has $12,800 to hire a consultant to complete the cybersecurity assessment. The assessment should be completed by June 30, 2026.

MRPC is looking for a firm with the following qualifications and expertise:

- Proven experience in conducting comprehensive cyber risk assessments for organizations of similar size and complexity.
- Certified cybersecurity professionals (e.g., CISSP, CISA, CISM, OSCP) on the team.
- Demonstrated knowledge of industry-standard methodologies and frameworks (NIST, ISO 27001, etc.).
- Expertise in vulnerability scanning tools and techniques.

Bid proposals should provide the following items:

- Cost to accomplish scope of work, including any potential additional costs for customized services. Please identify issues with scope of work which would delay the project or increase cost.
- Detailed project plan outlining methodology, timeline, and deliverables. Please provide details on how much on-site time will be required to accomplish work.
- Team composition with relevant qualifications and experience.
- References from previous clients with similar assessment scope.
- Sample assessment report for most recent client. (Can be sent electronically.)

Proposals will be evaluated based on the following:

- Cost to complete the scope of work
- Technical expertise and understanding of cyber risk assessment methodologies.
- Ability to tailor the assessment to our specific business needs and industry regulations.
- Clear communication and reporting capabilities.
- Project management skills and timely delivery.

MRPC reserves the right to reject any or all bids.

Submission Instructions:

Please submit your proposal by Feb. 2, 2026, by noon to cjones@meramecregion.org.

Contact Information

All questions concerning the project and Request for Proposals can be directed to:
Caitlin Jones, Marketing Communications Manager
4 Industrial Drive, St. James, MO 65559
573-265-2993, Ext. 125 | cjones@meramecregion.org