Request for Proposals (RFP)

Managed IT Services for Emergency Communications Center

1. Introduction

The Greenbrier County Commission is soliciting proposals from qualified Managed Service Providers (MSPs) to provide comprehensive IT support services for its Emergency Communications Center (ECC) located at 173 Arbuckle Lane, Maxwelton, WV 24957. The selected provider will be responsible for supporting and maintaining mission-critical infrastructure and ensuring the security and continuity of IT operations that directly support emergency dispatch and public safety communications.

Any work proposed to be performed in addition to the vendor's written proposal must be approved in advance by the Greenbrier County Commission or its authorized agent.

2. Background

The Greenbrier County Emergency Communications Center (ECC) is a Public Safety Answering Point (PSAP) responsible for providing 24/7 emergency dispatch and communications services to public safety agencies within Greenbrier County, West Virginia. The ECC relies on a variety of mission-critical systems and technologies to support emergency call handling, dispatch, and data services.

To ensure the availability, security, and performance of these systems, the ECC maintains a robust IT infrastructure that includes a virtualized server environment, backup and disaster recovery systems, endpoint protection, and secure network connectivity. The ECC also integrates with various third-party public safety platforms and software providers.

The ECC is seeking a qualified Managed Service Provider (MSP) to deliver comprehensive support for its core IT infrastructure, supplement in-house IT staff, and ensure alignment with cybersecurity best practices. The selected MSP will be expected to provide services in compliance with applicable APCO, NENA, and MS-ISAC guidelines to ensure operational integrity, public safety interoperability, and cybersecurity readiness.

3. Scope of Services

The selected Managed Service Provider (MSP) will be responsible for the monitoring, maintenance, and support of the Emergency Communications Center's mission-critical IT infrastructure, including:

3.1 Network Infrastructure

- Support and maintenance of the ECC's existing IP-based network, which includes approximately 50 networked devices across multiple secured VLANs, as well as around 100 client VPN users, including firewalls, switches, and routers
- Network performance monitoring, optimization, and security to ensure high availability for mission-critical communications
- Documentation of network topology and configurations, including regular updates to reflect any infrastructure changes

3.2 Virtualized Server Infrastructure

- Management of the ECC's VMware-based virtual server environment (or propose compatible alternative with justification and migration plan)
- Proactive server performance tuning, availability monitoring, and optimization
- Detailed patch management strategy, including scheduled patch cycles, emergency patch deployment, impact assessment, testing procedures, and rollback plans
- Coordination of high-availability, failover, and redundancy configurations

3.3 Backup and Replication (BAR) Services

- Administration of the ECC's Veeam Backup & Replication system, which includes local backups to on-site storage and long-term retention to an S3-compatible cloud storage service (e.g., Wasabi or equivalent) with immutable backup configuration to protect against accidental or malicious deletion
- Backups are configured for daily incremental backups with weekly fulls, retained for a minimum of 30 days locally and up to 1 year in offsite cloud storage
- Daily monitoring and alerting on backup success/failure with defined escalation procedures
- Regular backup verification (at least twice per year) and disaster recovery testing at least twice per year, including simulated recovery scenarios
- Rapid response support for file-level and full-system data recovery needs

3.4 Endpoint Protection

- Deployment and management of antivirus/antimalware protection on all servers, workstations and supported devices
- Centralized management and alerting for endpoint threats
- Support for secure VPN access and MFA for remote users
- CJIS-compliant security practices

3.5 SMTP Mail Relay Services

- Provide and maintain reliable SMTP mail relay services for system-generated notifications (e.g., backups, alerts)
- Ensure deliverability and log access for auditing purposes
- Configuration assistance for integrating with existing systems

3.6 Remote Monitoring and Management (RMM)

- Provide and maintain RMM software for real-time monitoring of endpoints and servers
- Patch management, scripting, and automated remediation capabilities
- Alerting and reporting for CPU, disk, network, and memory utilization
- Secure remote access for support personnel
- Establish clear procedures for event response, including:
  - Immediate acknowledgment of alerts within defined SLA timeframes
  - Categorization and prioritization of events based on severity and potential impact on mission-critical systems
  - Automated or manual initiation of remediation steps for common issues
  - Escalation protocols to ECC staff or vendors for incidents beyond MSP scope
- Documentation and reporting of incident response activities and resolutions

3.7 General Support and Incident Response

- Provide 24/7 on-site support for emergency outages affecting mission-critical systems
- Supplement in-house IT staff with support during business hours for non-critical systems, projects, or routine maintenance
- On-site response for escalated or critical incidents as needed
- Proactive system monitoring and reporting aligned with agreed-upon SLAs
- Act as liaison with third-party vendors to assist with issue resolution and system coordination

3.8 Cybersecurity and MS-ISAC Compliance

- Ensure all cybersecurity practices align with the recommendations and standards set by the Multi-State Information Sharing & Analysis Center (MS-ISAC)
- Participate in or support ECC's participation in MS-ISAC services, including:
  - Albert sensor integration and monitoring (if applicable)
  - Malware Information Sharing Platform (MISP) and threat intelligence feeds
  - Security advisories and vulnerability notifications

- Implement security hardening measures in accordance with MS-ISAC guidelines
- Provide incident detection and response capabilities, including threat containment, analysis, and recovery
- Conduct or support periodic vulnerability scans and security audits
- Maintain documentation of cybersecurity controls and incident response procedures

3.9 CJIS Security Compliance

- Vendor must ensure all assigned staff complete and maintain current CJIS Security Awareness Training in accordance with FBI CJIS Security Policy
- Vendor will be required to provide documentation of compliance for all assigned personnel annually, or upon request
- Vendor must provide names for all personnel with access to the ECC systems requiring CJIS compliance, and update this list promptly upon any changes

4. Proposal Requirements

Proposals must include the following components to be considered complete:

- Executive summary outlining the vendor's understanding of the scope and approach to service delivery
- Company background, years in business, and organizational structure
- Detailed description of proposed services, tools, and methodologies (including RMM, endpoint protection, and cloud backup solutions)
- Staffing model and bios of key personnel assigned to the account
- Demonstrated experience supporting public safety or 911 environments
- Experience supporting or aligning with MS-ISAC cybersecurity standards, including any existing partnerships, tool integrations, or incident response support
- Description of processes in place to maintain CJIS security clearances and training for assigned personnel
- References from at least three organizations of similar size and/or complexity, preferably within government or public safety
- Proposed pricing structure (e.g., flat-rate, time and materials, tiered)
- Sample Service Level Agreement (SLA) with expected response and resolution times
- Description of onboarding and transition process from the current MSP (if applicable)
- An annual contract amount for performing all of the services outlined in Section 3 – Scope of Services.

- Vendors must be properly registered and in good standing with the WV Secretary of State, WV State Tax Department, as applicable, and any other entities as necessary. Each of these entities has different fees that may be applicable to their respective registration requirements.

5. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

Criteria	Description	Weight
Technical Approach	Quality of proposed services, tools, and understanding of ECC's IT environment and requirements	30%
Experience and References	Relevant experience supporting 911/public safety agencies and quality of references	25%
Security and Compliance	Adherence to cybersecurity best practices (MS-ISAC) and CJIS requirements, including staff clearances	20%
Support and Responsiveness	Availability of 24/7 outage support and ability to provide timely on-site assistance	15%
Pricing and Value	Overall cost and value of services relative to scope and quality offered	10%

6. Submission Instructions

- All Proposals must be submitted in accordance with the provisions of these instructions and the Solicitation. Failure to do so will result in the disqualification of a Vendor's proposal.
- Vendors must be properly registered and in good standing with the WV Secretary of State, WV State Tax Department, as applicable, and any other entities as necessary. Each of these entities has different fees that may be applicable to their respective registration requirements.
- Questions regarding this RFP should be directed to Kelly Banton via email at: kelly.banton@greenbriercounty.net.
- To be considered, proposals must include the following:
    - Signed Proposal Form;
    - Copy of a Certificate of Good Standing from the West Virginia Tax Division;
    - Verification of General Liability Insurance in the amount of $1,000,000; and

    - Acceptance of the Addendum to Vendor's Standard Contractual Terms.
- If accepted, the Vendor's Proposal, together with this Request for Proposals and County Addendum shall become the terms of an enforceable contract between the County Commission and the Vendor.

All proposals must be mailed or hand-delivered in a sealed envelope clearly marked **"ECC Managed Services RFP"** no later than **Wednesday, June 18, 2025, at 4:00 PM EDT** to:

Kelly Banton
Greenbrier County Commission
912 Court St N
Lewisburg, WV 24901

Electronic submissions will not be accepted. Late submissions will not be considered. All Notices to the Vendor shall be made to the address supplied to the Vendor or its agent as registered with the WV Secretary of State.