REQUEST FOR PROPOSAL (RFP)
RFP #2026-19
24/7 CYBERSECURITY MONITORING, PATCH MANAGEMENT, AND CYBER NETWORK MONITORING SERVICES
JASPER COUNTY, SOUTH CAROLINA
JUNE 4, 2026

---

1. INTRODUCTION

1.1 Purpose

Jasper County Government ("County") is soliciting sealed proposals from qualified cybersecurity managed service providers (MSPs), managed security service providers (MSSPs), or cybersecurity consulting firms to provide comprehensive **24/7 cybersecurity monitoring, cyber network monitoring, patch management, incident response support, and compliance-related cybersecurity services** until **Wednesday, July 1, 2026, at 1:00 p.m**. at which time the names of the Proposers will be publicly read aloud in the Jasper County Council Chamber.

The County seeks a vendor partner capable of leveraging the County's existing cybersecurity and IT infrastructure, tools, and software platforms while enhancing the County's overall cybersecurity posture. The selected vendor should provide continuous monitoring, proactive threat detection, vulnerability management, patch management, incident response coordination, reporting, and audit support.

Additionally, the selected vendor shall be responsible for assisting with and completing all required NCIC, CJIS, and South Carolina Law Enforcement Division (SLED) cybersecurity audits, compliance reviews, documentation, and reporting requirements applicable to Jasper County Government.

---

2. BACKGROUND

Jasper County Government operates a diverse technology environment supporting county administration, public safety, emergency services, judicial systems, public works, finance, GIS, and other county operations. The County maintains cybersecurity tools and software currently in place and desires a cybersecurity partner capable of integrating with and utilizing existing systems wherever feasible.

The County's primary goals include:

- Enhancing cybersecurity visibility and protection
- Providing continuous 24/7 monitoring and alerting
- Reducing cybersecurity risk exposure
- Improving incident response readiness

- Maintaining compliance with CJIS, NCIC, SLED, and applicable state and federal cybersecurity standards
- Strengthening vulnerability and patch management processes
- Ensuring operational continuity and cybersecurity resilience

---

3. SCOPE OF SERVICES

The selected vendor shall provide the following services at a minimum.

3.1 24/7 Security Operations Center (SOC) Monitoring

Vendor shall provide continuous 24 hours per day, 7 days per week, 365 days per year cybersecurity monitoring services.

Services shall include:

- Continuous monitoring of network traffic, endpoints, servers, firewalls, switches, routers, and security devices
- Monitoring of security events, alerts, and logs
- Threat detection and correlation analysis
- Real-time alerting and escalation procedures
- Detection of ransomware, malware, unauthorized access attempts, and suspicious activity
- Continuous review of security telemetry and threat indicators
- Identification and triage of critical cybersecurity incidents
- Threat intelligence integration
- Continuous monitoring of cloud-based systems and services where applicable
- Security event management and reporting
- Security log review and analysis
- Security alert prioritization and escalation

Vendor shall provide documented escalation procedures and incident notification timelines.

3.2 Cyber Network Monitoring

Vendor shall provide comprehensive cyber network monitoring services for the County's IT infrastructure.

Services shall include:

- Network traffic analysis
- Internal and external network monitoring
- Firewall monitoring and rule review
- Intrusion detection and prevention monitoring
- Unauthorized device detection

- Network anomaly detection
- Bandwidth and suspicious communication monitoring
- Monitoring for lateral movement within the network
- DNS monitoring and analysis
- VPN monitoring
- Remote access monitoring
- Monitoring of privileged accounts and administrative access
- Continuous health monitoring of cybersecurity systems

Vendor shall provide recommendations for improving network security architecture where vulnerabilities or weaknesses are identified.

3.3 Patch Management Services

Vendor shall provide comprehensive patch management services utilizing the County's existing software and patch management tools whenever feasible.

Services shall include:

- Operating system patch management
- Third-party software patch management
- Firmware update management
- Security update testing and validation
- Critical vulnerability remediation
- Patch deployment scheduling and coordination
- Emergency patch deployment for critical threats
- Patch compliance reporting
- Vulnerability prioritization
- Documentation of applied patches and remediation activities
- Verification and validation of successful patch deployment

Vendor shall maintain procedures to minimize operational disruption while ensuring timely remediation of vulnerabilities.

3.4 Vulnerability Management

Vendor shall provide ongoing vulnerability management services.

Services shall include:

- Routine vulnerability scanning
- Internal and external vulnerability assessments
- Vulnerability prioritization based on risk
- Remediation recommendations
- Validation of remediation efforts

- Reporting of critical vulnerabilities
- Risk scoring and tracking
- Assistance with remediation planning
- Coordination with County IT staff

Vendor shall provide monthly vulnerability assessment summaries and remediation status reports.

3.5 Incident Response Services

Vendor shall provide incident response support services.

Services shall include:

- Incident detection and analysis
- Incident containment recommendations
- Threat eradication support
- Recovery assistance
- Root cause analysis
- Incident documentation
- Forensic coordination support
- Coordination with County IT staff and leadership
- Escalation procedures for critical incidents
- After-action reporting and recommendations

Vendor shall provide emergency contact procedures and escalation paths available 24/7.

3.6 Existing Tools and Software Integration

The County intends to maintain and continue utilizing existing cybersecurity and IT management tools where operationally feasible.

Vendor shall:

- Assess and integrate with the County's existing cybersecurity tools
- Utilize existing monitoring, logging, and endpoint solutions whenever possible
- Minimize unnecessary replacement of existing systems
- Provide recommendations only where improvements are necessary
- Identify any required licensing or integration costs
- Coordinate with County IT staff regarding compatibility and implementation

Vendor shall clearly identify:

- Tools currently supported
- Additional tools proposed

- Any required software changes
- Any additional hardware requirements
- Any licensing dependencies

3.7 Compliance and Audit Support

The selected vendor shall be responsible for supporting and completing cybersecurity-related audits and compliance requirements applicable to Jasper County Government.

This includes, but is not limited to:

- NCIC audit preparation, management, and support
- SLED cybersecurity audit support and completion
- CJIS audit preparation, compliance support, and documentation management
- CJIS Security Policy compliance assistance
- Security documentation maintenance
- Policy and procedure review assistance
- Audit evidence collection and preparation
- Remediation planning for audit findings
- Compliance reporting
- Coordination with state and law enforcement entities as required
- Assistance with cybersecurity risk assessments
- Documentation necessary for compliance reviews

Vendor must demonstrate familiarity with:

- NCIC requirements
- CJIS Security Policy
- South Carolina state cybersecurity requirements
- SLED audit expectations
- Government cybersecurity best practices
- Law enforcement system security requirements

Vendor shall assume primary responsibility for completing all required cybersecurity audit deliverables under the scope of this contract.

3.8 Reporting Requirements

Vendor shall provide detailed reporting including:

- Weekly cybersecurity briefing reports summarizing incidents, vulnerabilities, remediation activities, patching status, and threat activity
- Weekly status meetings or virtual briefings with County IT leadership as requested
- Comprehensive monthly executive cybersecurity reports
- Incident summaries

- Patch compliance reports
- Vulnerability remediation status reports
- Threat activity summaries
- Security event metrics
- Compliance and audit status updates
- Recommendations for cybersecurity improvements
- Quarterly cybersecurity posture reviews
- Audit readiness and compliance status reporting for NCIC, CJIS, and SLED requirements

Vendor shall also provide immediate notification for critical cybersecurity incidents.

---

4. VENDOR QUALIFICATIONS

Vendors responding to this RFP must demonstrate the following minimum qualifications:

4.1 Organizational Qualifications

- Minimum of five (5) years providing managed cybersecurity services
- Experience supporting local government or public sector clients
- Experience supporting CJIS/NCIC environments preferred
- Demonstrated experience providing 24/7 SOC services
- Demonstrated experience with patch management and vulnerability management
- Demonstrated incident response capabilities

4.2 Staffing Qualifications

Vendor shall provide qualified personnel with appropriate cybersecurity certifications, including but not limited to:

Vendor must provide at least one dedicated onsite cybersecurity support resource a minimum of (4) days per week at Jasper County Government facilities. The onsite resource shall coordinate directly with County IT staff, assist with cybersecurity operations, support incident response activities, assist with audit preparation and compliance activities, participate in meetings, and provide hands-on support for remediation and cybersecurity initiatives.

- CISSP
- CISM
- Security+
- CEH
- GIAC certifications
- Microsoft certifications
- Network security certifications

Vendor shall identify:

- Onsite support personnel assigned to Jasper County Government
- Proposed onsite support schedule
- Key personnel
- Escalation contacts
- SOC staffing model
- On-call procedures
- Technical support structure

---

5. TECHNICAL REQUIREMENTS

Vendor shall describe:

- SOC capabilities and locations
- Monitoring platforms utilized
- SIEM capabilities
- Threat intelligence sources
- Incident response processes
- Vulnerability scanning tools
- Patch management methodologies
- Security reporting capabilities
- Escalation procedures
- Service availability commitments
- Integration capabilities with existing systems

Vendor shall describe how services will be delivered with minimal operational disruption, including coordination between remote SOC operations and the required onsite support personnel.

---

6. SERVICE LEVEL REQUIREMENTS

Vendor shall provide proposed Service Level Agreements (SLAs), including:

Severity Level	Response Time	Escalation Requirement
Critical Security Incident	Within 15 minutes	Immediate escalation
High Severity Incident	Within 1 hour	Escalation to County IT
Medium Severity Incident	Within 4 hours	Standard escalation
Low Severity Incident	Within 1 business day	Routine notification

Vendor shall describe:

- Alert notification procedures
- Incident escalation process
- Remediation coordination
- Availability guarantees
- Reporting timelines

---

7. PROPOSAL REQUIREMENTS

Proposals shall include the following:

7.1 Executive Summary

Provide a summary of the vendor's understanding of the project and proposed solution.

7.2 Company Profile

Include:

- Company history
- Years in business
- Office locations
- Relevant experience
- Public sector experience
- Government references

7.3 Technical Approach

Describe:

- Proposed monitoring approach
- SOC operations
- Cybersecurity technologies utilized
- Patch management methodology
- Vulnerability management process
- Incident response procedures
- Compliance support approach
- Integration with existing County tools

7.4 Staffing Plan

Provide:

- Organizational chart
- Assigned personnel
- Relevant certifications
- Escalation contacts
- Support structure

7.5 References

Provide at least three (3) references for similar government or public-sector engagements.

7.6 Pricing Proposal

Provide detailed pricing including:

- Monthly recurring costs
- One-time implementation costs
- Licensing costs
- Optional services
- Hourly rates for additional services
- Audit support costs
- Incident response costs if separate

Pricing shall remain valid for a minimum of 120 days.

---

8. CONTRACT TERM

The County anticipates entering into an agreement for an initial term of three (3) years with optional renewal periods subject to County approval.

---

9. INSURANCE REQUIREMENTS

The successful Proposer shall be required to provide proof of insurance in the following amounts.

1. Workers' Compensation - The vendor shall provide coverage for its employees with statutory workers' compensation limits, and no less than $1,000,000.00 for Employers' Liability. Said coverage shall include a waiver of subrogation in favor of the Owner and its agents, employees, and officials.

2. Commercial General Liability - The vendor shall provide coverage for all operations including, but not limited to Contractual, Products and Completed Operations, and Personal Injury. The limits shall be no less than $1,000,000.00, per occurrence, with a $2,000,000.00 aggregate.

3. Business Automobile Liability - The vendor shall provide coverage for all owned, non-owned and hired vehicles with limits of not less than $1,000,000.00, per occurrence, Combined Single Limits (CSL) or its equivalent.

4. Professional Liability / Errors and Omissions Insurance

5. Cyber Liability Insurance

---

10. CONFIDENTIALITY AND DATA SECURITY

Vendor shall:

- Maintain confidentiality of County data
- Comply with all applicable laws and regulations
- Ensure secure handling of sensitive information
- Maintain CJIS compliance where applicable
- Ensure background checks for applicable personnel
- Execute confidentiality agreements if required

Vendor personnel accessing CJIS or NCIC systems may be required to undergo background screening and comply with all applicable security requirements.

---

11. EVALUATION CRITERIA

Proposals will be evaluated based on, but not limited to, the following criteria:

Criteria	Weight
Relevant Experience and Qualifications	25%
Technical Approach and Solution	30%
Government and CJIS/NCIC Experience	15%
Pricing and Cost Effectiveness	20%
References and Past Performance	10%

The County reserves the right to request interviews, demonstrations, or additional information from vendors.

---

12. COUNTY RIGHTS

Jasper County Government reserves the right to:

- Reject any or all proposals
- Waive informalities or irregularities
- Request clarification of proposals
- Negotiate with selected vendors
- Cancel or modify this RFP at any time
- Award contracts in the best interest of the County

---

13. SUBMISSION INSTRUCTIONS

Proposal Instructions

Proposals should be typed on company letterhead or on a document which provides the Vendor's name, address, phone number, and other pertinent contact information, and reference "**24/7 Cybersecurity RFP #2026-19**." An original and five copies of the Proposal should be submitted.

The successful Vendor will be required to furnish an Internal Revenue Form W-9, all appropriate business licenses, and all required insurances.

Proposal Submission Method and Deadline

To be deemed "received," the Proposal may be submitted electronically through the County's vendor registration webpage to ensure that it remains sealed until the scheduled Proposal opening date and time. A link to the County's vendor registration webpage may be found under Proposals & Solicitations, on the County's website at www.jaspercountysc.gov/services/bids-and-solicitations/.

The Proposal may also be submitted via mail or hand delivered in a sealed envelope to the address below with "**24/7 Cybersecurity RFP #2026-19**" written on the outside of the envelope. It must be received no later than **1:00 p.m. on Wednesday, July 1, 2026**. Vendors choosing to submit a hard copy should submit an original and five copies. Any Proposals submitted or delivered after the above time will **NOT** be accepted under any circumstances. Proposals submitted by email will **NOT** be accepted.

The Proposal can be mailed or hand delivered to:

Kimberly Burgess, Dir., Administrative Services
Jasper County Government Building
358 Third Avenue, Suite 304
PO Box 1194
Ridgeland, SC 29936

The Proposal name reading will take place in the Jasper County Council Chamber located at:

Clementa C. Pinckney
Jasper County Government Building
358 3rd Avenue, Third Floor
Ridgeland, SC 29936

Questions Regarding the RFP

All questions regarding this RFP shall be submitted in writing to:

Lekisha Brown
Deputy Director
Information Technology
252 Russell St.
Ridgeland, SC 29936
labrown@jaspercountysc.gov

Any questions regarding this Proposal must be submitted in writing via email to labrown@jaspercountysc.gov or through the vendor registration portal located on Jasper County's Proposals and Solicitations webpage, https://www.jaspercountysc.gov/services/bids-and-solicitations/ **NO LATER** than **Monday, June 22, 2026, by 5:00 pm**.

All submitted questions will be addressed and posted on Jasper County's Proposals and Solicitations webpage and the vendor registration portal end of day **Wednesday, June 24, 2026**.

14. CONCLUSION

Jasper County Government seeks a qualified cybersecurity partner capable of delivering proactive, responsive, and comprehensive cybersecurity monitoring and management services while leveraging the County's existing technology investments.

The selected vendor must demonstrate strong technical capabilities, public sector experience, compliance expertise, and the ability to support NCIC, CJIS, and SLED cybersecurity requirements as part of an ongoing cybersecurity partnership.

All Proposals will remain subject to acceptance for sixty (60) days after the day of the Proposal reading. Jasper County (the Owner) reserves the right to cancel this solicitation, or all Proposals may be rejected, including without limitation, the right to reject any or all nonconforming, non-responsive, unbalanced, or conditional Proposals. The Owner also reserves the right to waive all informalities not involving price, time, or changes in the Work and to negotiate contract terms with the successful Proposer.