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

ADDENDUM #1
QUESTIONS AND ANSWERS

QUESTION 1 – Subcontract onsite

Hi, would proposal be accepted without onsite support but subcontracted out?

ANSWER 1 – No, onsite support is a requirement.

QUESTION 2 – Licensing and Additional Questions

Hello, I have a few questions I'd like to ask before submitting a formal bid.

1. How many endpoints, servers, users, firewalls, network devices, and sites are in scope?
2. What EDR, SIEM/logging, vulnerability scanning, and patch management tools are currently in use?
3. Does the County already own licenses for these tools, or should vendors include licensing?
4. Is the onsite resource required every week for the full contract term?
5. Are after-hours onsite responses expected, or can critical response be remote unless requested?
6. What CJIS/NCIC/SLED audit deadlines or known findings are currently active?
7. Should pricing assume unlimited incident response, or should major incident response be priced separately?

Please let me know if you need clarification.

ANSWER 2 –

1. Endpoints 630, servers 135, users 435, firewalls 41, network devices 140, and yes.
2. We do have an EDR+MDR. Scanning tools are available patching tools.
3. The County already owns licenses.
4. It is required every week for the term of the contract.
5. Onsite when necessary.
6. There are none pending.
7. All pricing should include incident.

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

QUESTION 3 – Clarifying Questions

Onsite staffing (Section 4.2). The RFP requires at least one dedicated cybersecurity resource onsite a minimum of four (4) days per week.

1. Will the County consider a hybrid delivery model — a primary 24/7 remote Security Operations Center paired with a named onsite resource present on a reduced or scheduled cadence (for example, one to two days per week plus incident-driven and audit-period onsite presence)?
2. If a strict four-day onsite minimum is required, may that resource be a qualified, locally based subcontractor working under the prime vendor's direction? CJIS / NCIC / SLED compliance (Section 3.7).
3. For the required compliance and audit support, does the County expect the vendor to hold a specific certification or authorization, or is demonstrated familiarity with the CJIS Security Policy together with a documented compliance methodology sufficient at proposal stage?
4. Will the County's current CJIS/NCIC documentation and audit history be made available to the selected vendor? Existing tools (Section 3.6).
5. Can the County provide a list of the cybersecurity, monitoring, logging, and endpoint tools currently in place, so vendors can scope integration accurately? References (Section 7.5).
6. The RFP requests three references for similar government or public-sector engagements. Where directly relevant to this scope, will the County also consider references from regulated commercial environments (for example, HIPAA-regulated healthcare technology)? Submission method (Section 13).
7. Please confirm that an electronic submission through the County's vendor registration portal fully satisfies the submission requirement in lieu of original and five (5) printed copies.

ANSWER 3 –

1. No, the County will not consider a hybrid solution. The RFP is written as full time employee onsite.
2. Yes.
3. Yes.
4. Yes.
5. Yes
6. Yes
7. Please follow RFP requirements.

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

QUESTION 4 – Could you provide the following information for me?

- Number of Sites Managed-
- Number of Users-
- Number of Computers/Workstations-
- Number of Servers-
- Number of Firewalls-
- Number of Mobile Devices-
- Total Terabytes of Data Being Backed Up

ANSWER 4 –

- Number of Sites Managed- about 100
- Number of Users- 435
- Number of Computers/Workstations- 630
- Number of Servers- 135
- Number of Firewalls- 41
- Number of Mobile Devices- 160
- Total Terabytes of Data Being Backed Up- 300TB

QUESTION 5 – Does the County already own a SIEM solution?

a. If so, which SIEM solution?

ANSWER 5 – Yes, Datto and Kaseya

QUESTION 6 – Current Cybersecurity Environment

Can the County provide an inventory of its current cybersecurity and IT infrastructure, including existing SIEM, endpoint protection, vulnerability management, patch management, firewall, logging, monitoring, and cloud security tools currently in use?

ANSWER 6 – Yes

QUESTION 7 – Scope and Asset Counts

Can the County provide estimates regarding the number of users, workstations, laptops, servers, network devices, firewalls, cloud environments, remote users, and physical locations that will fall within the scope of monitoring and patch management services?

ANSWER 7 – Over 1000

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

QUESTION 8 – Existing Support Structure

Which cybersecurity functions are currently performed by County IT staff and/or incumbent vendors, and which functions are expected to transition to the selected contractor under this engagement?

ANSWER 8 – We perform patching, updates, campaigns, scans, etc. The functions to be transitioned are TBD upon award.

QUESTION 9 – CJIS, NCIC, and SLED Compliance Support

Can the County provide additional details regarding the current compliance posture, frequency of audits, outstanding findings (if any), and the specific audit-related deliverables for which the selected vendor will be expected to assume primary responsibility?

ANSWER 9 – Yes, this information can be provided.

QUESTION 10 – Dedicated Onsite Resource Requirement

The RFP requires at least one dedicated onsite cybersecurity support resource four days per week. Can the County clarify the expected work hours, primary responsibilities, work location(s), and whether this resource must be exclusively dedicated to Jasper County?

ANSWER 10 – The hours expected are 7am-5pm, 4 days a week at the IT Department. The resource must be exclusively dedicated to the County. Primary responsibilities will be discussed once awarded.

QUESTION 11 – Incumbent Contractor and Historical Metrics

1. Is there an incumbent provider currently supporting these services?
2. If so, can the County share any historical operational metrics, such as average monthly alert volume, incident volume, vulnerability findings, or patch compliance statistics, that may assist vendors in appropriately sizing and pricing their proposed solutions?

ANSWER 11 –

1. No, there currently is no incumbent provider.
2. N/A

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

QUESTION 12 – Resume Requirements

The RFP requests information regarding assigned personnel, certifications, escalation contacts, and support structure.

1. Can the County clarify whether resumes are required as part of the proposal submission?
2. If so, should resumes be provided for all proposed personnel, only key personnel, the dedicated onsite resource, or other specifically designated positions?

ANSWER 12 –

1. Yes. The resumes should contain a brief history of work.
2. Provide a resume for the company and for the dedicated onsite resource.

QUESTION 13 – Dedicated Onsite Resource Requirement

The RFP requires at least one dedicated onsite cybersecurity support resource, a minimum of four (4) days per week. Can the County clarify:

a. The expected work hours, primary responsibilities, and work location(s) for the onsite resource;

b. Whether the onsite resource must be a resident of Jasper County or the State of South Carolina;

c. Whether the resource must be exclusively dedicated to Jasper County; and

d. Whether travel-related costs (e.g., mileage, lodging, per diem, or other travel expenses) associated with onsite support should be included in the proposed pricing or will be reimbursed separately by the County.

ANSWER 13 –

a) The hours expected are 7am-5pm, 4 days a week at the IT Department
b) The onsite resource does not need to be a resident of Jasper County or South Carolina
c) Yes, they must be exclusively dedicated to Jasper County
d) Travel related costs should be included in the proposal.

QUESTION 14 – Pricing Clarification

Should the pricing be a separate proposal or included?

ANSWER 14 – Included in the fee schedule

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

QUESTION 15 – Bid Submittal
2. Just to confirm, we can submit our proposal online through Bidnet, correct?
ANSWER 15 – Yes, before the closing date and time.

QUESTION 16 – Budget Question
Do you have a budget for these services?
ANSWER 16 – No

QUESTION 17 – Service Provider
What is most important to you in your next service provider?
ANSWER 17 – Reliable, ability to fulfill goals and complete the tasks.

QUESTION 18 – MBE Consideration
Do you have any minority requirements within Jasper County?
ANSWER 18 – Yes, but not a requirement for this proposal

QUESTION 19 – What is the total number of users in scope?
ANSWER 19 - 435

QUESTION 20 – Please confirm the number of Active Directory user accounts.
ANSWER 20 - 435

QUESTION 21 – What is the total number of workstations, laptops, endpoints, mobile devices, tablets, IoT devices, and specialty devices in scope?
ANSWER 21 – Over 1000

QUESTION 22 – What is the total number of physical, virtual, cloud-hosted, Windows, and Linux servers in scope?
ANSWER 22 – A total of 135 servers.

QUESTION 23 – What is the total number of firewalls, routers, switches, wireless devices, IDS/IPS devices, VPN devices, and other network appliances in scope?
ANSWER 23 – Over 1000

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

QUESTION 24 – How many County facilities, remote locations, branch offices, public safety locations, and other physical sites are included in scope?
ANSWER 24 - About 100

QUESTION 25 – Which departments, business units, and facilities are included in scope?
ANSWER 25 - All Departments

QUESTION 26 – Can the County provide a detailed inventory of endpoints, servers, network devices, cloud workloads, and security appliances?
ANSWER 26 – Yes, when needed.

QUESTION 27 – What is the total amount of data currently being backed up (TB)?
ANSWER 27 - 300 TB

QUESTION 28 – EXISTING CYBERSECURITY & IT TOOLS

1. Can the County provide a complete inventory of cybersecurity and IT management tools currently deployed, including vendor, version, licensing status, and deployment scope?
2. What solutions are currently used for SIEM, EDR, vulnerability management, patch management, network monitoring, RMM, backup/BCDR, email security, identity management, and threat detection?
3. Which tools and licenses are owned by the County versus expected to be provided by the selected vendor?
4. Which tools are expected to remain in place versus potentially being replaced?
5. Does the County utilize a ticketing or ITSM platform and is vendor integration required?

ANSWER 28 –

1. Yes.
2. Vipre MDR and EDR, Datto, Cisco DUO, Cisco Meraki, Veeam, and Proofpoint.
3. We provide our own tools and licenses. We will also be open to purchasing tools where we see need.
4. All
5. No, but it would be nice.

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

QUESTION 29 – SIEM, SOC & MONITORING

1. Does the County currently have a SIEM platform? If so, which solution is in use?
2. What is the current SIEM log ingestion volume (EPS, GB/day, or annual ingest)?
3. Is 24x7x365 SOC monitoring required across all in-scope assets?
4. Which asset types are expected to be monitored?
5. Is the selected vendor expected to utilize existing monitoring platforms or provide additional SOC technologies if current tools are insufficient?
6. What level of monitoring and remediation is expected?

ANSWER 29 –

1. Datto
2. N/A
3. Yes
4. All
5. We have our own, but we are open to options.
6. Complete

QUESTION 30 – CLOUD & MICROSOFT ENVIRONMENT

1. Which cloud platforms and SaaS environments are currently in use?
2. Are cloud workloads and SaaS platforms included within the monitoring scope?
3. What Microsoft licensing model is currently in use?
4. Are Microsoft security capabilities expected to be monitored?
5. Are there any planned Microsoft licensing or cloud platform changes during the contract term?

ANSWER 30 –

1. Just Microsoft
2. We don't have any cloud environment
3. Standard
4. Yes
5. No

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

QUESTION 31 – IDENTITY & ACCESS MANAGEMENT

1. Does the County utilize Active Directory, Entra ID, or a hybrid identity environment?
2. Is MFA enforced across user accounts?
3. Are PAM controls currently in place?
4. How are privileged accounts currently managed?

ANSWER 31 –

1. Active Directory
2. Yes
3. Yes
4. IT, we decide what users need on account.

QUESTION 32 – NETWORK MONITORING & INFRASTRUCTURE

1. What firewall, VPN, network monitoring, and remote access platforms are currently deployed?
2. Is DNS centralized and available for monitoring?
3. Is network performance monitoring required in addition to security monitoring?
4. Is configuration review and rule optimization expected as part of ongoing services?
5. Is a network diagram or topology available?
6. Does the County maintain a CMDB or asset inventory system?
7. How should unauthorized device detection and response be handled?

ANSWER 32 –

1. Cisco Meraki and Splashtop.
2. Yes
3. No
4. Yes
5. Yes
6. Yes
7. N/A

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

QUESTION 33 – PATCH MANAGEMENT & VULNERABILITY MANAGEMENT

1. What patch management platform is currently used?
2. How many assets are included in patch management scope?
3. Does patch management include endpoints, servers, third-party applications, and network device firmware?
4. Are any systems excluded from automated patching?
5. What is the current patch compliance rate?
6. What vulnerability scanning platform is currently used?
7. Should vendors provide vulnerability management tooling and licensing?
8. How frequently should vulnerability scans be performed?
9. How many internal and external assets require scanning?
10. Is remediation validation required after vulnerabilities are addressed?
11. Is the vendor expected to assist directly with remediation?

ANSWER 33 –

1. Datto
2. 565
3. Yes
4. No
5. 94%
6. Nexxus
7. No
8. They are done once monthly
9. All
10. Yes
11. That's why an onsite person is required to be here 4 days a week working 8 to 10 hours a day.

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

QUESTION 34 – INCIDENT RESPONSE

1. What is the County's current incident response process?
2. Does the County maintain a formal Incident Response Plan?
3. What level of incident response responsibility is expected from the selected vendor?
4. Should incident response services be included in recurring fees or priced separately?
5. Are forensic investigation services required?
6. Does the County require tabletop exercises or readiness assessments?
7. For major incidents, should the vendor perform recovery activities or provide advisory support only?
8. How many cybersecurity incidents occurred during the previous 12 months?

ANSWER 34 –

1. Notify management and resolve incidents as they occur.
2. We are currently developing a formal plan.
3. Immediately when an issue occurs or something abnormal is noticed.
4. Yes.
5. No, but if needed, Jasper County will pay for it separately.
6. We have a service in place for this.
7. After notification, the vendor may be asked to provide support which would be provided by the onsite staff that is required 4 days a week.
8. Maybe 3 or 4 but no major issues.

QUESTION 35 – CJIS / NCIC / SLED COMPLIANCE

1. What level of support is expected for CJIS, NCIC, and SLED compliance activities and audits?
2. What is the current compliance status?
3. What audits have been completed during the past three years?
4. When are the next audits scheduled?
5. Are there any open findings, remediation items, corrective action plans, or compliance deficiencies?
6. Will current CJIS/NCIC/SLED documentation, audit reports, findings, and gap assessments be made available?

7. How many CJIS-connected users, devices, terminals, facilities, and departments are in scope?
8. Are vendor personnel required to complete CJIS background checks?
9. Is onsite participation required during audits?
10. Is the vendor expected to lead audit preparation and remediation activities or provide support only?

ANSWER 35 –

1. I expect my onsite person to be able to complete reports and have them in a timely manner.
2. We are currently compliant.
3. CJIS, NCIC, and SLED
4. January 2027
5. Yes, but they are currently being managed and resolved.
6. Yes
7. 125
8. Yes
9. Yes, that will be the job of the onsite personnel that is requested.
10. Yes

QUESTION 36 – ONSITE RESOURCE REQUIREMENTS

1. Is the four-day-per-week onsite requirement mandatory or flexible?
2. Will hybrid delivery models be considered?
3. May the onsite resource be provided through a subcontractor?
4. What facility will serve as the primary onsite location?
5. What working hours are expected?
6. Will workspace and access credentials be provided?
7. Is the onsite resource expected to remain dedicated throughout the contract term?
8. Must the resource be dedicated exclusively to Jasper County?
9. Can multiple qualified personnel rotate through the onsite role?
10. What skills, certifications, and experience levels are expected?
11. Will the County participate in selecting the onsite resource?
12. Will the resource operate under County direction or vendor management?

ANSWER 36 –

1. It is Mandatory.
2. No
3. Yes
4. IT Department Office
5. 7am to 5pm with on-call availability.
6. Yes
7. Yes. If you fail to keep to this requirement, this will be considered violation of the contract and can result in contract termination.
8. Yes, when onsite.
9. Yes, that is fine, but we prefer some consistency and reliability.
10. Basic IT knowledge and cybersecurity with their agency to support advance cybersecurity issues.
11. The county IT Department can assist if desired by the vendor.
12. Both. Jasper County will coordinate with the vendor management to ensure success.

QUESTION 37 – CONTRACT, INCUMBENT & TRANSITION

1. Is there an incumbent provider currently delivering any portion of these services?
2. If so, please provide the incumbent name, contract value, contract period, and scope of services.
3. Is this a new initiative or a continuation/replacement of an existing program?
4. Has the County previously utilized an MSSP or SOC provider?
5. Will a transition and knowledge transfer period be provided?
6. Will documentation, runbooks, network diagrams, inventories, and audit materials be available?
7. What are the anticipated award and project start dates?
8. What are the renewal terms and pricing expectations?

ANSWER 37 –

1. No
2. N/A
3. No
4. Yes
5. Yes
6. Yes
7. End of July
8. 3 to 4 year contract

QUESTION 38 – BUDGET & PRICING

1. Is there an approved budget, estimated budget range, or not-to-exceed amount for this engagement?
2. Has funding already been allocated?
3. Should pricing separate licensing, implementation, and managed services costs?
4. Is the County seeking services only, or services plus software licensing?

ANSWER 38 –

1. No
2. No
3. Yes
4. Services only.

QUESTION 39 – REPORTING & GOVERNANCE

1. What reporting cadence is expected?
2. Are there preferred reporting templates, dashboards, or executive reporting formats?
3. Who is the intended audience for executive reports?
4. Are recurring status meetings expected?

ANSWER 39 –

1. N/A
2. No
3. IT Director, Deputy Director
4. Once a week or bi-weekly meetings

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

QUESTION 40 – REFERENCES & PROPOSAL SUBMISSION

1. Will the County accept references from regulated commercial environments?
2. May anonymized references be submitted during the proposal stage?
3. Does electronic submission fully satisfy proposal submission requirements?
4. Would the County consider extending the proposal due date?

ANSWER 40 –

1. Yes
2. Yes
3. Please follow the requirements of the RFP
4. No

QUESTION 41 – INSURANCE & LEGAL REQUIREMENTS

1. What minimum limits are required for Professional Liability / Errors & Omissions and Cyber Liability Insurance?
2. Are umbrella or excess liability policies acceptable?
3. Are subcontractor insurance policies acceptable?
4. When must the South Carolina business license be obtained?
5. Is a mandatory pre-bid conference or site visit required?

ANSWER 41 –

1. 4 million dollars
2. We will make a determination at the time of award.
3. Both vendor and subcontractor must follow the insurance requirements in the RFP.
4. When bid is awarded. A license is required for the local town and municipality.
5. No

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

QUESTION 42 – BACKUP, BUSINESS CONTINUITY & DISASTER RECOVERY

1. What backup and disaster recovery platform is currently in use?
2. What are the County's documented RTO and RPO requirements?
3. Is backup testing performed regularly and documented?

ANSWER 42 –

1. Veeam
2. RTO acceptable downtime window is 4 hours. RPO acceptable data loss 1 business day.
3. Yes

QUESTION 43 – INTERNAL IT STAFF & SUPPORT MODEL

1. What is the current size and structure of the County IT organization?
2. How many personnel currently support cybersecurity and related operations?
3. Are services currently performed internally, by an MSP, or by an MSSP?
4. What communication and escalation procedures are expected between County IT and the selected vendor?
5. Is the County seeking assistance with non-cybersecurity project work or escalation support?

ANSWER 43 –

1. IT staff consists of 6 employees.
2. 1
3. No
4. Phone call for critical and email for non-critical.
5. No

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

QUESTION 44 – FUTURE STATE, MODERNIZATION & ARCHITECTURE

1. Are there known cybersecurity or infrastructure gaps that vendors should be aware of?
2. Should vendors prioritize leveraging existing technologies whenever possible?
3. Is the County open to replacing or supplementing existing tools?
4. Are there preferred technologies that must be used?
5. Are there planned modernization projects, cloud migrations, platform upgrades, or infrastructure initiatives that may impact scope?
6. Is the desired solution expected to be on-premises, cloud-based, or hybrid?
7. Are any platforms required to remain on-premises?

ANSWER 44 –

1. No
2. Yes
3. If it is justified.
4. Preferred to keep as many paid for resources as possible.
5. Yes
6. On premises.
7. All platforms.