# Bryan County Board of Commissioners

P.O. Box 430 Pembroke Georgia 31321-0430

Phone: (912) 653–5252: Fax: (912) 653-4691

*Carter Infinger, Chairman*
*Noah Covington, District 1*
*Wade Price, District 2*
*Dallas Daniel, District 3*
*Patrick Kisgen Jr., District 4*
*Dr. Gene Wallace, District 5*

*Ben Taylor, County Administrator*
*Kathryn Downs, Asst. County Administrator*
*Lori Tyson, County Clerk*
*Charlene Bunch, Finance Director*
*Kirk Croasmun, County Engineer*
*Riley Johnson, HR Director*

## Request for Proposal (RFP) Addendum

| | |
|---|---|
| RFP Description: | Cybersecurity Services |
| RFP Response Due Date & Time: | Thursday, June 27, 2024, at 2:00 PM |
| Addendum: | 1 |
| Addendum Date: | June 20, 2024 |

RFP Addendum Response to Vendor Questions Submitted Via Email

1. How many copies are required?
   **Per the RFP, 2 copies and 1 soft copy**

2. Can the sealed and labeled envelope be delivered inside a sealed and labeled box? **Yes**

3. Budget Flexibility: Is there any flexibility in the budget to accommodate unforeseen cybersecurity needs or upgrades? **Yes**

4. Will there be an opportunity for a Q&A session or pre-bid meeting to discuss the RFP further?
   **Not this time there is no pre-bid meeting or Q&A session scheduled.**

5. Should the cost proposal include a breakdown of costs for each service component separately? **Yes, please list it separately**.

6. Do you have any local IT staff that are to be involved in the services delivered by the chosen company? If so, how many people will be involved?
   **Yes, we have onsite IT staff who will be involved with the cybersecurity set-up and response. Currently, we have three onsite IT personnel available to assist**.

7. Which type of firewall do you use?
   **We currently use Meraki firewalls.**

8. Which type of network equipment do you use?
   **We use Meraki network equipment.**

9. Do you have one data center, or do you have one in Richmond Hill and one in Pembroke? Or do you have more than one or two?
   **We have two data centers: one in Pembroke and another in Richmond** Hill.

10. Is all of your County data traffic presented on a single core switch?
    **No, each site in Bryan County has its own network. These networks can communicate with each other as needed.**

11. Do you have a network access control (NAC) system? If so, what is it?
    **We utilize the Meraki security appliance for our Network Access Control (NAC) system**.

12. You have about 400 end devices (workstations)--what type of devices and operating systems do you run?
    **The devices are of various brands. All workstations run either Windows 10 Pro or Windows 11 Pro.**

13. Are all of those 400 devices County owned, or do you allow BYOD?
    **Yes, all 400 devices are County-owned. We do not allow BYOD. Personal devices are not permitted on County admin networks, but we do offer guest Wi-Fi for internet access only for those devices or visitors.**

14. What email system do you currently run, and will that email system continue?
    **The County uses Microsoft 365 for our email system and will continue to use it.**

15. How many servers do you maintain? Are they maintained in one place, two places (Pembroke and Richmond Hill), or are they sited in more than two places?
    **The servers are maintained in our two data centers. Currently, the County has 16 servers.**

16. 11. Do you use cloud-based servers (Azure, Google, Amazon, etc.) and if so, how many are there?
    **No, we do not use cloud-based servers.**

17. Do you need protection software installed on the servers as well as on the workstations?
    **Yes, we need protection software installed on both the servers and the workstations**.

18. How many devices are to be monitored with the new SIEM? If you know, how many events/second (EPS) do you expect to collect and report on with your new SIEM?
    **The new SIEM will monitor all devices. We do not currently know the expected events per second (EPS) to be collected and reported**.

19. Do you currently use SIEM? If so, what is it, and why are you seeking to change?
    **Yes, we currently use a SIEM that is monitored by a SOC team as well as Bryan County IT staff.**

20. Is all I.T. infrastructure equipment on the premises and in one building, and if not, then how is the infrastructure laid out?
    **IT equipment is located in various buildings locations throughout the North and South ends of the County.**

21. Does this RFP also include coverage for your buildings and building systems such as elevators, lighting, access controls, etc.?
    **No, this does not include building systems.**

22. What is the term length? **Existing contracts have been in 6-month increments**

23. Do you have any servers that need protection or is this only for user's workstations? If you do have servers, how many? **16 Servers**

24. Did you have network infrastructure that needs protected? (Switches, firewalls, etc)
    **Yes**

25. How long did you need SIEM retention for? (1,3,6,12, and 18 months are available)
    **12 Months**

26. What existing cybersecurity measures and technologies are currently in place?
    **MDR/XDR, SIEM, Email, Intune, Phishing testing/training**

27. Are any particular areas (e.g., endpoint protection, email security) a higher priority? **No**

28. Are there particular areas where you feel your staff needs more training or support? **No**

29. Are there specific third-party applications or services that need to be integrated?
    **Microsoft 365, Meraki, Active Directory**

30. Do you currently have an Endpoint Protection System. If so, which vendor? **Yes**

31. Are you looking for an Incident Response Plan for the services being managed or for the whole
    - How many people would participate in the tabletop exercises? **unknown**
    - What ticketing system do you use? **IT Ticketing System**
    - Does your organization use MFA? **Yes**
    - On average, how many end user reported phishing emails do you get in a week or month? **Unknown**

32. Current Cybersecurity Posture: Can you provide details on your existing cybersecurity infrastructure and any known vulnerabilities or past incidents? **No**

33. Specific Threats and Concerns: What are the primary cybersecurity threats or concerns Bryan County has faced or anticipates facing? **Unknown**

34. Compliance Requirements: Are there specific regulatory or compliance requirements (e.g., HIPAA, CJIS) that the proposed solution must adhere to? **CJIS, HIPAA**

35. Service Level Agreements (SLAs): What are your expectations regarding SLAs, particularly concerning response times and escalation procedures? **24/7, 365, Response within minutes**

36. Incident Response History: Can you provide examples of past security incidents and the effectiveness of your response protocols? **No**

37. Project Timeline: Are there any critical deadlines or milestones for the implementation of the cybersecurity services? **60 Days**

38. User and Endpoint Growth: Do you anticipate any significant changes in the number of users or endpoints during the contract period? **Yes**

39. Collaboration with Internal Teams: What level of collaboration is expected between our team and your internal IT and security teams? **Full Collaboration**

40. Scalability Requirements: How scalable should the proposed cybersecurity solutions be to accommodate future growth and technological changes? **Open to changes**

41. Are there any integration requirements with existing security systems or platforms and if so what vendors?
    **Microsoft 365, Meraki, Active Directory**

42. What types of email-based threats are most concerning (e.g., phishing, spam, malware)? **All**

43. Could you specify the expected volume of log data (e.g., events per second or daily volume)? **Unknown**

44. What are the most common types of security incidents encountered? **Unknown**

45. What are the response time expectations for different types of incidents? **24/7, 365**

46. What are the expected hours of operation for ongoing monitoring (e.g., 24/7, business hours)? **24/7**

47. How should critical alerts and incidents be communicated to the client?
    **Phone call, text message, Teams Channel**

48. Who are the key stakeholders that will receive these reports? **CIO**

49. Who are the key personnel involved in the incident response process? **CIO**

50. Regular Updates and Maintenance:
    - What is the expected frequency for updates and maintenance activities? **unknown**
    - Are there specific windows or schedules for maintenance tasks? **No**
    - What level of disruption, if any, is acceptable during maintenance? **Unknown**

51. Continuous Threat Assessment and Response:
    - How should threat assessments be documented and communicated?
      **Email, Teams Channel**