BID ON: MANAGED DETECTION AND RESPONSE (MDR) SOLUTION
BID NO.: RFP #25-28
BID OPENING: JUNE 10, 2025 @ 10:00 AM

QUESTION AND ANSWER SHEET

Date of Question: May 14, 2025
QUESTION:

1. In regards to the RFP in the subject line, are out of state firms allowed to place a bid in this for this particular work?

ANSWER:
Yes.

QUESTION:

2. Is electronic submission acceptable?

ANSWER:
2.1 Response Submission

Responses to this RFP must be submitted in sealed packages and delivered to the Purchasing Office, Mobile County Public School District, 1 Magnum Pass, P.O. Box 180069, Mobile, AL 36618 no later than the Bid Opening scheduled for Monday, June 10, 2025 @ 10:00 AM (Central). It is the sole responsibility of the respondents to ensure their responses arrive in a timely manner. The Customer will reject all late arrivals. The Vendor must submit one (1) original and five (5) printed copies and one (1) electronic EXACT copy (Adobe PDF format) of the response along with any required supporting documentation. 25-28 "MANAGED DETECTION AND RESPONSE (MDR)" should be clearly marked on the face of the envelope/container containing the bid along with the bid opening date. Failure to comply with this may cause the bid to be misdirected and therefore not to be considered.

Oral, telephone, faxed, emailed, electronic, or telegraphic bids shall not be considered, nor will modifications of bids by such communication be considered. The completed bid form shall be without erasures or alterations. Signatures on the proposals shall be in longhand and executed by an individual duly authorized by the Vendor to make a contract. Bids completed in pencil will NOT be accepted.

DATE OF QUESTION: MAY 19, 2025
QUESTION:

3. Is the district open to managed service MDR rather than self-managed MDR?

ANSWER:
We currently have a managed solution, which is mentioned in the bid.

DATE OF QUESTION: MAY 20, 2025
QUESTION:

4. When are the answers uploaded to the website? I know questions are due 5/28 but based on the answer to this question I may have additional questions and want to ensure I would have time to submit.

ANSWER:
The question and answer sheet will be updated on a regular basis. It is the responsibility of the bidder to keep checking the website. The deadline to submit questions is May 28, 2025, at 4:00 pm cst.

DATE OF QUESTIONS: MAY 21, 2025
QUESTION:

5. Of the 20,000 endpoints, how many are faculty/staff versus student devices?

ANSWER:
These are faculty devices.

QUESTION:

6. Is the same license level needed for the student devices as the faculty/staff devices?

ANSWER:
It is not.

QUESTION:

7. Do you plan to ingest data from a third-party source (i.e. firewall, O365, Active Directory, Azure, etc.)?

ANSWER:
We do plan to ingest data from a Firewall, O356, Ad and Azure but, please clarify what you mean by a 3rd party. We manage these services.

QUESTION:

8. Would there be consideration for a three-year proposal of pricing that includes annualized payments (equal over each year)?

ANSWER:
As stated in section 1.4
A contract will be awarded for a period of one (1) year, starting July 1, 2025, to June 30, 2026. The contract may be renewed for an additional two (2) years, or renewed annually if both parties agree to the same terms and conditions. The renewal options, if permitted by bid law, shall be executed at the Customer's discretion and as mutually agreed upon, provided pricing remains the same as originally agreed upon, the Vendor continues to meet all requirements as specified herein, the Customer continues to be funded through the Cybersecurity Pilot Program (CPP), and when executing the renewal options does not violate State of Alabama Bid laws or CPP rules or guidelines.

It is not in the school district's best interest to commit to this type of contract because this is a pilot program, and funding may not be guaranteed for three years

QUESTION:

9. Is a bid bond required for this RFP?

ANSWER:
NO.

DATE OF QUESTIONS: MAY 27, 2025
QUESTION:

10 What specific type of endpoints?

ANSWER:
The RFP specifies coverage for approximately 20,000 endpoints, composed of:

- **89% Windows**
- **10% MacOS**
- **1% Linux**
    - Can we get a breakdown on total laptops? Servers? Etc?

ANSWER:
The RFP does not provide a detailed breakdown by device type (e.g., laptops vs. servers). However, the MDR solution must support:

- **Windows 11**
- **Windows Server**
  MacOS X

QUESTION:

11. Will there be endpoints that will be off the internal network at any time?
    a. Do students or staff take devices home?

ANSWER:

Yes. The RFP explicitly states:

The solution should work on and off-premises, with threat alerts and responses potentially differentiated based on location.

QUESTION:

12. No mention of firewalls, how is that being handled?

ANSWER:

Yes, there is no mention of firewalls.

We have two self-managed perimeter firewalls.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

13. Per SOW, goal is to cover 20k endpoints, Why is the goal only 20,000 endpoints when there 60k students & 130k devices?

ANSWER:

The RFP states:

"Our goal is to cover approximately 20,000 endpoints.

We have a Bring Your Own Devices Policy (BYOD) and allow students and faculty to connect their devices to the network. However, BYOD is outside the scope of this project. The 20,000 figure represents a core deployment target, while the pricing sheet reflects maximum potential licensing needs under the Cybersecurity Pilot Program. Please use the license counts in the bid form.

QUESTION:

14. What type of Identity Protection specifically? MFA, SSO, etc

ANSWER:

The RFP specifies:

The solution should detect and prevent whether credentials are used in a suspicious manner (lateral movement).

It also requires integration with Active Directory/Microsoft Entra ID and the ability to feed data to a log server.

QUESTION:

15. What is meant by lateral movement?

ANSWER:

In this context, "lateral movement" refers to:

The unauthorized use of credentials to move between systems within the network, often as part of a broader attack. The MDR solution is expected to detect and prevent such activity.

DATE OF QUESTIONS: MAY 28, 2025

QUESTION:

16. How many devices are currently scanned with the existing Arctic Wolf's Managed Risk solution?

ANSWER:

Arctic Wolf is scanning ~9500 user devices.

QUESTION:

17. Do they have virtualization hosting capabilities, e.g. VMWare, for MDR on-premises components (Log Collector, Honeypot, Orchestrator, Vulnerability Scanner VMs)

ANSWER:

Yes.

QUESTION:

18. Do they require SOAR response automation capabilities

ANSWER:

The RFP does not explicitly mention SOAR (Security Orchestration, Automation, and Response). However, it does require:

"The software and services provided should be capable of multiple remediation methods…"

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

19. Do they require internal Vulnerability Scans to assess and prioritize critical vulnerabilities for remediation of non-endpoint systems (IoT devices, network infrastructure, network appliances)

ANSWER:

The RFP does not explicitly mention internal vulnerability scanning for non-endpoint systems. However, the inclusion of:
AW-MR-SE or Equal — Arctic Wolf Managed Risk server license — Quantity: 220.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

20. Do they need to retain MDR security data for longer than 60 days (up to 365 days)

ANSWER:

The RFP includes:
AW-MDR-90DAY or Equal — Arctic Wolf MDR Log Retention - 90 days — Quantity: 622

This indicates a 90-day retention period is currently scoped. There is no mention of a requirement for 365-day retention.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

21. Are they interested in deploying Deception Technology (Honeypots)

ANSWER:

There is no mention of deception technology or honeypots in the RFP.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

22. To assess potential security log sources to ingest into MDR platform, can they provide a basic summary of their network device types (routers, switches, firewalls, UTMs, VPNs, Active Directory servers, LDAPs, DHCP, DNS, syslog-capable systems, etc)

ANSWER:

The RFP does not provide a detailed inventory of network device types. However, it does state: "The solution should integrate with Active Directory/Microsoft Entra ID and be able to feed information to a Log server."
We have Two Perimeter Firewalls, 5000+ Network Switches, and 8000+ Access Points. 200+ Servers, 500+Network printers.

QUESTION:

23. Do they need network sensors to monitor traffic as it traverses their network

ANSWER:

Yes. The pricing sheet includes:
AW-MDR-10XX-S-10GFNB or Equal — Arctic Wolf 1000 Series Sensor — Quantity: 3
This confirms that MCPSS uses network sensors to monitor traffic.

QUESTION:

24. There are currently 3 arctic wolf sensors, each with 4x10Gb interfaces. Regarding network sensors at high volume locations
- •define high volume (volume, rate, specific network segments)
- •how many such locations
- •can they host hardware network sensors at these locations
- •can they host virtualized network sensors at these locations

ANSWER:

The RFP does not define a high-volume location or specify the number of such locations or their hosting capabilities (hardware or virtualized). All Sensors will be housed in our Data Center, and we can host virtualized network sensors there.

QUESTION

25. In the RFP, it says you need coverage for up to 130k devices on the network and also for 20k endpoints. Are the endpoints inclusive of the network device count or is it 20k endpoints that are off the network?

ANSWER:

The 20,000 figure represents a core deployment target, while the pricing sheet reflects maximum potential licensing needs under the Cybersecurity Pilot Program. Please use the license counts in the bid form.

QUESTION:

26. Would we be able to set up a scoping call so we can get a more accurate idea of what the pricing and deployment will be?

ANSWER:

The RFP does not include scoping calls, but it does provide instructions on how to submit questions. We regret that we cannot accommodate scoping calls at this time.
"All questions concerning this solicitation are to be submitted in writing to the Customer's Purchasing Department personnel… Questions must be submitted by May 28, 2025 @ 4:00 PM (Central Time)."

QUESTION:

27. We can provide 2 offerings- We leverage AI to provide the MDR services on its own but we can also include people behind it as well. Could we submit both options?

ANSWER:

Yes, the RFP allows for flexibility in solution offerings:

"The Bidder is strongly encouraged to address all evaluation criteria… If the bidder fails to adequately respond to an evaluation factor, it may be deemed non-responsive."

You can submit both options as long as each is clearly defined and meets the evaluation criteria. Be sure to use the provided price proposal format and clearly distinguish between the two offerings.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

28. Are Chromebooks needing to be covered with the MDR service?

ANSWER:

No. Chromebooks are not mentioned as part of the required endpoint coverage. The RFP specifies:

"Our goal is to cover approximately 20,000 endpoints, composed of about 89% Windows, 10% MacOS, and 1% Linux."

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

29. Are you looking for NDR?

ANSWER:

The RFP is focused on endpoint and cloud-based MDR capabilities. There is no mention of NDR.

"MCPSS uses a state-of-the-art Managed Detection and Response (MDR) solution to protect its network from cyber threats. This MDR solution provides comprehensive, 24/7 monitoring across endpoints and cloud environments.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

30. Can you please provide clarification on the 20,000 endpoint quantities (under Scope of Services section) versus the Arctic Wolf quantities at the end of the bid document?

ANSWER:

The 20,000 figure represents a core deployment target, while the pricing sheet reflects maximum potential licensing needs under the Cybersecurity Pilot Program. Please use the license counts in the bid form.

QUESTION:

31. What endpoint protection solution is MCPSS currently utilizing today?

ANSWER:

Cisco Secure Endpoint Protection

QUESTION:

32. Does MCPSS require the solution to have the same interface and platform as the MDR services team, with full visibility into investigations and actions taken?

ANSWER:

Yes. MCPSS requires dashboards that provide both summary and detailed information, indicating a unified interface with full visibility.
"The MDR should provide summary and detailed information and relevant dashboards."

QUESTION:

33. Is MCPSS requiring full-service incident response capabilities, including unlimited response actions within your in-scope environment?

ANSWER:

The RFP specifies the need for multiple remediation methods and proactive/reactive threat hunting, which implies full-service incident response.
"The software and services provided should be capable of multiple remediation methods (e.g., block, quarantine, isolate, send for analysis)."
"Services should include proactive and reactive threat validation, prioritization, and hunting."

QUESTION:

34. Is MCPSS requiring direct, in-platform access to a SOC analyst, rather than going through an intermediary like a concierge?

ANSWER:
As Stated in the RFP.
Advice
"Solution should provide MCPSS Information Technology Services Department with actionable advice on addressing root causes of threats and solutions for hardening systems via a certified security advisor—periodic/quarterly planned meetings to review reports and ways to reduce our threat surface."

QUESTION:

35. From a dashboard view perspective, is MCPSS requiring the ability to run advanced queries, correlate data, or conduct in-depth investigations?

ANSWER:
As stated in the RFP.
"The MDR should provide summary and detailed information and relevant dashboards."

"The software provided should be capable of multiple detection methods: (e.g., rules-based, behavioral, and AI-based)."

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

36. Is MCPSS requiring full incident response service included with the solution, or are you limited to a starter retainer that requires additional purchases during a breach?

ANSWER:
The pricing sheet includes an "IR JumpStart Retainer," suggesting a starter model is acceptable, but the scope also emphasizes comprehensive remediation.
"AW-IR-JSR or Equal — Arctic Wolf IR JumpStart Retainer or Equal"

"The software and services provided should be capable of multiple remediation methods…"

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

37. Is MCPSS requiring that generated alerts are correlated, contextualized, and accurately tied to the correct device to reduce noise and improve response efficiency?

ANSWER:

The RFP emphasizes detection of abnormal activity and location-based alert differentiation, which implies contextual and accurate alerting.
"The solution should detect activities outside of a normal baseline."

"The solution should work on and off-premises, with threat alerts and responses potentially differentiated based on location."

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

38. Does MCPSS have a data retention beyond 90 days?

ANSWER:

The pricing form includes a 90-day log retention item, with no mention of longer retention being required.
"AW-MDR-90DAY or Equal — Arctic Wolf MDR Log Retention - 90 days or Equal".

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

39. Is MCPSS requiring the provided solution to allow MCPSS staff to have full access to log data without additional costs or delays?

ANSWER:

While dashboards and detailed reporting are required, the RFP does not explicitly mention unrestricted log access or cost-free access.
"The MDR should provide summary and detailed information and relevant dashboards."

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

40. In Section 1, its outlined that MCPSS has between 50-130K devices on the network. Under Background and Context, it states the goal is to cover approximately 20K endpoints. Attachment A (last page) shows more detailed quantities. (6221) user licenses, (58,000) student licenses and various other quantities. Is the goal to provide the MDR solution for all devices connecting to the network or just a subset of devices?

ANSWER:

The 20,000 figure represents a core deployment target, while the pricing sheet reflects maximum potential licensing needs under the Cybersecurity Pilot Program. Please use the license counts in the bid form.

QUESTION:

41. Does MCPSS require access into the dashboard to view alerts in real time for self- remediation?

ANSWER:

The RFP specifies that the MDR solution should provide:
"summary and detailed information and relevant dashboards"
Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

42. In Section 1.4 the contract term is identified as 1 year with an option to renew for two additional years. If there is significant savings would MCPSS consider prepaid option?

ANSWER:

The RFP does not explicitly mention prepaid options. However, it states:
As stated in section 1.4
A contract will be awarded for a period of one (1) year, starting July 1, 2025, to June 30, 2026. The contract may be renewed for an additional two (2) years, or renewed annually if both parties agree to the same terms and conditions. The renewal options, if permitted by bid law, shall be executed at the Customer's discretion and as mutually agreed upon, provided pricing remains the same as originally agreed upon, the Vendor continues to meet all requirements as specified herein, the Customer continues to be funded through the Cybersecurity Pilot Program (CPP), and when executing the renewal options does not violate State of Alabama Bid laws or CPP rules or guidelines.

It is not in the school district's best interest to commit to this type of contract because this is a pilot program, and funding may not be guaranteed for three years.

QUESTION:

43. Is network detection required, in addition to cloud and endpoint?

ANSWER:

The RFP emphasizes coverage for:

- **Cloud environments**
- **Identity protection**
- **Integration with Active Directory and log servers**

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

44. How will the service's start date be affected by the revised RFP close date?

ANSWER:

The RFP states:

"Installation [must be] completed (fully tested & operational) 48 hours prior to July 1, 2025"
The service start date will only be affected if there is an issue on the part of the Customer
Additionally, the RFP outlines that all proposals should include detailed timelines for implementation, ensuring alignment with the specified deadlines. Vendors are encouraged to demonstrate flexibility in scaling services to future-proof solutions as organizational needs evolve.

QUESTION:

45. Are you expecting the MDR provider to cover endpoints, network, and cloud environments under their managed services?

ANSWER:

Yes. The RFP specifies:
"24/7 monitoring across endpoints and cloud environments".

QUESTION:

46. Do you prefer that incident response actions are automated and/or manual?

ANSWER:

The RFP requires:
"multiple remediation methods (e.g., block, quarantine, isolate, send for analysis)".

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

47. Is integrated threat intelligence a requirement?

ANSWER:
While not explicitly stated, the RFP emphasizes:
"proactive and reactive threat validation, prioritization, and hunting".

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

48. Does the XDR solution need to integrate with your existing IT ticketing tools? If so, what tools?

ANSWER:
This is not mentioned in the RFP. Our current solution is not integrated with our IT Ticketing system.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

49. What privacy or regulatory compliance requirements must the solution meet? For example, FERPA (Family Educational Rights and Privacy Act), CIPA (Children's Internet Protection Act), COPPA (Children's Online Privacy Protection Act), CIPA (Children's Internet Protection Act), HIPAA), ADA (Americans with Disabilities Act) and any state and local Data Privacy Laws?

ANSWER:
The RFP does not list specific compliance frameworks, but as a public school system, MCPSS is subject to:

- **FERPA**
- **CIPA**
- **COPPA**
- **HIPAA (if health data is involved)**
- **ADA**
- **State/local data privacy laws**

Vendors should assume compliance with these standards is required.

QUESTION:

50. What types of telemetry do you need the solution to ingest (e.g., from endpoints, firewalls, cloud applications, identity providers)?

ANSWER:
The RFP mentions:

- **Endpoints (Windows, MacOS, Linux)**
- **Cloud environments**
- **Identity systems (Active Directory/Microsoft Entra ID)**
- **Log servers [2]**

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

51. How frequently do you expect threat assessments to be completed? (e.g., monthly, quarterly, annually)

ANSWER:
The RFP states:
"periodic/quarterly planned meetings to review reports and ways to reduce our threat surface".

QUESTION:

52. As an MDR provider, will we be granted permission to isolate endpoints, terminate malicious processes, or perform other remote response actions?

ANSWER:
Yes. The RFP includes:
"remediation methods (e.g., block, quarantine, isolate)".

QUESTION:

53. What are your expectations around alert escalation workflows?

ANSWER:
The RFP does not detail escalation workflows but does require:
"immediate notification of detected threats and remediation as agreed upon" .

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

54. Should automated response playbooks be customizable to your policies?

ANSWER:
Yes. The RFP emphasizes flexibility and adaptability to:
"rapidly changing operational needs"
Customizable playbooks would align with this requirement.

QUESTION:

55. What are your expectations regarding Security Operations Center (SOC) staffing and escalation procedures?

ANSWER:
The RFP does not specify SOC staffing levels or escalation procedures. Vendors should describe their SOC model and escalation paths in their proposal.

QUESTION:

56. Do you track Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)? What targets are you aiming for?

ANSWER:

The RFP does not mention MTTD or MTTR. Vendors may propose industry-standard benchmarks and offer SLAs.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

57. In addition to Windows and MacOS operating systems, do you require support of Chrome OS?

ANSWER:

The RFP specifies support for:

- **Windows 11**
- **Windows Server**
- **MacOS X**
- **Linux**

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

58. Do you have specific requirements regarding the geographical location of your data storage?

ANSWER:

No specific data residency requirements are mentioned in the RFP. However, given that MCPSS is a public school system, vendors should assume that compliance with U.S.-based data residency and privacy regulations (such as FERPA, CIPA, and COPPA) is expected, even if not explicitly stated. If your solution involves data storage outside the U.S., clarifying this in your proposal and confirming acceptability with MCPSS would be prudent.

QUESTION:

59. In addition to the July 1st service start date, are there any other critical deadlines or phases we should be aware of?

ANSWER:

The only critical date mentioned is:
"Service Start Date: July 1, 2025"
No other phases are outlined.

QUESTION:

60. What, if any, training will be needed for your internal teams?

ANSWER:

The RFP does not specify training requirements. Vendors may propose onboarding and training as part of their solution.
Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

61. Do you require real-time dashboards and alerts to monitor your security posture and incidents?

ANSWER:
Yes. The RFP requires:
“summary and detailed information and relevant dashboards”.

QUESTION:

62. Would customizable reports for district leadership or compliance purposes be required?

ANSWER:
Yes. The RFP mentions:
“periodic/quarterly planned meetings to review reports”.

QUESTION:

63. Do you need the ability to automate report generation and scheduling? If yes, how frequently should these reports be delivered, and to whom?

ANSWER:
This is not mentioned in the RFP.
Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

64. What are your expectations for support ticket acknowledgment and resolution times, and do you categorize tickets by priority or severity—and additionally, do you have minimum service availability or uptime requirements (e.g., 99.9%)?

ANSWER:
Not specified. Vendors should propose SLAs and support tiers.
Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

65. Would you expect remediation actions or penalties from the vendor if agreed-upon SLOs (Service Level Objectives) are not met? If yes, what form should those take (e.g., service credits, escalation paths)?

ANSWER:
Not mentioned. Vendors may propose service credits or escalation paths as part of their SLA.

Any additional solution options with pricing can be added to the Specification Variance Sheet.

QUESTION:

66. What are the numbers of each staff, faculty, and students that are in scope for this RFP?

ANSWER:

The RFP states that the Mobile County Public School System (MCPSS) serves approximately:

- **60,000 students**
- **7,500 staff members**

QUESTION:

67. Is the district interested in seeing additional service offerings from the MDR provider such as vulnerability scanning, Endpoint protection, etc.

ANSWER:

Any options with pricing not listed in the RFP should be added to the specification variance sheet only.

QUESTION:

68. Are there any formatting requirements for the response document itself? e.g. font size, spacing etc.

ANSWER:

Yes, there are formatting guidelines:

- **Proposals must not exceed 60 pages total, excluding the front cover, section dividers, letter of transmittal, and required forms.**
- **Each sheet face printed with text or graphics counts as one page.**
- **There are no specific instructions on font size, spacing, or margins, but clarity and professionalism are implied expectations.**

BIDDERS ARE RESPONSIBLE FOR CHECKING THE MCPSS WEBSITE FOR THE QUESTION & ANSWER SHEET ON A REGULAR BASIS FOR UPDATES.

DEADLINE FOR SUBMITTING QUESTIONS IS MAY 28, 2025, AT 4:00 PM CST.