# INVITATION FOR BID

## IFB 2024-09

## Bay County Information Systems Division (ISD)
## Managed Detection and Response Services (MDR)

JIM BARCIA
BAY COUNTY EXECUTIVE

**INVITATION TO BID – THIS IS NOT AN ORDER OR OFFER**

IF FOR ANY REASON YOU CANNOT RETURN THIS BID, PLEASE RETURN THE NON-BIDDERS FEEDBACK FORM TO ENSURE THAT YOUR FIRM MAY BE RETAINED ON OUR BIDDER LIST

| | |
|---|---|
| **DATE OF REQUEST** | APRIL 12, 2024 |
| **REFERENCE BID NUMBER** | IFB 2024-09 |
| **DEADLINE FOR VENDOR QUESTIONS** | APRIL 19,2024<br>5:00 PM |
| **ADDENDUM ISSUED** | APRIL 26, 2024<br>5:00 PM |
| **PROPOSED DATE/TIME REQUIRED** | MAY 10, 2024<br>11:00 AM |
| **BID SUBMITTAL** | BAY COUNTY FINANCE DEPT.<br>ATTN: JESSICA FOSS<br>BAY COUNTY BUILDING<br>515 CENTER AVENUE<br>7TH FLOOR<br>BAY CITY, MI 48708-5128 |
| **MARK BID** | "BAY COUNTY ISD<br>MANAGED DETECTION AND RESPONSE SERVICES" DELIVER BID TO FINANCE DEPARTMENT IMMEDIATELY" |

**REST OF THIS PAGE IS INTENTIONALLY BLANK**

**INTRODUCTION:**

Bay County is seeking a 24x7 Managed Detection and Response system to provide vulnerability monitoring and incident response capabilities to its Information Systems Division.

**GENERAL REQUIREMENTS:**

**I. Implementation and Service Methodology**

1. Provide a brief overview of your Managed Detection and Response (MDR) services and any supporting products.
2. Is your Security Operation Center (SOC) staffed 24/365? Describe your approach to supporting 24/365 remote security monitoring and device/agent management, including any use of "follow the sun" staffing.
3. Describe the architecture of your Managed Security Services (MSS)/MDR delivery capability, including elements in your SOC, data center (on your premise, colocations, and private and public cloud services), network, and our premises, as well as the centrally delivered log management, analytics and portal tiers, and capabilities for collecting event logs and data from other locations (e.g., Software as a Service [SaaS] and Infrastructure as a Service [IaaS]). Provide example architectural diagrams and descriptions. Indicate where there are any regional differences in architectures or technologies used. Finally, include and identify any elements that are delivered by third-party partners.
4. List the primary tools used to deliver your services. Describe the function or service offering they support, and indicate whether they are proprietary, commercial, or open source, for example, log collection, log management and storage, analytics, reporting, case management and workflow, and incident response.
5. Explain how these services, and any supporting products, will interact with common security-related products, including log correlation systems, security incident and event monitoring systems, Intrusion Prevention Systems (IPS), and firewalls. Specific details of the environment will be shared under Non-Disclosure Agreement (NDA) to selected respondents.
6. Will your services require the use of proprietary technology that Bay County must purchase or install? If so, please list all pertinent information related to this technology, including hardware, software, networking, middleware, and database requirements. Include any associated costs as a separate line item in your quote.
7. Explain how you use external data (e.g., threat intelligence feeds) to analyze potential threats to Bay County's environment and describe what access to this data Bay County will have.
8. Please provide an overview of your customer notification and escalation process. Include details on how often a customer is notified of a security event, and on the methods of notification.
9. Indicate how your services can be delivered in internal or virtual infrastructure. Include details about how the services will accommodate the scaling (larger or smaller) of the virtual environment, the implications for technology deployment to support monitoring, and related contractual, license or cost implications.
10. Indicate how your services can be delivered in an external or cloud-based infrastructure. Include technology and contractual or licensing requirements related to provisioning, ongoing monitoring, and de-provisioning of services to the cloud infrastructure. Describe the process to add or remove monitoring sources in a public cloud infrastructure.
11. Describe your support for monitoring security or other related events from SaaS providers, specifically Microsoft O365. List which providers can be monitored natively. Do you require and/or support Cloud Access Security Brokers (CASBs)?
12. Explain how you will complete an initial assessment, and how you will establish a baseline security level. Include specifics on your implementation timeline; infrastructure requirements; data transfer, data storage and segregation, backup systems, and encryption standards.
13. Describe the frequency and opportunities for continuous improvement during the implementation phase.
14. Please provide an example of how your services detected and addressed a recent security incident.
15. Explain your methodology for detecting custom or targeted attacks directed at our users or systems.

## II. Managed Detection and Response

1. Indicate the capabilities of your services to correlate endpoint and network information to identify risks to customer environments.
2. Explain your ability to analyze data from various technologies to provide real-time alerting of security incidents.
3. If certain third-party technologies or other services are required to provide the MDR service, please list, describe, and provide pricing information for each, including any necessary hardware and software to support them (network taps, log servers, end point software, etc.).
4. Please describe the use of any signature-based rules and how your company keeps these signatures/rules updated.
5. Explain support for the creation and management of customized rules. Explain the capabilities available to our staff for doing so. Describe any limitations, such as data sources, age, and query frequency.
6. Explain your ability to analyze this data to identify when changes in behaviors of users or systems represent risk to our environment.
7. Explain your methodology for reducing false positives and false negatives and for classifying security-related events that represent a risk to Bay County.
8. Describe how false positives are managed, and how your company will incorporate false positive feedback from Bay County.
9. Describe in specific detail the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to an analyst for evaluation through the triage, validation, prioritization, and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts.
10. Indicate in detail, the level of interaction and support that our staff can expect from your security analysts to assess, investigate, and respond to incidents.
11. Indicate any included support for consulting on high priority findings or information on the ability to contract for such support.

## III. Security Information Management

1. Indicate the data sources supported for log collection, reporting, and retention. Can logs be collected from any source? Describe the collection methods (e.g., forwarded syslog, Windows Management Instrumentation [WMI], local forwarding agent). Also, describe how the information will be used to support specific use cases.
2. Will all our raw event logs and data be collected and forwarded to your platform for storage? If not, describe the variation and options for full log event retention (if applicable).
3. Will our logs be compressed and encrypted in transit, and is it a guaranteed delivery via a store and forward type of solution? If so, please describe.
4. Indicate any limitations to your log collection capabilities, such as peak event rates, volume, or sources.
5. Explain the capabilities that allow our staff to search for and browse original log data. Describe any limitations to this capability.
6. Explain the capabilities of our staff to create and modify reports based on collected log data. Indicate any limitations, such as number of reports, complexity of queries, and age of data.
7. Indicate your standard data retention policies and ability to modify them to meet our requirements.
8. Is there a minimum and maximum of times that log retention can be offered? Describe what is actively available and indexed versus what is kept offline and archived. If 365 days of storage is required, how will that be priced for Bay County?
9. Specify how your company approaches the online/warm/cold types of storage.

10. What is the process for adding additional log sources to the scope of service? Include the implications for deployment architecture, integration costs and ongoing costs.

## IV. Advanced Analytics and Capabilities

1. Does your company's MDR offer or utilize advanced analytics capabilities? If so:
   Describe your capabilities around the use of machine learning or artificial intelligence in modeling behaviors and analytics.
2. Describe your ability to implement watch-lists, both those you define, and those we define.
3. What technologies are used to enable advanced analytics?
4. How do you profile and monitor entity and user activities and behaviors (e.g., user and entity behavior analytics [UEBA])? Describe specific approaches and models/algorithms used, including any regional variations.
5. Describe your use of predictive analytics, including specific approaches and models/algorithms used, and any regional variations.
6. Describe any specific network monitoring and/or network forensics features, capabilities, or offerings to detect advanced, targeted attacks.
7. Describe any specific payload analysis features, capabilities, or offerings to detect advanced, targeted attacks.
8. Describe any specific endpoint behavior analysis and/or endpoint forensics features, capabilities, or offerings to detect advanced, targeted attacks. Also describe how these are maintained and updated.
9. How is streamed data with real-time advanced analytics supported? Describe and list any technologies supported (e.g., Kafka, NiFi).
10. Describe the data and threat visualization capabilities available to us via the portal.
11. Describe any managed detection and response-type service offerings (e.g., managed endpoint detection and response, threat hunting, remote response, and containment).
12. Describe specifics around threat hunting services (e.g., how frequent threat hunting is performed, threat hunting techniques, and scope of threat hunting activities)
13. Explain if/how you leverage big data platforms for the collection, retention, and analysis of large volumes of operational and security data for analysis.
14. How are big data platforms used to support the collection/analysis of network and endpoint data? Does your company require the deployment of its own advanced analytics tools and technologies, or does your company support offerings from other vendors?

## V. Incident Response

1. Are there any remote and/or on-site incident response (IR) activities included as part of the service? If so, describe the services provided, including specifics on what is included in the core services versus what is available as an additional service/offering.
2. Do you provide incident response activities, including breach response services, via an optional retainer? If so, describe the packages, Service-Level Agreements (SLAs), costs and included services. Do you offer proactive services as part of a retainer? Which services can be delivered remotely (both proactive and reactive), and which require your staff to be physically on our site(s)? Do you provide any IR activities outside of a retainer, such as a "just in time" type services?
3. Do you assist with creating specific IR use cases and maintaining a run book? If so, describe how this is achieved.
4. Do you require specific IR providers?
5. Describe any self-service features for incident response provided via the portal (e.g., automated malware analysis, custom signature, or correlation rule implementation).

## VI. Vulnerability Management Services

1. Does your company's MDR utilize reports and information from third-party Vulnerability Management (VM) services, either commercial or public? If so: please list those services.
2. Indicate the technologies used to conduct security scans, both commercial and open source.
3. Provide details on your methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.
4. Describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan results and actions carried out. Is the VM data also used in the same fashion for MDR services, if applicable?
5. Describe integration capabilities with vulnerability assessment data, including how the vulnerability data is used in support of triaging and investigating potential security events, and alerting and reporting capabilities.
6. How can vulnerability scans be scheduled, initiated/managed via your MSS/MDR portal? How are results viewed in the portal?
7. Indicate your ability to intake results from scanning devices already situated in the Bay County environment.
8. Indicate the frequency your MSS/MDR can scan our environment.
9. How frequently is the vulnerability database updated, and what are the data sources used for that?
10. Indicate the application-specific scanning that you carry out as part of your VM services.

## VII. Internet of Things Capabilities

1. Does your company's MDR include Internet of Things (IoT) in its scope? If so: what notable Internet of Things partnerships do you have?
2. Provide some examples of the IoT use cases you support.
3. How many customers do you have where you are monitoring IoT devices?

## VIII. Portals, Reports and Dashboards

1. Indicate any local language support or localization features in your portal and note any regional differences.
2. Describe the information provided by and features available through the web-based portal or console associated with your services. Describe the underlying technology (HTML5, JavaScript, etc.). Also, include details on your support for Role-Based Access Control (RBAC), customization of screens and data presentation, predefined correlation rules, and predefined reports.
3. Be prepared to demonstrate the console and any dashboards that would be available as part of the service. Also indicate if there are customization options.
4. Indicate whether all services and MSS/MDR features, including those delivered by partners, will be available via a single portal, regardless of region or part of business delivering the services.
5. What authentication and identity management system does your portal use? Do you provide support for federated identity management (FIM)?
6. How does the portal provide us access to external threat intelligence feeds?
7. Describe support for bidirectional threat intelligence using open standards, such as Structured Threat Information eXpression (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII)/Open Indicators of Compromise (OpenIoC).
8. Can Bay County access and search log event data via your MSS/MDR portal?
9. Describe user roles available to us and how those roles can be used to restrict access to logs and reports (e.g., administration, view/report, etc.).
10. Describe any real-time chat/instant messaging and/or live video interaction available with your analysts.
11. Describe any integration capabilities with third-party service desk and ticketing tools and services. How is this achieved (e.g., email, application programming interfaces [APIs], etc.)? Also, indicate if you provide single-direction or bidirectional support, and whether the integrations are subject to additional costs.

12. Describe the portal capabilities to enable our staff to create, update, and close support tickets.
13. Describe how much visibility your company provides on the tasks of the support workflow. Consider how many alerts there are, your staff level (e.g., Level 1, Level 2, Level 3), and how long they are on a particular phase in the process.
14. Is there a smartphone/tablet application available? If so, briefly describe the supported platforms and functionality.
15. Describe operational, regulatory, and executive reporting capabilities.
16. Indicate the number of predefined reports, including specific regulatory and compliance items supported, that will be available to Bay County. Please provide examples.
17. Explain how report data can be exported to or used by an external report writer or risk dashboard.
18. Explain the capabilities for our staff to create customized, ad hoc queries, and reports. Describe any limitations to ad hoc query or report generation, including data sources, data age, and query frequency.
19. Are regular threat intelligence briefings provided to Bay County ISD staff? What information is provided in these briefings and how often are they conducted?
20. Will threat intelligence databases be made available to Bay County ISD staff?

## IX. Service Management

1. Explain the expected working relationship, roles, and responsibilities between your security staff and Bay County ISD staff.
2. Indicate the frequency of meetings or teleconferences to review performance, issues, threat environment, and responses. Explain the types of analysts and account management support provided during those meetings.
3. Indicate the frequency of executive business meetings to review the overall performance, value, and continuous improvements of services.
4. Indicate device/agent management, and real-time event management notification service levels. Explain how they are measured, and how they will be communicated to Bay County.
5. Provide a sample of an SLA including response times.
6. Describe your problem resolution and escalation procedure.
7. Describe your SLA performance reporting. If applicable, indicate whether these methods are used in some or all regions.
8. Does your company have standard time frames, after which a given security product is no longer supported? If so, please describe the details, including proprietary and third-party software time frames.
9. Please provide details on support agreements. If a third-party software update is required, when does the SLA between you and Bay County begin?
10. Describe the process for adding services or new technologies.
11. What process will determine if a change is within the original scope of the supplied technology or a new feature? How will the costs be determined?
12. What access to internal-auditing documentation will you provide if our auditors, customers, or business partners require this documentation in support of legal, regulatory, or contractual requirements? What is your process for requesting documentation? What are the time frames to which you will commit for producing documentation?
13. Describe the process should Bay County have a complaint.
14. Indicate your process for notifying us of your noncompliance with the SLA, and vice versa.
15. Describe the remedies available to Bay County should you fail to meet any SLAs. Explain any regional variations to remedies.
16. Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another MSS/MDR, if applicable.
17. Describe how Bay County’s data would be obtained during the termination process.

18. Describe how Bay County's data (including data generated by your company about security events and incidents affecting Bay County) will be governed and protected in transit. Consider this from a technological perspective, as well as via processes and procedures. How will the treatment of Bay County's confidential data assist with better job performance (e.g., creating internal architecture and topology maps)?
19. Will you allow Michigan law to govern?
20. Provide examples of how your company has met specific regulatory or statutory requirements to the data within specific geographic or political boundaries. Provide answers only for regions or specific countries where there is concern.

## X. Pricing and Contracts

1. Indicate and describe the licensing model(s) for your MSS/MDR offering.
2. Indicate and describe the pricing model for managing/monitoring virtualized security devices or log sources.
3. Provide the base cost and pricing methodology.
4. Please indicate details on the number of devices or data sources (e.g., networks, workstations, servers) that are included in the cost.
5. Is pricing differentiated according to the sophistication of analytics used?
6. How are costs negotiated for upgrading or expanding services? Can we add devices or data sources without affecting pricing or services?
7. How would the purchase of new security devices (or upgrading our current devices) affect pricing?
8. Provide details on one-time costs and recurring costs.
9. Is there a minimum commitment for usage, total volume, individual spend, or aggregate spend to receive the rates and terms provided in the proposal? If so, explain.
10. The proposal shall remain in force for 120 days from the date of submission.
11. Provide any licensing and warranty information for third-party products you may require Bay County to purchase in support of this service.
12. Indicate the discounts available, based on government, volume of services, and contract length.
13. Will you allow Bay County to test your service for a defined trial period?
14. Indicate any consulting support hours built into your standard MSS/MDR contracts.
15. Indicate hourly or daily pricing for additional consulting hours we can purchase during the MSS/MDR engagement.
16. Indicate any training hours or classes that are built into your standard contracts.
17. Indicate the cost of additional training or classes that may be available.
18. Please explain in detail your contract liability limitations — is this limited by the price of the paid contract?
19. Explain the terms of contract termination and prorated costs that can be recovered.

## XI. Corporate Capabilities

1. Indicate the number of years your company has been in business.
2. Indicate the number of years your company has offered each of the services in the MSS/MDR portfolio.
3. Please provide the number of clients and revenue for each service.
4. Where is your company headquartered? Indicate how many security operation centers (SOCs) you have, and where each one is located.
5. Do you have venture capital or other funding supporting your MSS/MDR business?
6. What percentage of your security service revenue for the trailing 12 months is from MSS/MDRs?
7. What percentage is from security professional services or consulting?
8. What percentage of your company's revenue is spent on MSS/MDR research and development (R&D)?
9. Describe all documented policies, procedures and audit requirements that will ensure maintaining the privacy, and confidentiality of Bay County's data from the data of your other customers.

10. Describe alliances with other companies you have that are related to your MSS/MDRs, such as using third-party software as part of your MSS/MDR portfolio.
11. Does your company subcontract MSS/MDR work to other third parties? If so, please list them, based on the services in scope, and describe your business relationship with each one.
12. Please provide an overview of your plans for continuity of service to Bay County.

**XII. Qualifications and Staffing**

1. Indicate how many MSS/MDR customers you have.
2. Indicate the total number of employees in your company, and the number of employees responsible for MSS/MDR delivery.
3. Please describe the relative distributions of employees in your MSS/MDR company providing delivery, project management, customer service, and how these employees are geographically distributed.
4. What percentage of your staff has security certifications (list the certifications), and what is the average number of years of experience they have in performing security monitoring or security consulting? Are there any differences based on geographic location and/or SOC in terms of your staff's certifications and experience?
5. Please describe the citizenship requirements per geographic location and/or per security operations center for governance purposes.
6. Provide a job description and/or resume for each level of your security-monitoring staff. Include a summary of the technical expertise and/or special capabilities required.
7. Describe the process for screening and hiring your MSS/MDR staff.
8. Explain the process of initial and ongoing training of your security-monitoring staff, including relevant industry-recognized certifications.
9. What is the ratio of monitored security devices to personnel? What is the ratio of managed security devices to personnel?
10. What is the average employment time of an MSS/MDR analyst within your company?
11. Describe your customer support tiers, including the capabilities and location of staff at each tier.
12. Indicate any industry certifications/attestations your security operation centers hold, such as Statement on Standards for Attestation Engagements (SSAE) 16 Type 2, or International Organization for Standardization (ISO) 27001. If so, please provide evidence.

**REQUIREMENT OF BIDDERS:**

1. Each bidder must provide with its formal Bid a written sworn statement certifying that it has not colluded with any competing bidder or County employee or entered into any type of agreement of any nature to fix, maintain, increase, or reduce prices or competition regarding the items covered by this Invitation to Bid.
2. Pricing will only be accepted on the attached Bid Summary form.

**CONTENTS OF BID SUBMISSION PACKET:**

**The submission must be detailed below.**

1. Cover Sheet.
2. Bidder’s Checklist.
3. Certificate.
4. Price sheet.

**The above sections 1-4 are provided at the end of this bid request.**

5. Section I. Implementation and Service Methodology.
6. Section II. Managed Detection and Response.
7. Section III. Security Information Management.

8. Section IV. Advanced Analytics and Capabilities.
9. Section V. Incident Response.
10. Section VI. Vulnerability Management Services.
11. Section VII. Internet of Things Capabilities.
12. Section VIII. Portals, Reports and Dashboards.
13. Section IX. Service Management.
14. Section X. Pricing and Contracts.
15. Section XI. Corporate Capabilities.
16. Section XII. Qualifications and Staffing.

**GENERAL INFORMATION:**

1. CHANGES TO IFB: All additions, corrections or changes to the solicitation documents will be made in the form of a written Change Form signed by Assistant Purchasing Agent, Jesica Foss, only. Firms shall not rely upon interpretations, corrections, or changes made in any other manner, whether by telephone or in person. Additions, corrections, and changes shall not be binding unless made by such a written, signed Change Form. All written, signed Change Forms issued shall become part of the Agreement documents. Change Forms will be sent to all known potential firms by e-mail.

2. CONTACT INFORMATION: To receive future communications related to this IFB, firms are asked to immediately send contact information by email to Jessica Foss, Bay County Assistant Purchasing Agent, at purchasing@baycounty.net; failure to do so may limit your ability to submit a complete, competitive proposal.

3. RIGHT TO WITHDRAW BIDS: By submitting a Bid in response to this IFB, Firm agrees to be bound by this IFB's terms and conditions. Bids may be withdrawn by the Firm without penalty at any time before notification that the Firm's Proposal has been selected. However, if the Firm withdraws after selection of its Bid but before executing the Contract for any reason ("Late Withdrawal"), Firm shall pay liquidated damages to the County in an amount equal to five percent (5%) of the amount of the Bid ("Liquidated Damages"). The County and Firm intend these Liquidated Damages to constitute compensation and not a penalty. The parties acknowledge and agree that the harm caused to the County by such a Late Withdrawal of a Proposal would be impossible or very difficult to accurately estimate at the time of the Late Withdrawal and that the Liquidated Damages are a reasonable estimate of the anticipated or actual harm that might arise from such a Late Withdrawal. Firm's payment of the Liquidated Damages shall be Firm's sole liability and entire obligation and County's exclusive remedy for Late Withdrawal of Firm's Proposal.

4. IFB, PROPOSALS AND ACCEPTANCE DO NOT OBLIGATE: The parties agree that they will not consider either distribution of this IFB or receipt of Bids by the County or even notification of Bid acceptance by the County as an obligation or commitment by the County to enter into a contractual agreement. Rather, the parties understand that the County will have no binding obligation until it signs the Contract approved by its legal counsel.

5. TAX-EXEMPT STATUS: The County is a tax-exempt entity. A tax-exempt form will be provided to the successful firm.

6. FOIA: All bids are confidential until the listed bid opening time and date; however, as a public entity, the County is subject to the Michigan Freedom of Information Act (FOIA). Information contained in the proposals may be subject to FOIA requests.

7. INSURANCE: The Firm shall purchase and maintain insurance sufficient to protect it from any and all claims which may arise out of or result from the Firm's services related to this RFP and any resultant contract, whether such service be by the Firm individually or by anyone directly or indirectly employed by Firm, or by anyone for whose acts Firm may be liable, including independent contractors. Insurance policies purchased and maintained shall include, but are not limited to, the following:

a. Workers' compensation insurance for claims under Michigan's Workers' Compensation Act or other similar employee benefit act of any other state applicable to an employee in the minimum amount as specified by statute.
b. Employer's liability insurance, in conjunction with workers' compensation insurance, for claims for damages because of bodily injury, occupational sickness or disease or death of an employee when workers' compensation may not be an exclusive remedy, subject to a limit of liability of not less than $100,000 each incident.
c. Motor vehicle liability insurance required by Michigan law including no-fault coverage for claims arising from ownership, maintenance, or use of a motor vehicle with liability limits of not less than $1,000,000 per occurrence. Coverage shall include all owned vehicles, all non-owned vehicles, and all hired vehicles.
d. Commercial General Liability insurance for claims for damages because of bodily injury or death of any person, other than the Firm's employees, or damage to tangible property of others, including loss of use, which provides coverage for contractual liability, with a limit of not less than $1,000,000 each occurrence and a mandatory $2,000,000 annual aggregate.

Insurance required shall be in force until acceptance by the County of the entire completed work and shall be written for not less than any limits of liability specified above. Certificates of insurance, acceptable to the County, shall be provided to the County's Department of Corporation Counsel no less than ten (10) working days prior to commencement of the project.

All coverage shall be with insurance carriers licensed and admitted to do business in Michigan, and are subject to the approval of the County.

All Certificates of Insurance and duplicate policies shall contain the following clauses:

1. "It is understood and agreed that thirty (30) days advance written notice of cancellation, non-renewal, reduction and/or material change in coverage will be mailed to Bay County's Department of Corporation Counsel, 515 Center Avenue, Suite 402, Bay City, MI 48708"; and
2. "It is understood and agreed that the following are listed as additional insureds: The County of Bay, including all elected and appointed officials, all employees and volunteers, all boards, commissions, departments and/or authorities and their board members, employees and volunteers."

8. NON-DISCRIMINATION: In the performance of the proposal and resultant contract, firm agrees not to discriminate against or grant preferential treatment to any individual or group on the basis of race, sex, color, ethnicity, or national origin in the operation of public employment, public education, or public contracting. Firm shall not discriminate against any employee or applicant for employment to be employed in the submission of this Proposal or in performance of the duties necessitated by an award of the proposed contract with respect to his or her hire, tenure, terms, conditions or privileges of employment, or any matter directly or indirectly related to employment, because of his or her race, color, religion, national origin, ancestry, gender, height, weight, marital status, age, except where a

requirement as to age is based on a bona fide occupational qualification, or disability that is unrelated to the individual's ability to perform the duties of a particular job or position. Any breach of this provision will be regarded as a material breach of the contract.

9. COST OF DEVELOPING BID: The Firm shall be responsible for all costs incurred in the development and submission of its Bid.

10. QUESTIONS: All questions about this IFB must be received by **APRIL 19, 2024,** 5:00 p.m. in writing, via email, to:
Jessica Foss
Assistant Purchasing Agent
purchasing@baycounty.net

Every attempt to answer your inquiries will be made, however Bay County reserves the right to not answer any questions received after the **APRIL 19, 2024,** due date.

Responses to any inquiries will be issued in one (1) Addendum no later than APRIL 26, 2024, and will be sent to all known firms.

Correspondence or inquiries made directly from firms regarding their proposals are to be directed to those County employees designated above for appropriate review and response. In addition, the person listed above will issue all valid responses and changes to this IFB. Contact with other County staff or County Board Commissioner could be reason for disqualification.

Any significant explanation desired by a firm regarding the meaning or interpretation of the Invitation for Bid must be requested with sufficient time allowed for a reply to reach all prospective firms to submit their proposals. Any information given to a prospective firm concerning the Invitation for Bid will be furnished to all prospective firms as an amendment or addendum to the Invitation for Bid if such information would be of significance to uninformed firms. The County shall make the sole determination as to the significance to uninformed firms.

11. RESPONSIBILITY: Firms are solely responsible for ensuring their bid is received by Bay County Purchasing in accordance with the solicitation requirements, before the date and time specified in this Request, and at the place specified.

Bay County Purchasing shall not be responsible for any delays in mail or by common carrier or mistaken delivery. Delivery of proposal shall be made to Bay County Purchasing, Bay County Building, 7th Floor, Bay City, MI 48708. Deliveries made before the due date and time but to the wrong office will be considered non-responsive unless re-delivery is made to the office specified before the due date and time specified in this request.

12. BID DELIVERY: Bids must be returned no later than **MAY 10, 2024 @ 11:00 A.M.** in a sealed envelope clearly marked **"BAY COUNTY ISD MANAGED DETECTION AND RESPONSE SERVICES (MDR) - DELIVER TO PURCHASING IMMEDIATELY."** Please provide five (5) printed copies of the submission. The submissions may be hand delivered or sent by mail to Bay County Purchasing Office, Bay County Building, 7th Floor, Bay City, Michigan 48708.

**The County will not accept proposals sent by FAX machine or E-mail.**

13. BID OPENING: There will be a public bid opening immediately following the deadline to receive bids in the Bay County Finance Department conference room located in the Bay County Building, 7th Floor, 515 Center Avenue, Bay City, Michigan. All firms are invited to attend and hear the proposals read.

14. BID REJECTION/ACCEPTANCE: The County reserves the right to accept or reject any or all proposals, to waive any irregularities and to make the final determination as to the best low qualified proposal.

15. BID AWARD: In the event the proposal is awarded directly by the Finance Officer, a Notice of Intent to Award will be used to notify all firms of her intent to award the proposal to the Firm providing the best value to the County.

16. CONTRACT: The County's award of any proposal is subject to and conditioned upon execution of a formal agreement for products and services between the successful firm and the County. In submitting a proposal, the firm acknowledges that the contents of the IFB will become incorporated within any formal agreement. This IFB does not include every term and provision which shall be included in the formal agreement. In the event that the firm fails to execute the formal agreement within 14 days of its presentment by the County, the County may reject the selected firm, and proceed to accept another qualified proposal, or reject all proposals.

    A copy of a firm's suggested terms and conditions may be submitted with firm's Bid, however, neither the County's acceptance of any bid nor award of any contract pursuant to this IFB shall be construed as any definitive acceptance by the County of Firm's suggested terms and conditions. In the event of a conflict in terms, the order of precedence to resolve the conflict will be as follows: Michigan State law, the terms and conditions of the signed contract, the terms and conditions of the IFB, and last, the Firm's Proposal.

17. DISPUTES: In the event a firm disagrees with the recommendation of the Bay County Finance Officer concerning this award, the firm may obtain a Bid Protest Form from the Purchasing Office. This form must be completed and returned to Frances Moore, Bay County Purchasing Agent, Bay County Purchasing Division, 7th Floor, Bay County Building, 515 Center Avenue, Bay City, MI 48708-5128, **within ten (10) working days from the date of the notice of intent to award.**

**ADA ASSISTANCE**:
The County of Bay will provide necessary and reasonable auxiliary aids and services, such as signers for the hearing impaired and audio tapes of printed materials being considered, to individuals with disabilities upon two days' notice to the County of Bay. Individuals with disabilities requiring auxiliary aids or services should contact the County of Bay by writing or calling:

Amber Davis-Johnson
Corporation Counsel
Bay County Building
515 Center Ave. 4th Floor
Bay City, MI 48708-5128
(989) 895-4098
(989) 895-4049 TDD

Jessica Foss, Assistant Purchasing Agent
Bay County Finance Department
Purchasing Division
Bay County Building
515 Center Ave. 7th Floor
Bay City, MI 48708
purchasing@baycounty.net

**THIS BID PROCESS WILL BE CONDUCTED IN CONFORMITY WITH THE BAY COUNTY PURCHASING POLICY AS FOUND ON THE BAY COUNTY WEBSITE**

**www.baycounty-mi.gov**

**REST OF THIS PAGE IS INTENTIONALLY BLANK**

**SEE ATTACHED**

**REQUIRED DOCUMENTATION**

**REST OF THIS PAGE IS INTENTIONALLY BLANK**

**NON-BIDDERS FEEDBACK FORM**

Bid #: 2024-09

Managed Detection and Response Services

*If you are not submitting a bid for this Bid, please indicate the reason(s) by checking off one or more items below and email this form to purchasing@baycounty.net.*

_____ Unable to bid at this time but would like to receive future bid requests.

_____ Service(s) or material(s) not provided by our firm.

_____ Service(s) or material(s) we offer do not fully meet all the requirements specified.

_____ We cannot meet the timetable required.

_____ Insufficient time allowed for preparation and submission of bid.

_____ Specifications not clearly understood or applicable as follows: (ex. too vague, too rigid, etc.)

_____ Other: _____
_____
_____

Please remove our name from your bidders list for
_____ This commodity group
_____ These item(s) or material(s)
_____ All bids

Signature: _____

Print Name: _____

Title: _____

Company Name: _____

Company Address: _____

Email: _____

Phone: _____ Date: _____

**Bid Response Cover Sheet**
Bid #: 2024-09
Managed Detection and Response Services

**ALL BIDS MUST INCLUDE THIS COVER SHEET (OR THIS SHEET REPRODUCED ON LETTERHEAD) AS A COVER SHEET OR PAGE ONE (1) OF THE BID**

TO: County of Bay
515 Center Ave, 7th Floor.
Bay City, MI 48708

FROM: _____

Company Name
[ ] an individual,
[ ] a corporation
*(Please mark appropriate box)*,

Duly organized under the laws of the state of: _____

Year Firm Established _____ Years in Business: _____

The undersigned, having carefully read and considered the Invitation to Bid (IFB) for Bay County ISD Managed Detection and Response Services, does hereby offer to perform such services on behalf of the County in the manner described and subject to the terms and conditions set forth in the attached Bid, including, by reference here, the County's IFB document. Bids must be signed by an official authorized to bind the provider to its provisions for at least a period of 90 days.

BY: _____
(Signature of authorized representative)

_____
(Please Print Name and Title)

PRINCIPAL OFFICE ADDRESS:

Street Address: _____

City: _____ County: _____

State: _____ Zip Code: _____

Telephone: _____ Fax: _____

Email: _____

TIN #: _____ UEI #: _____

**BAY COUNTY**
**PURCHASING DIVISION**
**BIDDERS CHECK LIST**
Bid #: 2024-09
Managed Detection and Response Services

| | YES | NO |
|---|---|---|
| 1. I have read ALL the instructions and specifications. | _____ | _____ |
| 2. I have read and acknowledge the information contained in the "General Information" section of the Bid | _____ | _____ |
| 3. I have filled in ALL the required documentation. | _____ | _____ |
| 4. I have provided all required information per the guidelines specified within the bid document. | _____ | _____ |
| 5. I am an officer of the company. | _____ | _____ |
| 6. I have the authority to obligate my company. | _____ | _____ |
| 7. I am returning the signed ORIGINAL and specified number of copies required per the bid document | _____ | _____ |
| 8. I have organized and labeled the bid per instruction. | _____ | _____ |
| 9. I have retained a copy of the submission. | _____ | _____ |
| 10. I have properly labeled the external envelope. | _____ | _____ |
| 11. If successful, the "Insurance Requirement Certificate" from an insurance company licensed to do business in the State of Michigan will be provided within ten working days after Notification of the award. | _____ | _____ |
| 12. I have provided the necessary information for the person responsible for follow-up. | _____ | _____ |

Signature: _____

Print Name: _____

Title: _____

Company Name: _____

Company Address: _____

_____

Phone Number: _____ Fax Number: _____

E-mail Address: _____

Date: _____

**CERTIFICATION**

Bid #: 2024-09

Managed Detection and Response Services

The individual signing below certifies:

1. They are fully authorized to submit this bid, including all assurances, understanding and representations contained within it which shall be enforceable as specified.

2. The individual has been duly authorized to act as the official representative of the firm, to provide additional information as required and, if selected, to consummate the transaction subject to additional, reasonable standard terms and conditions presented by County.

3. This Bid was developed solely by the Firm indicated below and was prepared without any collusion with any competing firm or County employee.

4. The content of this Bid has not and will not knowingly be disclosed to any competing or potentially competing firm prior to the Bid opening date, time, and location indicated.

5 No action to persuade any person, partnership, or corporation to submit or withhold a bid has been made.

Signature: _____

Print Name: _____

Title: _____

Company Name: _____

Company Address: _____

_____

Phone Number: _____

Fax Number: _____

E-mail Address: _____

Date: _____

**ATTACHMENT B**

**BID SUMMARY**

Bid #: 2024-09

Managed Detection and Response Services

| | |
|---|---|
| **Service Management** | **$** |
| Equipment (If Applicable) | **$** |
| Management and Detection Response | **$** |
| Implementation | **$** |
| Incident Response | **$** |
| **Total Bid Price** | **$** |

Signature: _____

Print Name: _____

Title: _____

Company Name: _____

Company Address: _____

_____

Phone Number: _____

Fax Number: _____

E-mail Address: _____

Date: _____