Request for Proposals –
Managed Security Services
Issued February 7, 2020

Table of Contents

MARC Organizational Structure and Activities ................................................................. 1
Objectives .......................................................................................................................... 1
Current Environment ......................................................................................................... 2
Proposal Requirements ..................................................................................................... 2
Questions ........................................................................................................................ 5
Response Requirements .................................................................................................. 5
Questions ........................................................................................................................ 5
Engagement ...................................................................................................................... 5
Response Requirements .................................................................................................. 6
Anticipated Schedule for Vendor Selection ....................................................................... 6
Evaluation Criteria ........................................................................................................... 6
Open Records Act and Proprietary Information ................................................................ 7

Closing Date and Time for Proposals – March 9, 2020, by 4 p.m. CDT
Contact Information – Sasan Baharaeeen, Information Technology Program Director,
sasan@marc.org
REQUEST FOR PROPOSALS
Managed Security Services

MARC Organizational Structure and Activities

The Mid-America Regional Council (MARC) is the metropolitan planning organization and association of city and county governments serving the bistate Kansas City region. It is a public, nonprofit agency. MARC serves 119 cities within a nine-county area, including Cass, Clay, Jackson, Platte and Ray counties in Missouri; and Johnson, Leavenworth, Miami and Wyandotte counties in Kansas.

MARC was formed in 1972 and is governed by a 33-member board of directors composed of city and county elected officials. In addition to the board, MARC has dozens of policy, technical and advisory committees and decision-making entities overseeing its work and providing important and diverse stakeholder involvement. This series of committees and working groups enables MARC to engage a diverse array of community interests and representatives from often under-represented constituencies.

The board and committee activities are supported by a professional staff headed by an executive director who is appointed by the board. MARC currently has more than 140 employees working in six departments: aging and adult services, community development, early learning, research services, financial affairs and transportation and environment. MARC services are funded by a variety of sources including contributions by member governments; formula and discretionary grants from Missouri, Kansas and the federal government; and contributions for specific programs from private foundations and civic organizations.

Objectives

MARC is requesting proposals from qualified vendors to provide Managed Security Services for Threat monitoring, SEIM and log management, and Event investigation for all devices. **Vulnerability Management should be included in the proposal as an optional service.** The proposal will be for services provided directly to MARC; however, the proposed pricing will be made available to MARC member governments. Although MARC will select its own system, the selected proposals will be made available to member governments who may select the product based on any signed agreements with MARC.

A proposer’s preparation and submittal of a proposal or subsequent participation in presentations or contract negotiations creates no obligation on MARC to award a contract or to pay any associated costs. All proposals and related materials will be retained by MARC and will be subject to disclosure as required in accordance with the Missouri Sunshine Law.
REQUEST FOR PROPOSALS
Managed Security Services

Current Environment

MARC uses Microsoft Hyper-V with two hosts and 35 virtual servers. Ten servers have external IP addresses. We have around 200 workstations and one firewall. More detailed information will be provided to verified vendors.

Proposal Requirements

- Company information
  - List your company’s legal name, address and telephone number.
  - Indicate the number of years your company has offered Managed Security Services (MSS) services.
  - Where is your company headquartered? Indicate how many security operations centers (SOCs) you have and where each one is located.
  - Describe all documented policies, procedures and audit requirements that will ensure maintaining the privacy and confidentiality of MARC’s data from the data of your other customers.
  - Describe alliances with other companies you have that are related to your MSSs such as using a third-party software as part of your MSS portfolio.
  - Does your company subcontract MSS work to other third parties? If so, please list them based on the services in scope and describe your business relationship with each one.
  - Are all your staff and contractors located in the United States?
  - Please provide an overview of your plans for continuity of service to MARC.

- Qualifications and staffing
  - Indicate how many MSS customers you have.
  - Please provide a list of MSS customers in the nonprofit and government industry. This should include three or more references of companies using your service that are of similar size to MARC.
  - Indicate the total number of employees in your company and the number of employees responsible for MSS delivery.
  - Please describe the relative distributions of employees and SOCs in your MSS company and how these are geographically distributed.
  - What is the average employment time of an MSS analyst within your company?
  - Describe the process for screening and hiring your MSS staff.
  - Explain the process of initial and ongoing training of your security monitoring staff.
  - What is the ratio of monitored security devices to personnel? What is the ratio of managed security devices to personnel?
  - Describe your customer support tiers, including the capabilities and location of staff at each tier.
  - Indicate any industry certifications your security operation centers hold.
REQUEST FOR PROPOSALS
Managed Security Services

- Implementation and services methodology
  - Provide a brief overview of your managed security services and any supporting products.
  - Are your SOCs staffed 24 hours a day, 365 days a year? Describe your approach to supporting 24/365 remote security event monitoring and device/agent management.
  - Describe the architecture of your MSS 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. Provide example architectural diagrams and descriptions. Include and identify any elements that are delivered by third-party partners.
  - 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, and case management and workflow.
  - Explain how these services, and any supporting products, will use or interface with products MARC has in place for Firewall management, information event management and log monitoring. Be sure to include details on how you intend to connect to MARC’s infrastructure to provide support.
  - Will your services require the use of proprietary technology that MARC 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.
  - Explain how you use external data (e.g., threat intelligence feeds) to analyze potential threats to MARC’s environment and describe our level of access to this data.
  - 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 the methods of notification.
  - Indicate if your services can also be delivered in our Office 365/Azure environment. If so, provide associated costs as separate options. Also, include technology and contractual or licensing requirements related to provisioning, ongoing monitoring and de-provisioning of services to the cloud infrastructure.
  - Explain infrastructure requirements; data transfer, data storage and segregation, and backup systems; and encryption standards.
  - Please provide an example of how your services detected and addressed a recent security incident.
  - Explain your methodology for detecting custom or targeted attacks directed at our users or systems.

- Security event monitoring
  - Indicate the capabilities of your services to monitor our firewall, intrusion detection system (IDS), intrusion prevention system (IPS), and Active Directory data.
  - Explain your ability to analyze this data and to provide real-time event correlation between data sources and real-time alerting of security incidents and system health incidents.
REQUEST FOR PROPOSALS
Managed Security Services

- Explain your ability to analyze this data to identify when changes in behaviors of users or systems represents risk to our environment.
- Explain your methodology for reducing false positives and false negatives and for classifying security related events that represent a risk to MARC.
- Describe how false positives are managed, and how your company will incorporate false positive feedback from MARC.
- Describe the typical workflow and process that occurs when the security analytics detects a security event, beginning with how that is presented to a SOC analyst for evaluation through the triage, validation, prioritization and customer alerting/notification process. Indicate where activities are automated versus manually performed by analysts.
- Indicate the level of interaction and support that our staff can expect from your security analysts to assess, investigate and respond to incidents.

- Service management
  - Explain the expected working relationship, roles and responsibilities between your security staff and our staff.
  - Indicate device/agent management and real-time event management notification service levels. Explain how they are measured and how they will be communicated to us.
  - Describe your problem resolution and escalation procedure.
  - Please provide details on support agreements.
  - Describe the process for adding services or new technologies.
  - 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?
  - 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?
  - Describe the process if we have a complaint.
  - Indicate your process for notifying us of your noncompliance with the Service Level Agreement
    - Describe the remedies available to us should you fail to meet any SLAs
  - Outline early termination penalties and charges. Describe how the costs are calculated to extract all captured data to be moved to another vendor, if applicable?
  - Describe how we would obtain our data during the separation process.
  - Describe how our data (including data generated by your company about security events and incidents affecting MARC) will be governed and protected in transit. Consider this from a technology perspective, as well as via processes and procedures.

- Vulnerability management services
  - Indicate the technologies used to conduct scans, both commercial and open source.
  - Provide details on your methodology for collecting and analyzing vulnerability and asset data (e.g., configuration) from all sources in scope.
  - Describe the process by which vulnerabilities are triaged and prioritized prior to reporting, including the integration of previous scan.
REQUEST FOR PROPOSALS
Managed Security Services

- 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.
- How can vulnerability scans be scheduled and initiated/managed via your MSS portal? How are results viewed in the portal?
- Indicate what frequency your MSS can scan our environment.
- How frequently is the vulnerability database updated and what are the data sources used for that?

- Pricing
  - Please provide the name, title and appropriate contact information of the authorized negotiator or contract-signing agent.
  - Provide details on one-time costs and recurring costs.
  - Indicate and describe the licensing model(s) for your services.
  - Provide the base cost and pricing methodology.
  - Please indicate details on the number of devices or data sources (e.g., IDS sensors, firewalls and servers) that are included in the cost.
  - How are costs negotiated for upgrading or expanding services? Can we add devices or data sources without affecting pricing or services?
  - How would the purchase of new security devices (or upgrading our current devices) affect pricing?
  - Provide any licensing and warranty information for third-party products you may require us to purchase in support of this service.
  - Indicate the discounts available based on volume of services and contract length. Is nonprofit or government pricing available?
  - Will you allow us to test your service for a defined trial period?
  - Indicate any consulting support hours built into your standard contracts.

Questions

All questions regarding this Request for Proposals (RFP) should be directed to Sasan Baharaeen by email at sasan@marc.org by March 2, 2020.

Response Requirements

Responses to this Request for Proposals should be directed to Sasan Baharaeen NO LATER THAN 4 p.m. CDT on March 9, 2020. Responses can be submitted in print or electronic formats. Printed responses should be delivered to:

Sasan Baharaeen
Mid-America Regional Council
600 Broadway, Suite 200
Kansas City, MO 64105
REQUEST FOR PROPOSALS
Managed Security Services

Electronic submittals should be emailed in PDF format to Sasan Baharaeen at sasan@marc.org.

Note: It is the responsibility of the vendor to verify the receipt of proposals or any related electronic communication by MARC staff as there is always the possibility of emails getting blocked by MARC’s firewall/spam filter.

Engagement

This Request for Proposals does not commit MARC to award a contract or to pay costs incurred in the preparation of a proposal in response to this request. MARC reserves the right to accept or reject any or all responses received as a result of this request if it is considered in the best interest of MARC. MARC may require the selected proposer to participate in negotiations and to submit price, technical or other information as needed to finalize a particular engagement for services.

Anticipated Schedule for Vendor Selection

The following schedule will be used for the selection of a vendor.

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue Request for Proposals</td>
<td>February 7, 2020</td>
</tr>
<tr>
<td>Deadline for Questions and Requests for Further Information</td>
<td>March 2, 2020</td>
</tr>
<tr>
<td>Deadline for Proposals</td>
<td>March 9, 2020, by 4 p.m. CDT</td>
</tr>
<tr>
<td>Select Preferred Vendor</td>
<td>March 25, 2020</td>
</tr>
<tr>
<td>Finalize Agreement and Issue Notice to Proceed</td>
<td>Week of April 1</td>
</tr>
</tbody>
</table>

Evaluation Criteria

The proposals submitted by each vendor will be evaluated by an internal committee of MARC staff according to the following factors:

A. Technical
   a. Experience and expertise
   b. Effective demonstration of similar projects
B. Quality, reliability, completeness and efficiency of the technical approach.
C. Physical presence in United States
D. Ability to complete the project in a timely manner
E. Price

During the evaluation process, MARC staff reserves the right, where it may serve MARC’s best interest, to request additional information or clarification from proposers or to allow corrections of errors or omissions.
Open Records Act and Proprietary Information

The Mid-America Regional Council (MARC) is a public organization and is subject to the Missouri Open Records Act (Chapter 610, RSMo). All records obtained or retained by MARC are considered public records and are open to the public or media upon request unless those records are specifically protected from disclosure by law or exempted under the Missouri Sunshine Law.

All contents of a response to a Request for Bids, Qualifications, Proposals or information issued by MARC are considered public records and subject to public release following decisions by MARC regarding the bid request. If a proposer has information that it considers proprietary, a bidder shall identify documents or portions of documents it considers to contain descriptions of scientific and technological innovations in which it has a proprietary interest, or other information that is protected from public disclosure by law, which is contained in a Proposal.

After either a contract is executed pursuant to the Request for Bids, RFQ or RFP, or all submittals are rejected, if a request is made to inspect information submitted and if documents are identified as “Proprietary Information” as provided above under Missouri Sunshine Law, MARC will notify the proposer of the request for access, and it shall be the burden of the proposer to establish that those documents are exempt from disclosure under the law.