Questions and Answers No. 4
Request for Proposal MDM0031023850
Systems Operations Support RFP
January 26, 2016

Ladies/Gentlemen: This list of questions and responses is being issued to clarify certain information contained in the above referenced RFP. Nothing in MHBE’s response to these questions is to be construed as agreement to or acceptance by the MHBE of any statement or interpretation on the part of the Offeror.

1. **Question:** Section 4.1 of the RFP outlines the proposal submission requirements via email. Is there a mailbox size limitation for the vendors who are submitting files?

**RESPONSE:** The MHBE requests that all submissions be provided in zip files of size not exceeding 25 MB.

2. **Question:** Section 4.1 of the RFP outlines the proposal submission for the Technical submissions. Are vendors allowed to submit individual files (per Tab) included in one zip file or are vendors required to submit one file inclusive of Tabs A through M?

**RESPONSE:** Vendors are allowed to submit individual files (per Tab) included in one zip file.

3. **Question:** Section 4.4.2.7 (Staffing Plan) does not have a Tab designation. Should the Staffing Plan fall under Tab E, or should we create a Tab E-1 for that section?

**RESPONSE:** Vendors should include the Staffing Plan under Tab E.

4. **Question:** Please provide the number of MHBE-approved current workarounds that are in scope of this RFP and associated effort or average effort taken for each.

**RESPONSE:** Standard operating procedures will be adopted in the event of any disruption to infrastructure, production or batch activities. Average effort to implement the approved current workaround is about 20-40 minutes.

5. **Question:** *Questions and Answers No. 1*, issued by MHBE and dated 1/15/2015, states that there were 26 Severity Level 1 and 47 Severity Level 2 incidents for the 2015 calendar year. What percentage of these incidents is in the scope of work of this RFP?

**RESPONSE:** All of the incidents referred to are in scope of this RFP. However, MHBE acknowledges that there are instances where combined efforts of different vendors and/or MHBE team are required to resolve the incidents.
6. **Question:** Is the initial triage of all IT Incidents part of this RFP or only the incidents related to the scope of the work in this RFP?

How many request for changes (RFCs) were released to production in 2015? How many were application-related and how many were infrastructure-related?

**RESPONSE:** Yes, initial triage of all IT incidents are part of this RFP, please refer to the response to the question 5 above for additional related information. We will not be providing Request for Change (RFC) statistics.

7. **Question:** How many IT audits were conducted in 2015?

**RESPONSE:** There are multiple audits in progress related to business and IT policies, procedures and governance. However, not all of the audits are focusing exclusively on IT.

8. **Question:** If the inbound file processing is delayed the probability of file availability for the external Contractor/Partner is very high and will most likely get delayed. Will MHBE remove the SLA for Inbound File Processing to avoid a duplicate penalty because the issue is the result of the same chain of events?

**RESPONSE:** The SLA will not be removed.

9. **Question:** Is it acceptable to the State if a vendor provides an alternate form of security (such as a letter of credit or a bank guarantee) equivalent to the amount asked in Performance bond?

**RESPONSE:** No. Pursuant to Section 1.41.3 of the RFP, "Acceptable security for the Performance Bond is limited to a bond in a form satisfactory to the MHBE underwritten by a surety company authorized to do business in this State."

10. **Question:** Is the State willing to mutually discuss and agree on the liquidated damages?

**RESPONSE:** No. While the liquidated damages provisions may be changed via amendment to the RFP, MHBE chooses not to issue such an amendment at this time.

11. **Question:** For unlimited liability clause, would State allow for a cap on the liability?

**RESPONSE:** No. While liability provisions may be changed by amendment to the RFP, MHBE chooses not to issue such an amendment at this time.

12. **Question:** Please provide details on any key Business and IT related challenges faced by the State with respect to the current contract / vendor.

**RESPONSE:** We will not be providing this information.
13. **Question:** Please provide a complete list of the application inventory in scope, with:
   - Application name
   - Brief description
   - Technology stack
   - Business Criticality level
   - Complexity level
   - Stability
   - Third party products/tools/custom tools, etc. used/referred by the application
   - No. of internal and external interfaces
   - No. of Reports
   - No. of Batch jobs
   - FTEs currently supporting (if it can be disclosed)
   - Current support locations
   - Key current / upcoming Application Imperatives (such as Upgrade, decommissioning etc.)
   - Regulatory/audit considerations
   - Special language considerations
   - Tickets volume for last 14 months and their severity levels along with the categorization (Incidents, Adhoc requests, Problem Management tickets etc.)
   - Current Ticket backlog
   - Please provide the following for each technology / tower
     - # of Change requests (with breakup by classification, Ex - Normal, Standard, Emergency)

**RESPONSE:** Please refer to RFP Section 3 Scope of Work, associated attachments, amendments and responses provided to vendor questions.

14. **Question:** In the answer set 1, influx of severity 1 and severity 2 tickets has been given. There are no information for Severity 3 and severity 4. Are there any system to track severity 3 and severity 4 tickets? if there are, Could that information be provided for last year across applications and technologies in scope?

**RESPONSE:** There is an information system run by the current hosting vendor to track severity 3 and severity 4 tickets. The severity 3 and 4 tickets are predominantly managed by the hosting vendor and no further information on this will be provided.

15. **Question:** Are there any Peak and off-peak time frames in a year and on a typical day for each of the applications in scope.

**RESPONSE:** The system peak hours are from 8 am to 5 pm every day of the week. However, during Open Enrollment periods, the peak system hours may vary.

16. **Question:** Please confirm whether there is a Known Error Database available with the State / Incumbent Vendor. If yes, we assume that the database will be accessible to the new contractor. Please confirm.
    Are there any statistics available on what % of tickets in the last 14 months were Known Errors?
RESPONSE: The new contractor will be provided with the requested information.

17. Question: Please provide 1) Typical size of changes 2) No. of changes done in the past 12 months 3) Average monthly effort spent on Change Requests as described in Section 3.2.1.9 Incident Management.

RESPONSE: We will not be providing this information.

18. Question: Are the monitoring mechanism integrated with the Ticketing tool as described in Section 3.2.1.4-Monitor and Execute Schedule System Activities (Batch Jobs)? If yes kindly advise if the Classification, Prioritization are done by the Helpdesk team or if it is automated.

RESPONSE: No, system monitoring functions are not integrated with ticketing tool.

19. Question: Can the MHBE please provide the total number and type of servers (Virtual & Physical) considered under scope for Monitoring and Management. A server inventory is preferred which includes information such as location, make, model, OS version, hardware configuration, criticality, environment and purpose (web/ application / DB etc). Can the MHBE please also provide the no. of WEBSPHERE instances and sites hosted in it also confirm the parameters which are being continuously monitored on all the servers (Sample Answer: % CPU utilization, memory thrashing, % disk utilization)? (Reference Section 3.2.1.5 Monitor Server Resource Utilization)

RESPONSE: The requested information will not be provided. However, please refer to the Amendment 2 under Appendix A HBX System Overview, Hardware and Software List for information related to the request.

20. Question: What are the parameters that are monitored for capacity planning? Are there any threshold values which act as trigger for upgrades?

RESPONSE: Please refer to RFP Section 3.2.1.6 and Appendix D Sample Capacity Plan. Capacity upgrade decisions will be made in collaboration with the System Operations Contractor, Hosting Vendor and MHBE.

21. Question: In the event of a disaster or significant disruption, does your organization have documented plans for business continuity and IT disaster recovery? If yes, please provide details on the type of failure scenarios and outages you plan for and the duration of time for that is assumed for each of the scenarios.

RESPONSE: Yes, MHBE has documented plans and procedures for IT disaster recovery. We will not be providing the details requested. However, the Contractor upon NTP will be provided such information.
22. **Question:** Do you have DR plans in place or a DR program that the MHBE documentation will align with? Do you have Post Test Reporting for previous DR tests? How are existing DR plans stored and maintained? Will the provider be responsible for DR support at time of incident for the infrastructure, Databases and applications? Is there a CMDB (Configuration Management Database) in place today? And, is the CMDB maintained in a database or on file system?

**RESPONSE:** Yes, MHBE has documented plans and procedures for IT disaster recovery. We will not be providing the details requested. However, the Contractor upon NTP will be provided such information. The Disaster Recovery (DR) plans are stored electronically in a system that is not hosted in the production data center.

23. **Question:** Can the MHBE please provide the number of Remote machines in which the Scheduling agents are installed?

**RESPONSE:** At this time we have less than 5 installed.

24. **Question:** Has High Availability solution been implemented for critical databases? If Yes, for each technology, please share
1 - Technologies used (RAC, Dataguard, Streams, OS Cluster, etc)
2 - For each DB technology, # of Databases that are in HA (alternately, percentages can also be provided (Ex - Oracle: 5% of the total Databases are in HA))

**RESPONSE:** 1 - DB2 HADR (High Availability Disaster Recovery), SQL Server (Cluster)
2 - DB2 50% and SQL 50%

25. **Question:** Can the MHBE please share the details of the replication tools in use by DB technology?

**RESPONSE:** Currently the DB is synchronized using DB2 HADR.

26. **Question:** Can the MHBE please share the following - (i) Number of firewall that needs to be managed in Data Center and Disaster Recovery and Vendor details; (ii) Number of rules configured on each of the firewall?

**RESPONSE:** This information will not be provided. Managing firewalls is the responsibility of the hosting vendor.

27. **Question:** Can the MHBE please share the following: (i) Number of endpoints which are being managed by the anti-virus (Symantec); (ii) Number of events generated (EPS) and logs managed (No of log collectors, connectors) by QRadar. (Per day, Quarterly, yearly etc.)?

**RESPONSE:** This information will not be provided.

28. **Question:** Can the MHBE please share the number of applications configured in Site Defender (Akamai Kona) for management.
RESPONSE: This information will not be provided. The maintenance of Akamai is not part of the scope of this RFP.

29. **Question:** Is PKI managed and issued by external vendor? Is there any portal to manage the services?
   - What is the number of certificates to be issued and managed per year? Please also mention the purpose of those certificates issued? (Ex: Web server certificate?)
   - Can the MHBE please share Key management and archival policy?

RESPONSE: This information will not be provided.

30. **Question:** Is there any HCM for storing and protecting the keys? Please also mention the HCM policies for managing the keys.

RESPONSE: This information will not be provided.

31. **Question:** Can the MHBE please share the kind of support for Firewall, Site Defender, Anti-virus, Symantec and Qradar currently in place? (Ex: Premium support, Gold support etc.). Can the MHBE please also share the license and support details?

RESPONSE: This information will not be provided.

32. **Question:** There are a lot of terminologies mentioned like Data encryption at rest, encryption need at Disk level, file level done via SAS Encryption and via SSL or TLS in transit. Can the MHBE please clarify the exact requirements for this RFP under the purview of Encryption?

RESPONSE: The encryption related requirements of the RFP do not exceed beyond the RFP Section 3 Scope of Work.

33. **Question:** Section 3.8.3 references Information Security, does it require key management for securing the key and key-rollover for a definite period of time? If so, is there any existing Key management solution already in place that can be leveraged for this solution or needs to be newly considered for this RFP response?

RESPONSE: The existing process for key management shall be utilized.

34. **Question:** Does the need for data masking extends to the non-production environment of Dev, Testing, SIT and Training Environments? Does MHBE have an existing masking solution that can be leveraged? Please provide details. If not, can we propose our own data masking tool if required?

RESPONSE: Due to security concerns, this question will not be answered. However, there is no production data in the environments referenced in this question.
35. **Question:** We understand that IBM Optim is currently used in the production environment, for data masking via Encryption or Tokenization? Please validate and provide details on its usage and scope.

**RESPONSE:** The statement referred related to IBM Optim is incorrect. The contractor shall support any security solutions suggested by MHBE to meet the requirements of RFP Section 3 Scope of Work.

36. **Question:** Can the MHBE please provide the type of Data stores need masking? Section 3.8.3-Information Security mentions that Staging requires 100 GB data with daily refresh but please confirm how much of it is needed related to masking in Non Production environments.

**RESPONSE:** Due to security concerns, this question will not be answered. However, the contractor shall support the security solutions suggested by MHBE to meet the requirements of RFP Section 3 Scope of Work.

37. **Question:** We understand that you have different data stores for non-production environments, is the data from a single common DB repository or does every environment have its own data storage or DB? Does Content Manager, DB2, Files indicate redundant data? Please validate and confirm.

**RESPONSE:** Each environment has unique data storage or database (DB). In the lower tiers there is a combination of shared and unique DB stores depending on the environment. There is no redundant data in the content manager.

38. **Question:** Are EDI or X12 files in scope for encryption purpose? Please clarify.

**RESPONSE:** Yes.

39. **Question:** Please confirm the following for Vulnerability Assessment:
   1. Number of web Apps for Dynamic Application Security Testing -
   2. Line of Codes for Static Application Security Testing -
   3. Infrastructure Security Testing volumetric details
   4. Application Penetration Testing volumetric

**RESPONSE:** Due to security concerns, the requested information will not be provided.

40. **Question:** If Infra Vulnerability assessment is in scope, then how many total IP addresses (internal+external IP's) would be in-scope for assessment? Does the IP addresses belong to the State or to a third party?

**RESPONSE:** RFP Section 3 Scope of Work covers the work expected of the Contractor. Due to security concerns, the IP address related requested information will not be provided.

41. **Question:** We understand there is IBM Security Identity and Access (IAM) tools that exist in the current security landscape, pls. confirm the following:
1. Version of ISAM for Access Management
2. Version of ISIM for Identity Management if any
3. Any other Identity & Access Management COTs tool from IBM or other vendor such as: (i) Federated Identity Management, (ii) Privileged Identity Management (iii) Adaptive Authentication / Multifactor Authentication or (iv) Access Governance / Recertification
   - Platform/technology details
   - Overview of currently functionalities implemented

           3. No

42. Question: Can the MHBE identify the list of Identity Management Use Cases Currently Supported?

   (i) No. Provisioning Targets and technology details
   (ii) List of Workflows Supported
   (iii) Number of Upstream (Authoritative Source) Systems Please provide insights on ISAM existing integration for SSO and Protocols supported for the following:
      (i) number of WEB applications integrated with ISAM
      (ii) number of partner applications integration for Federation if any
      (iii) number of Mobile applications integrated with ISAM
      (iv) Is there any Enterprise SSO implementation currently supported?

RESPONSE:  (i). Approximately 25-30, ISAM, Active Directory, SQL Server and DB2
           (ii). Operational workflow is supported.
           (iii). None.
              (i). Three.
              (ii). None.
              (iii). None.
              (iv). None.

43. Question: Can the MHBE please provide details about IBM Data Power Web Service Authentication process and list of Use cases currently supported?

RESPONSE: Authentication happens through Certificate authentication and user ID password. Currently there are two use cases supported.

44. Question: Can the MHBE please provide the volumetric details for: (i) Average number of ISIM/ISAM L1/L2/L3 tickets / month; (ii) average number of Security Device (Firewal, VPN, SIEM, Antivirus etc) L1/L2/L3 tickets / month?
RESPONSE: Due to security concerns, this question will not be answered. The hosting vendor manages the security devices as well such as firewall, VPN, SIEM and AV. The contractor is expected to perform operational support activities as specified in the RFP Section 3 Scope of Work.

45. **Question:** Can the MHBE please confirm if Microsoft AD is an Authoritative Centralized User Store for Authentication? Please provide the AD details such as number of domain and forest etc. Can we assume that all the users gets authenticated from the centralized user store and authorized at the application DB/Directory level? What is total user base? Please provide the same by User types only.

RESPONSE: Due to security reasons, the requested details related to Active Directory (AD) will not be provided. AD is only used for infrastructure management and will not be the responsibility of the system operations RFP Contractor.

46. **Question:** Can the MHBE please provide details on Security devices/Security Event Management /Identity & Access Management support requirements related to: Level of support required, is it L1/L2/L3? ; Support coverage is it 8*5, 16*5, 24*5, 24*7 or any other?

RESPONSE: The Offeror is requested to refer the RFP Section 3 Scope of Work and specifically Section 3.4 Service Level Agreements (SLA) for service level metrics and measurements.

47. **Question:** Can the MHBE please confirm if a.) The vendor can propose shared resources model and b.) Remote location can be Offshore Delivery Center outside US.

**RESPONSE:** MHBE is soliciting dedicated System Operations vendor staff under this RFP. Remote location cannot be offshore delivery center outside the United States.

Date Issued: January 26, 2016  
Michelle Compton  
Procurement Officer