

**Midwestern Higher Education Compact
Mobile Device Management and Related Services
Request for Proposal's
Vendor Questions and Answers
June 25, 2013**

Vendor A

Q1. What data security regulations are you required to adhere to?

A1. Several subject areas of higher education have laws and regulations governing the use of information technology for example: Federal (GLBA), State Statute(s), Employees (EEO-Civil Rights Act), Financial and Banking (PCI), Healthcare (HIPAA), Research, and Students (FERPA). This example does not include all information security and privacy laws and regulations an individual entity would or may require.

Q2. What are your top 4 general selection priorities for the mobility solution?

A2. 1) Meets the functional specifications of this RFP; 2) Shows willingness to explore solutions beyond a standard purchase agreement; 3) Displays innovation; and 4) Completeness, thoroughness and detail of response as reflected by the proposal's discussion and coverage of all elements of this RFP.

Q3. Do you have a rough idea of potential device quantities/volume?

A3. The potential is hundreds of thousands. MHEC has over 1000 Higher Education institutions or four million students across the 12-member Midwestern states, plus K-12 and an option to expand to states within the other three regional higher education compacts. Please reference Section E (page 6) of the RFP: Eligible Participants.

Vendor B

Q4. Will there be one award?

A4. MHEC may award one or more awards, depending on the range of options available to meet the needs of the region. Reference Section Q. Provider Selection.

Q5. Will this be the standard Mobility for all the agencies below (i.e, the winning manufacture is more a less sole source on the mobility needs of the below colleges).

A5. No.

Q6. Is there going to be a minimum order.

A6. No.

Q7. Will each agency be purchasing on their own based on the banded pricing they are expecting

A7. Yes.

Vendor C

Q8. How can vendor update information (including and not limited to - technical features, price, implementation, subcontractors) in the system after it has been initially incorporated.

A8. In the event a contract is awarded, the vendor will maintain with MHEC the most current product and service schedule offered under this agreement.

Q9. Please describe a typical use case scenario, procurement flow process for MDM software through MHECTECH.

A9. Each entity will have varying levels of delegated authority for making purchases. Eligible entities can purchase directly from MHEC contracts with the assurance that the competitive vetting process has already been statutorily complete. The procurement process may include a quote or statement of work for the MDM solution with a reference to the MHEC contract number. The entity has the right to review the contract terms and conditions and add an addendum as necessary.

Q10. How do MHECTECH compact members access information and initiate the procurement process.

A10. Please note the States are the members and the entities within the state: public and not-for-profit Higher Education, K-12, State agencies, and local government; are eligible to utilize MHEC contracts. Institutions have access to all of MHEC's contracts at <http://mhectech.org>. The vendor is expected to provide support information, marketing, and a commitment to educate their sales force.

Q11. What restrictions (if any) are in place for conducting business with members of the compact independent of MHECTECH procurement process.

A11. The Master Price Agreement will outline the expectations of the vendor when conducting business with eligible entities. Member states may have additional requirements for procurement compliance.

Q12. Can we nominate/update subcontractors from our list of partners, in real-time (relative to system being updated) and ongoing basis.

A12. Yes, authorized reseller lists can be updated.

Q13. Due to individual purchasing entity requirements, can the scope of our installation and order fulfillment be as wide and deep as needed for each particular requirement.

A13. Yes, eligible institutions will separately negotiate installation of services based on their requirements.

Q14. Do we need to provide breakdown of pricing such as license fees, install and deployment costs, ongoing support and maintenance or can we have a comprehensive price.

A14. Yes, either option is acceptable. However a comprehensive listing of all products and services (SKUs) is recommended.

Q15. Please describe the administration fee – is it a fixed annual subscription fee, per acquisition fee, per invoice charge or any other variation

A15. The fee for all purchases typically ranges from 0.05% on contracts over \$100 million or so, to 2% on contracts under a million. We're asking you to suggest a number.

Q16. Please describe the global procurement (outside the US) scenario – in terms of types of entities and countries

A16. The intent is to address U.S. institutions with a campus presence or deliveries degree programs abroad, e.g. China or Belize.

Q17. Will information populated about our offering be available in the public domain or restricted to members.

A17. Yes, contract information will be available in the public domain.

Vendor D

Q18. Does MHEC have an existing help desk infrastructure or do you desire a mobility help desk solution be included in the response?

A18. No, MHEC does not have a helpdesk. Yes, eligible institutions may be seeking a mobility helpdesk solution.

Q19. Does MHEC have any security requirements that need to be considered in defining the solution?

A19. Please refer to Vendor A, Q1 above for the answer.

Q20. On Page 9 item 20 - Administration fee. Please provide an example of an administration fee that is in place today?

A20. Please refer to Vendor C, Q15 above for the answer.

Q21. Section III Maintenance on page 14 discuss warranties, Does MHEC desire the respondents include mobile devices such as tablets included in the solution or does the warranty discussion relate only to MDM hardware?

A21. No, MHEC does not desire bids for mobile devices or tablets. Do include any hardware responses that are necessary for the implementation of the solution.

Q22. For sizing purposes, do you have an estimate of the initial number of devices that the MDM system will support?

A22. Please refer to Vendor A, Q3 above for the answer.

Q23. Will this MDM environment be strictly BYOD, or will there be a combination of personal and corporate liable devices?

A23. There will be a combination of both personal and institutional owned devices.

Q24. What annual growth do you expect?

A24. This is unknown and dependent on the vendor's sales growth and promotion of the MHEC

contract.

Vendor E

Q25. Page 9, Item 20. Mentions an “administration fee” for MHEC. Can please clarify and provide more information about the expected percentage of this fee?

A25. Please refer to Vendor C, Q15 above for the answer.

Q26. What vendors are expected to respond to the RFP? What vendors have submitted a response already or inquire about a submission?

A26. This is a competitive public solicitation and the names cannot be shared until contract(s) are in place.

Q27. Can you provide a listing of questions that have already been asked and addressed by vendors?

A27. Yes. All vendor question are included in this document.

Vendor F

Q28. “Respondents must offer services in at least eight of our member states. For service to be considered offered in a state it must be offered in the whole state. (Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, Nebraska, North Dakota, Ohio, South Dakota, and Wisconsin)”

- By stating “Must offer services” are you requiring a physical presence in at least 8 member states, or the ability to deliver services into those states from one of our field locations?

A28. We are requiring the ability to deliver services.

Q29. Software Management - This is the ability to manage and support mobile applications, content and operating systems.

a. Ability to force mandatory application deployment.

- Public or Private Apps?

d. A way to push application updates to device.

- Public or Private Apps?

A29. Yes, Public and/or Private Apps. If limitations exist, please explain.

Q30. Network Service Management - This is the ability to gain information off of the device that captures location, usage, and cellular and WLAN network information.

a. Forced wireless network authentication.

- Do you mean make wireless authentication automatic? What do you mean when you say Force

d. Capability to send Alerts and Messages to administrators.

e. Capability to send Alerts and Messages to users

- Did you have a specific method in mind? (Text, Email, or App)
- Is this alert system to be built into the MDM solution and not use existing network

infrastructure?

A30. a) By “force” we mean select preferred SSID’s and authentication. d) Yes. e) Explain method of delivery (by any method). For alert system please explain method used.

Q31. Hardware Management - Beyond basic asset management, this includes provisioning and support.

- a. Ways to make sure mobile devices are running latest OS/patches.
 - Is this to say you want upgrades forced to the device or is blocking access good enough until the proper version is installed?
- b. Remote Control for administrative purposes (Remotely view device screen and perform user actions like mouse clicks or stylus taps).
 - Remote control is only available on Android device. Is this still a requirement?
- c. Backup and Restore of critical business data.
 - What data type of data is being backed up?
 - Is there a requirement as to where the data that is backed up is stored?
 - Does the back have to be automatic and immediate as the data changes?
 - Does the backup have to be wireless?
- d. Ability to separate personal and private data on mobile device so parts are more restrictive where institutional data would reside.
 - Does the institutional data need to be in a separate container?
 - Does the institutional data (i.e. email) need to be in a completely separate memory store from the native App?

A31. a) Both options, please explain and detail the operating systems it won’t work on. b) This is a desired requirement. c) Dependent on each individual institution’s backup requirements, please detail the backup features of the solution. d) This is a desired requirement.

Q32. Security Management - This is the enforcement of standard device security, authentication and encryption.

- b. A way to make sure device is storing data encrypted.
 - Does the encryption method need to be independent of the devices encryption services?
- e. A way to implement Administration support tiers.
 - Are you asking for role based administration access to the MDM portal?
- f. A way to keep sensitive data out of email and documents.
 - What is the origin of the sensitive data? Where is located? On the device?

A32. b) Data on the device needs to be encrypted either by device operating system or the MDM solution. e) Yes, the role based administration. f) It is unknown.