PROCUREMENT AND STRATEGIC SOURCING
University of Maryland, Baltimore County
1000 Hilltop Circle, Baltimore, MD 21250
procurement.umbc.edu // p: 410.455.2273

DATE: September 27, 2023

TO: All Prospective Bidders
Cc: Procurement File

FROM: Lori Lynch

RE: Security Assessment, RFI # BC-21341-L, ADDENDUM #1

The following amends the above referenced solicitation documents. Receipt of this addendum must be acknowledged by completing the enclosed "Acknowledgement of Receipt of Addenda" form and submitting it along with your response to the University.

The due date and time for the response to be submitted to the University is **FRIDAY, OCTOBER 6, 2023, 2023 by 11:59 p.m.** (EDT) to the issuing office.

A. The following questions were submitted for a response.

1. How many physical facilities/buildings would UMBC have within the scope of the physical assessment engagement?

   Response: UMBC has a total of 96 facilities to include main campus, BWTech North and South, and off-campus. 38 are used for administrative operations. 16 are for academic activities. 32 are for residential student use. 9 are for service-related activities.

   It is not anticipated that UMBC would have all facilities included in the physical assessment. A representative sample of building types may provide an adequate picture of UMBC's physical security needs. UMBC would like to understand the methods and elements of a physical security assessment prior to determining how many buildings to include in an actual assessment.

2. Is physical security centrally managed for all UMBC buildings and facilities?

   Response: Yes, UMBC has its own police force as well as building managers overseeing specific buildings.

3. Would the vendor be using UMBC channels to store and control the information gathered during the assessment?

   Response: UMBC is flexible in this regard, what options are available?

4. Are there any specific regulatory requirements we need to consider within scope (e.g., FERPA, HIPAA, etc.)?

Response: UMBC has to comply with all regulatory requirements to include FERPA, HIPAA, but it is not anticipated that access to any data of this nature would be required.

5. What level of assessment would UMBC prefer? Is this a design-level assessment or will we be doing effectiveness testing?

   Response: UMBC would like to understand the difference between different levels of effort associated with a security assessment. If examples of different levels of effort (or different assessments) could be explained along with any pros and cons for these different assessments, it would aid UMBC in determining to what extent we desire our assessment to be.

6. How many business units will be in scope for this assessment?

   Response: UMBC is undecided as to the full scope of assessment we desire. Answers to the process and elements of various assessment that companies provide and the means in which these assessments are conducted will aid UMBC in making decisions of this nature.

7. What type of environment are we reviewing? Are systems on prem, at a data center, or cloud based?

   Response: If this question refers to data security, then all would apply. UMBC has not determined how much effort it desires for any data security assessment and answers regarding the levels of data security assessment will aid UMBC in this process.

8. Do you have any third-party vendors performing security actions on your behalf?

   Response: Yes, but very limited in scope and capacity.

9. What University personnel are currently responsible for implementing and enforcing its information security program?

   Response: Generally, our Department of Information Technology performs this function.

10. Has the University performed any previous security assessments in the prior 3 years?

    Response: No

11. What is the total number of servers (physical and virtual) that are part of the IT infrastructure at the University?

    Response: UMBC declines to answer this question as it is currently unsure of what level of assessment would be desired.

12. What is the total number of telecom closets at the University?

    Response: UMBC declines to answer this question as it is currently unsure of what level of assessment would be desired.

13. Is UMBC looking for a cybersecurity-focused risk assessment? Or does UMBC also want to include other scenarios that are a threat to security, such as active shooter, natural disaster, etc.?

    Response: UMBC is unsure of just what security elements are to be included in a security assessment. The purpose of this RFI is for UMBC to learn more about the elements involved with both physical and electronic/data security assessments and to make more informed decisions about the scope of such an assessment.

14. Does UMBC have a timeframe that this security assessment would need to be initiated and/or completed?

    Response: UMBC's timeframe is not firm, but we intend to start building a scope of work following this RFI process.

15. Does UMBC have a budget for the security assessment and if so, what is that budget?

    Response: No budget has been set as UMBC needs to understand the elements of an assessment as well as the timeframe to complete such assessments in order to determine to the extent of assessment that we desire.

16. Is the data security component of this assessment only as it pertains to electronic security systems (access control and camera systems) or data security related to all UMBC IT infrastructure, systems, and networks?

    Response: UMBC is unsure of how much data security we will assess versus how much electronic security we will assess. UMBC needs to better understand the levels of assessment that typically are performed in each area better prior to making this decision.

17. In evaluating the Physical and Data Security posture, is UMBC looking for a collaborative security audit, a penetration test, or both? A penetration test is a covert, tactical assessment designed to evaluate the effectiveness of current controls in place by emulating actual risks the university may face, such as an attacker bypassing a door control and gaining access to a data center. In contrast, in a security audit, the auditor would be escorted at all times, and evaluate the security of each building in scope.

    Response: If pros and cons of these assessments could be provided, that would aid UMBC in determining to what level the campus is assessed. UMBC is being cautious in not assuming what we need and are relying on industry experts like yourselves to outline the various assessments and the pros and cons of each so that we can make an informed decision

regarding the breadth and depth of an assessment.

18. Since Data Security and Electronic Security are identified under the same set of questions, please confirm whether or not UMBC is looking for physical onsite security around data and infrastructure, or if the physical security is onsite while the data security assessment is through remote system testing and controls?

    Response: Data and electronic security are identified under the same set of question because we desire to understand the difference between the two from the perspective of companies that perform these assessments. Understanding these differences and what the assessments for each entail will aid in our decision making. UMBC understands that some assessments may require a physical presence and others may not, but we would like to understand how companies that perform these assessments typically conduct them.

END OF ADDENDUM #1, DATED 09/27/23
(Original with enclosures were not mailed)

BID NO.: BC-21341-L

TECHNICAL BID DUE DATE: FRIDAY, OCTOBER 6, 2023, 2023 by 11:59 p.m. EDT

BID FOR: Security Assessment

NAME OF BIDDER: _____

ACKNOWLEDGEMENT OF RECEIPT OF ADDENDA

The undersigned, hereby acknowledges the receipt of the following addenda:

Addendum No. 1	dated 9/27/23
Addendum No. ___	dated _____
Addendum No. ____	dated _____
Addendum No. ____	dated _____
Addendum No. ____	dated _____

As stated in this Addendum, this form is to be returned with your response.

_____
Signature

_____
Printed Name

_____
Title

_____
Date

END OF FORM