OHIO TURNPIKE AND
INFRASTRUCTURE COMMISSION

ADDENDUM NO. 1
ISSUED MAY 16, 2024

to

RFP NO. 11-2024
FOR PAYMENT CARD INDUSTRY QUALIFIED SECURITY ASSESSOR SERVICES

PROPOSAL DUE DATE: 5:00 P.M. (EASTERN TIME), MAY 22, 2024

ATTENTION OF RESPONDENTS IS DIRECTED TO:

ANSWERS TO QUESTIONS RECEIVED THROUGH 12:00 PM ON MAY 15, 2024

Issued by the Ohio Turnpike and Infrastructure Commission through Aimee W. Lane, Esq, Director of Contracts Administration.

Aimee W. Lane

______________________________ May 16, 2024
Aimee W. Lane, Esq., Date
Director of Contracts Administration

ANSWERS TO QUESTIONS RECEIVED THROUGH 12:00 P.M. ON MAY 15, 2024:

Q#1 Can a copy of the 2023 ROC (not just AOC) be shared for QSA companies that are proposing on this project?

A#1 No, the Ohio Turnpike and Infrastructure Commission (hereinafter "OTIC") will share the 2023 ROC with the selected vendor upon execution of a contract.

Q#2 Is the ATPM a TPSP or in-house?

- **If in-house, do you develop the software or is it COTS.**

A#2 ATPMs are TPSP.

Q#3 Is the P2PE technology part of a validation solution listed on the PCI website?

- **If so, what is the name of the validate solution.**

A#3 The CDE is outsourced to multiple PCI-DSS certified third-party service providers.

Q#4 Who manages the OTIC E-ZPass website particularly the payment page?

- **Is there a TPSP involved, and if so, who?**
- **Is the IVR third-party or managed in-house?**
- **Is the service rep accessing the website or a software?**
- **What is the set-up for the E-ZPass back-office system (e.g., is it isolated)?**

A#4 The E-ZPass environment is fully separate from the corporate OTIC environment. E-ZPass, Swipe and IVR transactions processing environment is managed by a third party. The special permit portal is hosted at OTIC datacenter, but it uses an iFrame solution hosted and managed by a third party.

Q#5 What is the name of the website?

- **Who manages it?**
- **What is the payment process involved with this site?**

A#5 EZPassOH.com, which is managed by a third party (please see the response to Q#4).

Q#6 Do you have AOC's for the TPSP and other key players where applicable?

- **When do you expect to have this fully completed?**

A#6 Yes, AOC's are received for the TPSPs and other key players where applicable. The project completion date is November 2024.

Q#7 How many processors are involved and who are they?

A#7 Three payment processors, whereby the relationship between two of the three payment processors is managed by third parties. Details of payment processors will be shared with the selected vendor upon execution of a contract.

Q#8 Is segmentation in use and if so, was it tested during your latest penetration testing?

A#8 Yes, the environments in scope for the PCI project are segmented from the OTIC corporate network, and third-party service providers are responsible for penetration testing.

Q#9 Have you maintained 4 passing external scans/rescans during the "modernization" project(s)?

A#9 External scan data will be provided to the selected vendor on execution of the contract.

Q#10 Although it was stated that no credit card data stored electronically, has this been tested/scanned for?

A#10 No credit card data is stored electronically.

Q#11 Is there any credit card information stored in hard copy form?

A#11 No credit card data is stored in hard copy form.

Q#12 How many locations will be part of the assessment and what are their geographical locations?

A#12 Approximately 25 locations across Northern Ohio.

Q#13 If our legal team has a need to redline any of the agreements (e.g., the non-collusion affidavit) before we execute them, is this acceptable?

A#13 A respondent may provide a redline of the form contract (Appendix B) which will be considered by OTIC, but OTIC makes no representations or guarantees that it will approve any suggested revisions. However, OTIC will not accept any revisions to its standard non-collusion affidavit.

Q#14 Is OTIC considering only a designated "QSA Company" according to the PCI Security Standards Council? Or can we directly employ a QSA to meet the requirements of this RFP?

A#14 OTIC is seeking a certified QSA provider.

Q#15 What are the requirements for In-field physical site security assessments of OTIC locations? Will Ohio Turnpike reimburse the charges?

A#15 See section 2.4 of the RFP regarding reimbursable expenses.

Q#16 Are all in scope systems centrally managed under the same information technology department, policies and procedures?

A#16 OTIC's technology department is centrally managed at the Berea main campus (please see the response to Q#4).

Q#17 Is entity fully reliant on third-party service providers for managing any aspects of PCI compliance? (i.e. fully hosted web-site, managed service provider managing hardware, security impacting services, etc). If so, can you please provide detail about which aspects are managed by a third-party?

A#17 Please see the response to Q#4.

Q#18 Appendix A mentions the transition from gated toll to open road – would BOTH systems be in use at the anticipated time of the assessment?

A#18 OTIC fully transitioned to the new tolling system on April 10, 2024.

Q#19 Are systems that impact Cardholder Data Environment (CDE) segmented on the network? (i.e. do you have a separate CDE/VLAN/segment or is your network flat?)

- **If so, how many PCI specific segments exist?**
- **If so, how is that segmentation being achieved?**

A#19 Please see the response to Q#4.

Q#20 How many in-scope applications being utilized to store or transmit payment card information?

- **Are they developed in-house or do you have source code to modify the application?**
- **If third party software, are they PCI SSF/P2PE compliant (please specify)?**

- **Of these applications how many are web applications (please specify the number of externally facing, number of internal facing, and/or both internal and external use please)**

A#20 *In-scope applications are all managed by third-party service providers. One uses a desktop application; the others are web-based applications (Please see the response to Q#10).*

Q#21 Please provide the number and description of system components in scope for PCI (please include all servers, databases, POS/POIs).

A#21 *This information will be shared with the selected vendor upon execution of a contract.*

Q#22 How many physical locations do you process, store or transmit cardholder data? This should include duplicate operational infrastructure, backup, fail-over or redundant sites housed in a second physical location (i.e. another city), and/or additional operational sites in different geographic regions.

A#22 *Approximately 25 locations across Northern Ohio.*

Q#23 Do you utilize any wireless in your CDE? Are any of these wireless networks transmitting cardholder data?

A#23 *No wireless network transmitting of cardholder data is utilized.*

Q#24 Are calls recorded on the IVR system? If so, does the call recording contain the spoken 16-digit PAN, or tones equating to the 16-digit PAN?

A#24 *Cardholder data is not recorded and is input by the customer.*

Q#25 For the 2 eCommerce solutions, which method is the payment information captured and transmitted: Direct POST/Web Form, JavaScript, iFrame, full redirect to a third party, or other?

A#25 *Please see the response to Q#4.*

Q#26 Does management have any customized controls vs the standard approach? If so, how many?

A#26 *This information will be shared with the selected vendor upon execution of a contract.*

Q#27 Does management have any compensating controls? If so, how many?

A#27 This information will be shared with the selected vendor upon execution of a contract.

Q#28 With respect to how OTIC receives credit card payments, it is stated that payments are received at time of travel through interaction with a human toll collector. Is the toll collector processing the payment as a card payment transaction?

A#28 Credit card payments received at time of travel can be processed as a card payment transaction either with a collector or ATPM.

Q#29 Are transactions processed by toll collectors done so via the P2PE solution mentioned in Appendix A?

A#29 Yes.

Q#30 Is the P2PE Encryption solution used at toll locations a Validated solution listed on the PCI Council's list of valid solutions? If not, has the solution undergone a NESA (Non-Listed Solution Assessment)?

A#30 Please see the response to Q#3.

Q#31 If the P2PE solution is a NESA solution, has the OTIC's acquirer agreed to accept it as a valid solution for scope reduction?

A#31 Please see the response to Q#3.

Q#32 Regarding payments for over-dimensional and overweight vehicles, is the website the only means of processing those payments? If so, is the website hosted by the OTIC or is it hosted by a third party?

A#32 Yes, please see the responses to Q#4 and Q#5.

Q#33 Does the website use any type of redirection to a third-party payment page?

A#33 Please see the response to Q#4.

Q#34 Does this payment channel also employ tokenization?

A#34 Please see the response to Q#4.

Q#35 Regarding payment taken by Customer Service Representatives, what application or payment channel do they use to process payments?

A#35 Please see the response to Q#4.

Q#36 Does the application used to process payments employ tokenization, or any type of redirection to a third-party payment page?

A#36 Please see the response to Q#4.

Q#37 Is the Customer Service function outsourced to a third-party?

A#37 The Customer Service function is in-house, the back-office (including IVR) is managed by a third-party (Please see the response to Q#4).

Q#38 Regarding payments taken via IVR, is the IVR hosted by OTIC or outsourced to a third party?

A#38 Please see the response to Q#4.

Q#39 Do the customer service representatives have the option of transferring a customer to the IVR for payment?

A#39 Please see the response to Q#4.

Q#40 Do customers have the option of requesting to speak to a customer service representative if they initiate the call via the IVR?

A#40 Yes.

Q#41 Regarding the E-ZPass website, is this hosted by the OTIC or outsourced to a third party?

A#41 Please see the response to Q#5.

Q#42 Does the website utilize tokenization or any redirection to a third-party payment page?

A#42 Please see the response to Q#4.

Q#43 Approximately how many credit card processors, system integrators, and other TPSP (Third Party Service Providers) are expected to be in scope for 2024?

A#43 Please see the response to Q#7.

Q#44 Will they be able to provide proof that the services they are providing are PCI Compliant by supplying an Attestation of Compliance (AoC) and corresponding responsibility matrix?

A#44 Please see the response to Q#6.

Q#45 Has the OTIC undergone a version 3.21. to version 4.0 Gap Analysis? If so, are there any significant issues requiring remediation prior to beginning the PCI Validation?

A#45 Version 4.0 Gap Analysis was completed in 2023.

Q#46 Does the OTIC anticipate utilizing a customized approach to address any of the 4.0 requirements?

A#46 OTIC is not anticipating a customized approach to address any of the 4.0 requirements at this time.

Q#47 How many locations will be in scope for this assessment?

A#47 Please see the response to Q#12 and Q#22.

Q#48 What type of facilities, i.e., Data Center, Call Center, Corporate officers, etc.?

A#48 Please see the response to Q#4, Q#12 and Q#22.

Q#49 Is the OTIC interested in obtaining information on other related services such as Penetration testing, external vulnerability scans, etc.?

A#49 Not as part of this Request for Proposal.

Q#50 How many policies and procedures are in place?

A#50 This information will be shared with the selected vendor upon execution of a contract.

Q#51 How many IT staff does the Commission have?

A#51 There are 20 full-time staff in our technology department.

Q#52 We do not share audited financial statements due to confidentiality reasons. In lieu of that, can we share our DUNS and/or GSA contract numbers?

A#52 Please mark the audited financial statement as confidential and, if you prefer, submit it to OTIC under password protection.

END OF ADDENDUM NO. 1