OHIO TURNPIKE AND INFRASTRUCTURE COMMISSION

ADDENDUM NO. 2
ISSUED MAY 20, 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 5:00 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

Aimee W. Lane, Esq.,
Director of Contracts Administration

May 20, 2024
Date

ANSWERS TO QUESTIONS RECEIVED THROUGH 5:00 P.M. ON MAY 15, 2024:

Q#53 With less than one week between the inquiry deadline and proposal due date, we request a 2-week extension from the date answers to questions are released.

A#53 The Commission will not extend the proposal due date because of time constraints for contract approval and execution and commencement of the work.

Q#54 Does a Respondent's good faith effort require all of these items in section E, subsections a through d be fulfilled?

A#54 Respondents must provide a response to subsections (a) through (d) under Section E. However, subsection (d) is intended to provide a way for non-Ohio based respondents to explain how, if selected for the contract at issue, they will be able to commit to a significant economic presence in Ohio through the actions listed in that subsection, as well as other non-listed actions.

Q#55 Would the commission consider reviewing a vendor provided agreement and negotiating final terms upon award or down selection?

A#55 No. The Commission includes a form contract in all RFPs to provide a level playing field and to set expectations for the resulting contract terms.

Q#56 What is the current PCI Compliance deadline for OTIC?

A#56 November 2024

Q#57 What is the date of the last PCI scoping exercise by OTIC?

A#57 November 2023

Q#58 Have Targeted Risk Analysis (TRA) documents been created for each PCI requirement defining periodicity?

A#58 No.

Q#59 What is the date of the last external / internal penetration test?

A#59 Penetration Testing was last completed in April 2024.

Q#60 What is the approximate number of in scope devices by type (Servers, Workstations, Point of Sale, Credit Card machines, etc.)?

A#60 Please see the response to Q#21.

Q#61 What is the approximate number of in scope facilities (offices, data centers, toll booths, etc.)?

A#61 Please see the response to Q#22.

Q#62 What is the number of in-scope payment applications? Are there any in-house developed payment applications by OTIC?

A#62 Please see the response to Q#20.

Q#63 Does Ohio Turnpike store credit card data of any kind (even if encrypted or tokenized)?

A#63 Please see the response to Q#10.

Q#64 Is wireless in scope for PCI?

A#64 Please see the response to Q#23.

Q#65 Are network and data flow diagrams current?

A#65 Yes, network and data flow diagrams are current.

Q#66 When was the last RISK assessment?

A#66 October 2023.

Q#67 Are E2EE or P2PE solutions used for scope reduction?

A#67 Please see the response to Q#3.

Q#68 When was the Incident Response Plan previously used or tested?

A#68 The Incident Response Plan is reviewed annually with TPSPs as part of our PCI attestation of compliance.

Q#69 Is there a requirement for the assessment or any scope of this contract to be performed on-site?

A#69 No specific requirement; left to the discretion of the QSA service provider.

Q#70 What PCI related training is required? Examples:

- **Trainer based PCI training or security awareness training**
- **Computer based training for PCI or security awareness**
- **Vendor developed training materials (presentations or videos) for PCI or security awareness**

A#70 PCI training is required annually for all staff who interact with systems in-scope for PCI attestation.

Q#71 Are the requested services within II Scope of Services within the RFP, required to be completed prior to the annual PCI assessment or as part of the on-going compliance management program?

A#71 Not all items listed in the Scope of Services are a requirement for the annual PCI assessment.

Q#72 Are resumes and certifications required of Vendor PCI QSAs as part of the RFP or upon beginning any PCI services after the contract is finalized?

A#72 Evidence of QSA certification is required.

Q#73 Will the Commission allow for additional terms to be included, as articles in the Contract or attachments/exhibits to the Contract?

A#73 After evaluating and scoring the proposals, the Commission may attempt to negotiate a contract with the top ranked respondent and if those negotiations are unsuccessful, may attempt to negotiate a contract with the next ranked respondent, and so on. If a respondent requests additional terms, attachments or exhibits, those items may be part of the contract negotiations, but the Commission makes no representations or promises that it will agree to such requests for additional terms, attachments or exhibits.

Q#74 Are payment terms of 30 days from invoice receipt, cited from a state statute or law? Also, can a specific resource title be used on the invoice instead of individual names?

A#74 Payment terms of 30 days from invoice receipt is not derived from statue or law, but is a non-negotiable standard Commission contract term. The Commission is amenable to discussing required information for invoicing with the selected respondent at the time of contract award.

Q#75 What is the total number of systems in scope for the assessment, based on system type?

A#75 Please see the response to Q#4.

Q#76 What is the total number of PCI related vendors (legacy and new) within the revised scope for PCI compliance?

- **Are all vendors compliant with PCI standards and have a current AoC available**?

A#76 Please see the response to Q#7.

Q#77 Approximately, how many physical locations each are in scope and could be visited for evaluation as a part of the Report on Compliance assessment?

- **Is sampling of sites acceptable, or is the expectation to visit all sites?**
- **Are physical locations configured in the same way? If not, how many different configurations are there?**

A#77 Please see the response to Q#12.

Q#78 Within section II Scope of services, one of the bullets discusses "Design and/or delivery of supplemental PCI DSS training materials such as videos, presentations, learning portal content, or written documentation.

- **How many individuals require supplemental training?**
- **Is there a defined frequency to conduct training?**
- **Will this training include focused training based on role (E.g., executives, developers, administrators) or general PCI awareness training for all users?**

A#78 Please see the responses to Q#70 and Q#89.

Q#79 Within section II scope of services, one of the bullets discusses "Assistance with preparation of Responsibility Matrices among OTIC and various toll system integrators".

- **Is there currently one in place for each vendor?**
- **Approximately how many vendors need to have a responsibility matrix completed?**

A#79 Please see response to Q#7; Responsibility Matrices have been completed and will be provided to the selected vendor upon execution of a contract.

Q#80 Within section II scope of services, one of the bullets discusses "Documentation of steps needed to remediate any gaps in compliance", is there a defined format/template desired?

A#80 No.

Q#81 Within section II scope of services, one of the bullets discusses "Create reusable structures to streamline future certification effort". Can you please provide clarification on types of structures expected?

A#81 The current process may be efficient as designed; however, any notable enhancements discovered during the engagement should be discussed or formalized for future use.

Q#82 We have numerous private sector clients who would serve as a reference but have limited government and public sector references, are government and public a requirement?

A#82 No, please see the response to Q#14.

Q#83 We are not currently registered with the state of Ohio but can be before work commences, is this a requirement?

A#83 The selected respondent must be registered with the State of Ohio Secretary of State prior to contract execution. Please confer with your legal counsel or other representative of choice if you have questions about this requirement.

Q#84 If we can only provide unaudited financial statements will this be sufficient?

A#84 Each respondent should submit an audited financial statement. In lieu of an audited financial statement, the Commission will accept financial statements signed by the respondent's chief financial officer with a statement that it is a true and accurate statement of respondent's financial condition.

Q#85 What is the total number of toll plaza locations?

- **What is the total number of P2PE devices at toll plazas?**
- **What is typical number of P2PE devices in use at each tool plaza location?**
- **What P2PE devices/solutions are in use?**

- **Are all toll plaza locations using the same P2PE device/solution? If not, please include number of each P2PE device type used and how many toll plazas use each type.**

A#85 Please see the response to Q#12.

Q#86 How many of the following system components are in scope for PCI? Please include Make/Model and/or operating system.

- **Firewalls**
- **Routers**
- **Layer-3 Switches used to VLAN any in-scope networks**
- **Load Balancers**
- **IDS**
- **Hypervisors**
- **Web Servers**
- **Application Servers**
- **Database Servers**
- **SFTP Servers**
- **Email Server**
- **Domain Controller**
- **VPN Server**
- **MFA Server**
- **Mainframes**
- **Workstations**
- **Other (please specify)**

A#86 This information will be shared with the selected vendor upon execution of a contract.

Q#87 Is network segmentation used to isolate the in scope cardholder data environment (CDE) network(s) from other out-of-scope networks?

A#87 Please see the response to Q#8.

Q#88 Are there any "Connecting To" or "Shared Services" systems that are outside of the CDE network(s) that connect to the CDE or could impact the security of the CDE? If so, please list how many systems along with functions and operating system types.

A#88 Please see the responses to Q#4 and Q#7.

Q#89 How many people are in scope for PCI?

- **Administrative personnel**
- **General users (e.g. customer service representatives, etc.)**

A#89 Approximately 300 toll collectors located across Northern Ohio are in scope. Customer service representatives do not receive credit card information but still receive annual PCI training.

Q#90 What is the total number of third-party service providers estimated to be in scope?

A#90 Please see the response to Q#7.

Q#91 From Appendix A.II – Scope of Services; Bullet 11: Design and/or delivery of supplemental PCI DSS training Materials such as videos, presentations, learning portal content, or written documentation. What specific training they are looking for and how often? Is it just general PCI DSS knowledge training and will one presentation do that can be accessed by employees?

A#91 The Commission seeks assistance in the preparation of general training materials for ongoing PCI compliance.

Q#92 For the payments received via OTIC E-ZPass website – who (which entity) is hosting and managing that particular website? (if third party – please specify the third party)

A#92 Please see the response to Q#5.

Q#93 For the payments received via the IVR telephone system – is the solution an in-house solution or is it a 3rd party solution (if third party – please specify the third party)

A#93 Please see the response to Q#4.

Q#94 How many toll plaza locations are there in scope?

A#94 Please see the response to Q#12.

Q#95 Where is the OTIC infrastructure hosted (on premise; cloud service provider; colocation)? Please list all that apply.

A#95 Please see the response to Q#4.

Q#96 Approximately how many servers and/or virtual machines are there in the PCI CDE?

A#96 Please see the response to Q#4. TPSPs manage most aspects of the CDE, the details of which will be shared with the selected vendor upon execution of a contract.

Q#97 Please confirm that the expected deliverables are one (1) PCI DSS v4.0 Level 1 Attestation of Compliance (AoC) and the associated Report on Compliance (RoC). If this is not correct, please list the expected deliverables.

A#97 Correct, performed annually. The deliverables associated with other items listed in Section II of the RFP are subject to mutual agreement.

END OF ADDENDUM NO. 2