Rhode Island Turnpike and Bridge Foundation

Jamestown, Rhode Island

ADDENDUM No. 1

Questions relating to Contract 18-14

Project: Contract 18-14: PCI, PII, HIPAA Compliance

Date: January 15, 2019

1. When was the last time the Authority performed a PCI DSS Assessment and what SAQ(s) or ROC was/were used to report compliance?
   12/28/2016 PCI SAQ D 3.2

   Roughly how many devices at each location? 12

2. And, will the reports be made available at the onset of the engagement?
   Yes

3. How many payment card transactions do you process a year? What Level Merchant is the Authority?
   Approximately 775,000

4. How many and what type of facilities are in scope?
   1. Customer Service Center
   2. Lanes

5. Where and how are card not present transactions processed?
   1. Call Center – in the Account Management Programs – Toll CRM and Toll Invoice
   2. Walk In Center –
   3. Back Rooms – Toll CRM and Toll Invoice

6. Where and how are card present transactions processed?
   1. Lanes – Have both swipe and insert
   2. Walk In Center - Cards are manually entered into the Account Management Programs
   3. Website

7. Are the POS applications currently in use commercially available or developed in house? If commercially available are the PA-DSS certified?
   Emovis does not have POS onsite, only a cash draw application

8. How many e-commerce application(s) need to be assessed?
   There are 3:
   1. TOLLCRM
   2. Image Review (no CDE data)
   3. Transactional Website

9. Where are the in scope systems and applications of the cardholder data housed?
   On-site

10. What database technology is currently deployed within the environment, i.e. Oracle, SQL, etc.? And approximately how many are deployed in the credit card environment?
    SQL Emovis utilizes SQL 2016 for the DB and there is 1 database within the CDE

11. What middleware, (i.e. WebSphere, Apache, IIS) is currently deployed within the CDE?
    IIS 2016 web farm

12. Does any of the CDE definition and scoping documentation currently exist or is it expected that they will be developed as a part of the engagement?
    Be developed as part of the engagement.

13. Can you provide a detailed listing of the in scope cardholder data environment including applications, workstations, POS terminals, servers, operating systems, firewalls, routers and cloud services?
    Yes, to the company that is awarded the RFP.

14. How many externally facing active IP addresses does the Authority have that require ASV scans?
    2

15. Is the network segmented to reduce scope?
    Yes

16. Are wireless networks in the CDE at this time?
    Separate form the CDE

17. Do you outsource any portion of your IT environment? If so please list which IT functions?
    The design and installation of Network and Blade systems. Also Website development.

18. Do you currently employ any managed services (i.e., managed firewalls, IDS, etc.)? If so can you please list how many and the services provided?
    No

19. Have you outsourced your collections or 'toll runners' to third party vendors?
    No

20. Can the Authority confirm that no major changes to the environment are anticipated that would impact the level of effort to complete re-validation of the CDE?
    No, there will be ongoing updates to the system during this process.

21. Is there an incumbent vendor? And can you share who it is?

    Yes. Mega Planet has done past PCI scans.

22. Are you self- insured? No

23. Is the QSA requirement is firm, since you don't actually need a QSA audit?
    Yes

24. Do you currently have documented privacy, security or cybersecurity policies and procedures?
    No

25. The title of the RFP included HIPAA compliance, what locations are in scope and what format is the protected health information (PHI) in? Paper format, electronic format, or both?
    Paper one location

    -If electronic, what electronic medical record if RIBTA using?

26. Have you ever gone through a HIPAA risk assessment in the past? If so, when?
    No.