Rhode Island Turnpike and Bridge Authority
P.O. Box 437 | Jamestown, Rhode Island 02835-0437

March 28, 2025

ADDENDUM NO. 01
Request for Proposals 25-01

Comprehensive Assessment of PCI 4.0.1 DSS Requirements

Prospective Proposers and all concerned are hereby notified of the following changes/comments related to the Request for Proposals (RFP) document 25-01. These changes/comments shall be incorporated in and shall become an integral part of the RFP.

Below are questions posed by Prospective Proposers along with RITBA's response:

1. Is MBE participation required in order to be considered for selection/aware of this contract for PCI assessment and penetration testing? No.
2. There appears to be a conflict with proposal due date and project start date
   a. On page 2 the RFP indicates:
      The proposal must be received no later than 2:00pm EDT April 15, 2025, EDT
   b. However, on page 5 - #6 Timelines and Milestones indicates:
      Assessment Start Date April 9, 2025 – The start date is before Proposal Due Date
   c. Can RITBA please clarify/provide an update? Assessment Start Date is May 15, 2025.
3. Please list all locations that are involved with storage, processing, or transmission of Card Holder Data (CHD), as well as locations that connect to or can impact the security of the referenced locations. Two Locations, Primary and Disaster Recover locations. Details will be provided to the awarded firm
4. Is IT service delivery organization centralized or de-centralized? Centralized
5. How many FTEs in the IT service delivery organization? Details will be provided to the awarded firm.
6. Does RITBA have any in-house ISA certified individuals? N/A
7. Does RITBA perform any in-house software development? No.
8. How many external IP addresses are in scope for penetration testing? 4 External Address
9. Is the organizations email on in-house systems, hosted (eg. MS365, Google, etc.) or hybrid? Please describe. Email will be outside the scope of this engagement
10. Please describe any internet facing/accessible applications that are in scope for the penetration testing. One website, details provided to the awarded firm
    a. Please include if any of referenced applications store, process or transmit Card Holder Data (CHD). No

b. Please describe if the referenced applications are Commercial Off the Shelf (COTS) or custom developed. Details provided to awarded firm
c. Please describe the following for each referenced application:
    i. Estimated number of static pages?
    ii. Estimated number of dynamic pages?
    iii. Estimated number of AJAX routes/API endpoints? Details provided to the awarded firm.
d. Please indicate if the referenced application is also considered part of your Cardholder Data Environment (CDE) – either within CDE, or CDE security impacting. N/A

11. Please describe any cloud/vendor hosted applications that need to be in scope for the external network penetration testing. No
    a. Please indicate if these are also considered part of your Cardholder Data Environment (CDE) – either within CDE, or CDE security impacting. N/A
12. Please describe the number of and size of internal LAN/WAN IP address segments?
    a. For example: twelve /24 network segments. Details provided to the awarded firm
13. How many servers? Details provided to the awarded firm
    a. Windows?
    b. Linux?
    c. Others?
14. How many employee end points (desktops, laptops, tablets, etc)? Details provided to the awarded firm
15. How many other/peripherals (routers, switches, multi-function devices, VoIP devices, others…)? Details provided to the awarded firm
16. How may Windows Active Directory Domains? Details provided to the awarded firm
17. Do you have an isolated CDE? Yes
    a. If yes, please describe the approximate number of hardware and software systems withing the CDE. Details provided to the awarded firm
18. How many merchant accounts are in use? One
19. How many card transactions does RITBA process each year? Details provided to the awarded firm
20. Please list the different acquirers that need to receive compliance reporting. One
21. Please indicate how many non-acquirers also require compliance reports. N/A
22. Has RITBA completed fully compliant reports each of the last two years? Yes
23. What reporting format does RITBA follow?
    a. ROC, SAQ-D, other SAQ? SAQ
24. Please describe each payment channel. Details provided to the awarded firm
25. Please describe each payment application in use. Details provided to the awarded firm
    a. Please indicate if the referenced application is COTS or custom developed. Combination of both
26. Please describe the make, model, and version of any payment hardware/card reading devices in use. Details provided to the awarded firm

a. Please indicate if card readers are “Approved PTS Devices.” Yes

27. If there are Compensating Controls being relied on, please indicate which defined control(s) is being replaced by a Compensating Control. N/A
28. If a Customized Approach is being relied on, please indicate which defined control(s) is being replaced by a Customized Approach. N/A
29. Is RITBA requesting the proposal include quote for services for quarterly ASV scanning? No
30. Please describe how/to what degree RITBA outsources responsibility for any in-scope PCI controls or processes. Details provided to the awarded firm
31. Please provide further detail on the July 1, 2025 due date for the final report. Is that for the completed SAQ and AOC, or for the gap analysis report? SAQ and AOC
32. Is RITBA currently PCI-compliant? Yes.
33. Would this be your first engagement with an external QSA firm? No.
34. Would you like us to include detail on assistance with remediation of items identified in the gap analysis report? No
35. Please detail the types of payment processes accepted (online, mail, in-person, phone) Online, Phone and In-Person
36. Are any payment processes fully outsourced? No
37. How many payment processors are engaged? Will be provided to the awarded firm
38. What is the driver for this compliance effort? Has a processor requested an AOC? Continued PCI compliance certification
39. Does RITBA store any payment card information? No
40. How many credit card transactions are accepted per year? Will be provided to awarded firm
41. Is the network infrastructure cloud-based, on-premises, or a hybrid environment? On-Prem
42. Who manages and owns the infrastructure? RITBA
43. How are payments accepted through https://www.ezpassritba.com/? (full URL redirect, inline frame, or through APIs?) To be provided to the awarded firm
44. Can you confirm the anticipated project start date? The solicitation document has April 9th listed as the start, but the RFP is due on April 15th. Please clarify. Please see response to question 2.c.
45. In the solicitation document there is mention of “RITBA requires respondents keep the proposals to a maximum of eight (8) double sided 8 ½ x 11 pages (no less than 12 font) for each discipline a firm is requesting to provided services for RITBA”, however there is no further mention of the disciplines referenced in the rest of the solicitation document. Please clarify if there are disciplines, we should be aware of. There are no other disciplines. Please disregard.
46. Is the M/WBE participation of a total of 15% a goal or requirement? This is required under state laws, however it is recognized that firms, especially those that self-perform, may not meet the 15%. Firms will not be “penalized” for not meeting the 15%.

47. Does the M/WBE need to be registered with the State of Rhode Island or does another state suffice? If they do, can the firm start the registration process during submission/award since it says the process can take up to 90 days? All M/WBE's must be state certified on the date of your submission.
48. Looking at the M/WBE firms, are any of those firms qualified to do the requested work? If yes, who? N/A
49. How old can the project references be? This is up to the proposer.
50. How many years have you submitted an SAQ? If so what type (i.e. SAQ-D etc.) To be provided to the awarded firm
51. How is account data (i.e. PAN, CVV) captured? Is it captured online? In person? To be provided to the awarded firm
52. Is wireless technology used to process or transmit PCI data? No
53. Has segmentation been utilized to isolate systems that store account data? Yes
54. If so, what segmentation methods have been used to isolate systems that store account data (i.e. DLP, Access Control Lists, etc.) To be provided to the awarded firm
55. How many applications that store process and/or transmit PCI data are in scope? To be provided to the awarded firm
56. How many network devices (load balancers, routers, switches and type? To be provided to the awarded firm
57. How many firewalls and type of firewalls? To be provided to the awarded firm
58. How many servers are in scope and what operating systems are they? To be provided to the awarded firm
59. Where are the data centers? Addresses provided to the awarded firm.
60. Are call centers used to collect credit card payments from customers? If so, are they managed in-house or by a third party? Will be provided to the awarded firm
61. Where are the main IT locations for security, development, administration, and operations? Jamestown RI
62. How many PCI- POS systems are in scope for the assessment? Will be provided to the awarded firm
63. Please clarify your needs with ASV scans. Do you want the QSA firm to review ASV scans or conduct ASV scans? ASV scans are done monthly via another vendor.
64. Have compensating controls been utilized to help meet PCI requirements? Answered previously line 27
65. How many PCI third-party service providers (TPSPs) are in scope for the assessment? Will be provided to the awarded firm
66. How many IP addresses and ranges are in scope and roughly how many live? Answered previously line 27.
67. Is the management of any part of the environment outsourced? Will be provided to the awarded firm
68. Is there an active response mechanism (e.g., intrusion detection system or IPS, web application firewall or WAF, or connection limits) in place? Yes, to all
69. Is the management of any part of the environment outsourced? No.

70. How many network addresses (e.g., 10 class C networks, 255 addresses, etc.) will be in-scope of the internal test? To be provided to the awarded firm
71. How many separate internal network segments (e.g., PCI CDEs) will be tested? Will be reviewed and identified with awarded firm
72. How many users are there in your network environment? Will be provided to the awarded firm
73. Please confirm the assessment start date. In RFP page 5 bullet 6, sub bullet assessment start date is April 9, 2025, which is before RFP response is due. Please see response to question 2(c).
74. RITBA expects the successful firm to execute this Agreement with no changes to the Agreement. Does this mean selected vendor cannot add terms or request updates to terms? Correct
75. Please clarify the duration, on page 6 states assessment report is due July 1, 2025, but contract terms will be for 5 years. This is for annual assessments (over 5 years, each due by July 1st).