भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

PRE BID REPLIES FOR NPCI:RFP:2013-14/0014 dated 28.08.2013-RFP for Appointment of Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) for Payment Card Industry - Data Security Standard (PCI DSS) Re-Certification

Sr. No#		Page No.	Clause No.	Description in RFP	Clarification Sought	Additional Remark (if any)	NPCI Replies
1	Section-4	14	4.2.4	The bidder should have conducted PCI DSS certification with compliant ROC (Report on Compliance) for at least 5 organizations with at least 3 financial institutions during last 3 years.	We have recently qualified as QSA for PCI - DSS hence we have few on-going projects for PCI DSS certification. We have successfully completed PCI-DSS compliance implementation projects for numerous financial institutions.	Any relaxation would be appreciated	No change in RFP
2	Section-4	14	4.2.5	The bidder should be registered with PCI Council as QSA and ASV.	We are registered with PCI Council as a QSA. For ASV we work with one of our partners, which are registered as ASV with PCI council	Can a joint bid with our partners would be eligible for this project?	No
3	Section-3	11	3.1	Initial Phase - d) PCI-DSS QSA assessment for verification of compliance e) PCI-DSS documentation & recommendations for closure of QSA assessment report	Does NPCI expect bidder to carry out Gap Assessment in Initial Phase for its entire scope or only for the applications / system components added to the existing certification scope? Does NPCI expect bidder to provide onsite remediation support and ensure closure of all gaps?		NPCI expect bidder to provide onsite remediation support and ensure closure of all gaps identified across the scope.
4	Section-3	11	3.1	Initial Phase - b) External application layer penetration tests. c)Internal application layer penetration tests	How many applications of NPCI are presently in scope of the PCIDSS compliance program that would be included as a part of these tests?		Please refer RFP section 3.3. The exact count will be shared to L1 bidder.
5	Section-3	11	3.1	e) PCI-DSS documentation & recommendations for closure of QSA assessment report	Does the process involve the creation of documentation / support or only the evaluation of the existing documentation and evaluating for PCIDSS compliance?		The bidders scope includes documentation and support for closure of gaps identified in initial gap assessment.
6	Section-3	13	3.3	Servers including DB Servers Routers & Switches Firewalls & IPS	Please share the exact count of Servers (Windows, Solaris, AS 400) in scope Please share the exact number of Database Servers (Oracle, SQL) in scope Please share the exact number of Firewalls, Routers, IPS and Switches in scope		Please refer RFP section 3.3. The exact count will be shared to L1 bidder.
7	Section-3	13	3.4	2. Ensure ASV scans, Penetration Testing, and PCI-DSS certification timelines.	Should the activities and the pricing related to the activities be provided for one year or for all 3 years?		Prices for 1 yrs. and repeat order for next 2 yrs. on 1st year price basis.
8	Section-3	13	3.4	Bidder has to submit the PBG for renewal period	What is PBG?		Performance Bank Guaranty
9	Section-3	13	3.4	4. Analysis and assessments should be completed from the perspective of PCI-DSS certification and ensure minimum two or more full-time Security Consultant(s) onsite as required for delivery of the services included in SOW i.e. Section 3.	More clarity is required on this item, should the consultants be QSA's?		The bidder team should have QSA to complete the tasks as per SOW.

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

PRE BID REPLIES FOR NPCI:RFP:2013-14/0014 dated 28.08.2013-RFP for Appointment of Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) for Payment Card Industry - Data Security Standard (PCI DSS) Re-Certification

Sr. No#		Page No.	Clause No.	Description in RFP	Clarification Sought	Additional Remark (if any)	NPCI Replies
10	Section-3	13	3.4	6. Complete documentation in the initial phase as required for PCI-DSS certification, in a timely manner.	Does NPCI expects bidder to draft all the required documentation for PCI DSS ?		Bidder is expected to complete all documentation identified during the initial GAP assessment.
11	Section-3	13	3.4	3. The service provider has to ensure that the quarterly ASV scans are executed in timely manner; per quarter and approved by NPCI. 8. The Service Provider has to ensure to provide Onsite and Offsite Support for changes in system.	More clarity is required on this item on what would be the role of the QSA for support for Changes. Is an impact analysis / gap assessment expected for changes?		Bidder is expected to provide onsite and offsite support for impact analysis, GAP assessment and solution recommendation.
12	Section-8	26	8.9 Price	Price shall remain fixed for a period of 1 year from the date of Notification of award / Purchase Order. The bidder has to provide the cost for 1 year and rate contract for next 2 years.	More clarity is required on this item, what are all the activities that needs to be included as part of rate contract? Is there any format for listing the services/activities? Solution		All Activities as per SOW Section 3.
13	Section-8	26	8.8	Offsite Support for PCI-DSS for 1 year after Certification. This is optional item. 100% payment shall be made at the end of support year, in case NPCI engages the selected bidder for this service.	What is the kind of support expected through offline mode?		PCI-DSS compliance consulting support is expected from offline mode, which include GAP assessment, impact analysis and solution recommendation.
14	Section-3	11	3.1	1. Initial Phase:	Please provide the exact number of external IP for: 1) ASV scan 2) External PT	EXAMPLES of Answer: 1) External PT IP- 2) ASV Scan IP -	Please refer RFP section 3.3. The exact count will be shared to L1 bidder.
15	Section-3	11	3.1	1. Initial Phase:	Count of external facing application for application Penetration Testing – External		Please refer RFP section 3.3. The exact count will be shared to L1 bidder.
16	Section-3	11	3.1	1. Initial Phase:	Count of Internal facing application for application Penetration Testing – Internal		Please refer RFP section 3.3. The exact count will be shared to L1 bidder.
17	Section-3	11	3.1	1. Initial Phase:	Please indicated the frequency for both External & Internal Application Penetration Testing	1) External - 2) Internal -	As per PCI-DSS Certification Requirements.
18	Section-3	11	3.1	1. Initial Phase:	Please indicated the depth of expected Penetration Testing for external & Internal application - A) Black Box Test (Testing for pre-login pages) or Grey Box Test (Testing for Post Login pages) or Code Review . B) Type: Automated or Manual	1) External - Black Box Scanned based 2) Internal - Grey Box Scan based	As per PCI-DSS Certification Requirements.
19	Section-3	11	3.1	1. Initial Phase:	If Grey Box Test is required for application, please give details for each app (no. Of pages, privilege level)	App 1: 34 page, 2 user privileges App 2: 40 page, 2 user privileges	NA / No change in RFP.

भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

PRE BID REPLIES FOR NPCI:RFP:2013-14/0014 dated 28.08.2013-RFP for Appointment of Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) for Payment Card Industry - Data Security Standard (PCI DSS) Re-Certification

Sr. No#		Page No.	Clause No.	Description in RFP	Clarification Sought	Additional Remark (if any)	NPCI Replies
20	Section-3	11	3.1	1. Initial Phase:	Please indicate if the internal assets are accessible from a single location or travel to multiple locations is required. Please indicate count of out of Mumbai locations if travel is required		Other locations are accessible from Mumbai location.
21	Section-3	11	3.1	1. Initial Phase:	Please clarify if the Internal Vulnerability scan & Internal Network level Penetration test is also required. If yes, Please indicate the no. Of IP for this	Yes / NO Internal Vul Scan IP- Internal PT IP -	No, Internal Network scan is not required. Although External Network Scan, Internal & External AppSec Scan are required as mentioned in Section 3.
22	Section-3	11	3.1	1. Initial Phase:	Does NPCI needs confirmatory / verification tests as well for each activity within the same frequency?		Yes required.
23	Section-3	51	C2	Annexure	C2 annexure is applicable after Yr. 1. i.e. for Yr. 2 & Yr. 3. Is the C2 pricing a unit pricing?		C2 pricing is for 1 year and NPCI reserves the right to extend the contract on repeat order for next 2 year on 1st year price basis.