भारतीय राष्ट्रीय भुगतान निगम
NATIONAL PAYMENTS CORPORATION OF INDIA

Registered Office - 1001A, B Wing, 10th Floor, 'The Capital', Bandra Kurla Complex, Bandra (E), Mumbai - 400 051

Corrigendum-1

This is with reference to NPCI's RFP No RFP no. NPCI/RFP/2022-23/IT/03 dated 29.06.2022. RFP for procurement of Breach & Attack Simulation Solution. The prospective bidders may please note the following changes:

Sr. No.	Document Reference	Description	Existing RFP Clause	Amended clause vide this note
1	Section 1 - Bid Schedule and Address, Sr. no. 6, Page no. 8	Last date and time for Bid Submission	19.07.2022 5.30 pm	**27.07.2022 5.30 pm**
2	Section 1 - Bid Schedule and Address, Sr. no. 7, Page no. 8	Date and Time of Eligibility & Technical bid Opening	19.07.2022 6.30 pm	**27.07.2022 6.30 pm**
3	Section 9 - Technical Specifications, Clause no. D25, Page no. 39	Use Cases Support	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps.	The Solution should provide **Proof of Attack** for manual assessments / simulation along with Mitigation steps.
4	Section 9 - Technical Specifications, Clause no. D31, Page no. 39	Use Cases Support	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	The solution should provide **technology/vendor specific remediation guidelines** and prioritization as mitigation recommendations
5	Section 9 - Technical Specifications, Clause no. C6, Page no. 38	Security Solutions Support & Integration	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)
6	Section 9 - Technical Specifications, Clause no. D2, Page no. 38	Use Cases Support	The solution should include attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets.	The solution should include **or support creation of custom** attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets.

7	Section Section 9 - Technical Specifications, Clause no. D42, Page no. 39	Use Cases Support	The solution should support use cases specific to Kubernetes, Docker, Container deployments Compliance – Must have	The solution should support use cases specific to Kubernetes, Docker, Container deployments **Compliance – Good to have (Optional)**
8	Section Section 9 - Technical Specifications, Clause no. D13, Page no. 38	Use Cases Support	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioural detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioural detection (EDR), signature-based detection (anti-virus).
9	Section Section 9 - Technical Specifications, Clause no. D34, Page no. 39	Use Cases Support	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC Compliance – Must have	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC **Compliance – Good to have (Optional)**
10	Section Section 9 - Technical Specifications, Clause no. D8, Page no. 38	Use Cases Support	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls, **Web Based applications etc.**
11	Section Section 9 - Technical Specifications, Clause no. D18, Page no. 38	Use Cases Support	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g. Gdrive, onedrive, dropbox, slack etc.)	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test).