NPCI/2023-24/PROC/1258 Date: 29th February 2024

**Corrigendum-3**

This is with reference to NPCI's EOI no. NPCI/EOI/2023-24/IT/03 dated 24th January 2024 - Invitation for Expression of Interest for Managed DDOS Protection Service. The prospective bidders may please note the following changes:

1) Change in the Last date and time for Bid Submission and date for Eligibility & Technical bid Opening:

| Document Reference | Description | Initial dates | Revised dates |
|---|---|---|---|
| EOI Schedule & communication address – page 7 | Last date and time for Bid Submission | 29-Feb-2024 05.30 pm | 08-March-2024 05.30 pm |
| EOI Schedule & communication address – page 7 | Date and Time of Eligibility criteria response opening | 29-Feb-2024 06.30 pm | 08-March-2024 06.30 pm |

2) Changes in the technical specification document & scope of work document as per detailed below:

| Sr. No. | Document Reference | Description | Existing RFP Clause | Amended clause vide this note |
|---|---|---|---|---|
| 1 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 37 Clause A.7 | A - Fundamental Requirements | Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc. | Solution should support to pass traffic on all layer 4 and layer 7 protocols . |
| 2 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 37 Clause A.9 | A - Fundamental Requirements | The Proposed solution must not modify MAC or IP addresses of passed frames. | Point to be dropped |
| | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 Clause C.1 | C – Integration Capabilities | DDOS solution should integrate with existing SIEM engine seamlessly through syslog | Sloution should be seamlessly integrate with existing SIEM thourgh API |
| 4 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 Clause C.3 | C – Integration Capabilities | DDOS solution should Integration with TACACS+ and RADIUS | Solution can integrate with Azure AD through API |
| 5 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 Clause B.9 | B – Security / DDoS Feature | The proposed Solution should support Flowspec. | Point to be dropped |
| 6 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 10 Chapter 3 | Scope of Work | 11. Bidder to factor and propose software-based solution as per their architecture which includes associated monitoring and management software(s) and database license if any. | Point to be dropped |
| 7 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 10 Chapter 3 | Scope of Work | 9. Bidder should ensure availability of on-site resources for end-to-end deployment of complete solution (with back-to-back support from OEM PS) until handover to NPCI operations team.<br><br>17. Bidders are expected to provide the onsite support post implementation if the technical issues are not remotely resolved. | As Solution is SAAS deployment no On-site resource required for Implementation. |

| | | | | |
|---|---|---|---|---|
| 8 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 9 Chapter 3 | Scope of Work | 5. Integrate the solution with On-prem NPCI's Active Directory system for authentication & other application based on rest APIs. | Solution has to intergrate with Azure AD through API.which is help users in RBAC. |
| 9 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 37 Clause A.21 | A - Fundamental Requirements | The committed uptime of the proposed solution should be 100% availability on yearly basis at each site. | Uptime can be 99.99999 |
| 10 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 38 A 20 | A - Fundamental Requirements | The proposed solution should support TLS1.2 and above based traffic. | Point to be dropped |
| 11 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 38 B.3 | B – Security / DDoS Feature | The proposed solution must have an updated threat feed that describes new malicious traffic (botnets, phishing) | Proposed solution should support all type of DDOS attack feed including zero day attacks . |
| 12 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 38 B.7 | B – Security / DDoS Feature | The proposed solution should have a mitigation mechanism to protect against zero-day DoS and DDoS attacks without manual intervention and response time should be minimal. | The proposed solution should have a mitigation mechanism to protect against zero-delay DoS and DDoS attacks without manual intervention and response time should be minimal. |
| 13 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 B.13 | B – Security / DDoS Feature | The proposed Solution must be able to detect and block HTTP GET/POST Flood and should support mechanisms to avoid False Positives. | Proposed solution has to support all flood attacks |
| 14 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 C.4 | C – Security / DDoL Feature | Solution should support MFA capabilities including FIDO2/Web Authentication, OATH (TOTP/HOTP) for access management. | Solution should support MFA capabilities including,SAML, FIDO2/Web Authentication, OATH (TOTP/HOTP) for access management. |
| 15 | EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024 Page 39 B.11 | Invitation for expression of interest (eoi) – managed ddos protection service | The proposed Solution should support for all protocols at layer 3. | The proposed Solution should support for all protocols at layer 3 to layer 7 |
| 16 | Additional clarification required | - | Does NPCI want the SaaS Platform to be able to customize the TLS connection attributed between PoP to Origin such as SNI Selection, Security Level, Origin Server Verification, MTLS. | No Change in RFP |
| 17 | Additional clarification required | - | Does NPCI want SAAS Platform to support Auto Certificate generation for delegated Domains or for non delegated domain should support Certificate minting | No Change in RFP |
| 18 | Additional clarification required | - | Does NPCI want the Platform to be able to support custom listening ports other than 80 & 443. Front end and Backend ports should be customizable | No Change in RFP |
| 19 | Additional clarification required | - | Does NPCI want the proposed SaaS Platform to support JS, Captcha and Policy based challenges to deal with Layer 7 | No Change in RFP |

| | | | | |
|---|---|---|---|---|
| | | | DoS attacks. This has been critical in various setup. | |
| 20 | Additional clarification required | - | Does NPCI want proposed SAAS platform to also have the ability to allow installations of customer edge nodes as well, in case NPCI requires same set of layer 7 security capabilities for internal apps or inside the landing zone of private or public cloud | No Change in RFP |
| 21 | Query | - | Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection | No Change in RFP |
| 22 | Additional clarification required | - | Does NPCI is looking at platform to provide a multi-phase protection system that protects web applications against Formjacking, Magecart, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation. | No Change in RFP |
| 23 | Additional clarification required | - | Does NPCI want the SaaS Platform to be able to customize the TLS connection attributed between PoP to Origin such as SNI Selection, Security Level, Origin Server Verification, MTLS. | No Change in RFP |
| 24 | Additional clarification required | - | Does NPCI want SAAS Platform to support Auto Certificate generation for delegated Domains or for non delegated domain should support Certificate minting | No Change in RFP |
| 25 | Additional clarification required | - | Does NPCI want the Platform to be able to support custom listening ports other than 80 & 443. Front end and Backend ports should be customisable | No Change in RFP |
| 26 | Additional clarification required | - | Does NPCI want the proposed SaaS Platform to support JS, Captcha and Policy based challanegs to deal with Layer 7 DoS attacks. This has been critical in various setup. | No Change in RFP |
| 27 | Query | - | Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection | No Change in RFP |
| 28 | Additional clarification required | - | Does NPCI is looking at platform to provide a multi-phase protection system that protects web applications against Formjacking, Magecart, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation. | No Change in RFP |
| 29 | Additional clarification required | - | Does NPCI want the SaaS Platform to be able to customize the TLS connection attributed between PoP to Origin such as SNI Selection, Security Level, Origin Server Verification, MTLS. | No Change in RFP |
| 30 | Additional clarification required | - | Does NPCI want SAAS Platform to support Auto Certificate generation for delegated Domains or for non delegated domain should support Certificate minting | No Change in RFP |

| | | | | |
|---|---|---|---|---|
| 31 | Additional clarification required | - | Does NPCI want the Platform to be able to support custom listening ports other than 80 & 443. Front end and Backend ports should be customizable | No Change in RFP |
| 32 | Additional clarification required | - | Does NPCI want the proposed SaaS Platform to support JS, Captcha and Policy based challenges to deal with Layer 7 DoS attacks. This has been critical in various setup. | No Change in RFP |
| 33 | Additional clarification required | - | Does NPCI is looking at platform to provide a multi-phase protection system that protects web applications against Formjacking, Magecart, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation. | No Change in RFP |
| 34 | Additional clarification required | - | Does NPCI want the SaaS Platform to be able to customize the TLS connection attributed between PoP to Origin such as SNI Selection, Security Level, Origin Server Verification, MTLS. | No Change in RFP |
| 35 | Additional clarification required | - | Does NPCI want SAAS Platform to support Auto Certificate generation for delegated Domains or for non delegated domain should support Certificate minting | No Change in RFP |
| 36 | Additional clarification required | - | Does NPCI want the Platform to be able to support custom listening ports other than 80 & 443. Front end and Backend ports should be customizable | No Change in RFP |
| 37 | Additional clarification required | - | Does NPCI want the proposed SaaS Platform to support JS, Captcha and Policy based challanegs to deal with Layer 7 DoS attacks. This has been critical in various setup. | No Change in RFP |
| 38 | Additional clarification required | - | Does NPCI want proposed SAAS platform to also have the ability to allow installations of customer edge nodes as well, in case NPCI requires same set of layer 7 security capabilities for internal apps or inside the landing zone of private or public cloud | No Change in RFP |
| 39 | Query | - | Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection | No Change in RFP |
| 40 | Additional clarification required | - | Does NPCI is looking at platform to provide a multi-phase protection system that protects web applications against Formjacking, Magecart, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation. | No Change in RFP |
| 41 | Additional clarification required | - | Does NPCI want the SaaS Platform to be able to customize the TLS connection attributed between PoP to Origin such as SNI Selection, Security Level, Origin Server Verification, MTLS. | No Change in RFP |

| | | | | |
|---|---|---|---|---|
| 42 | Additional clarification required | - | Does NPCI want SAAS Platform to support Auto Certificate generation for delegated Domains or for non delegated domain should support Certificate minting | No Change in RFP |
| 43 | Additional clarification required | - | Does NPCI want the Platform to be able to support custom listening ports other than 80 & 443. Front end and Backend ports should be customisable | No Change in RFP |
| 44 | Additional clarification required | - | Does NPCI want the proposed SaaS Platform to support JS, Captcha and Policy based challanegs to deal with Layer 7 DoS attacks. This has been critical in various setup. | No Change in RFP |
| 45 | Additional clarification required | - | Does NPCI want proposed SAAS platform to also have the ability to allow installations of customer edge nodes as well, in case NPCI requries same set of layer 7 security capabilties for internal apps or inside the landing zone of private or public cloud | No Change in RFP |
| 46 | Query | - | Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection | No Change in RFP |
| 47 | Additional clarification required | - | Does NPCI is looking at platform to provide a multi-phase protection system that protects web applications against Formjacking, Magecart, and other malicious JavaScript attacks. This multi-phase protection system includes detection, alerting, and mitigation. | No Change in RFP |