NPCI/EOI/2023-24/IT/03 dated 24th January 2024
INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE
RESPONSES TO PRE-BID QUERIES

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
1	B] Other than start-ups:	13	7	Bid earnest money (EMD)	We are the MSME Company and would request for the EMD submission exemption.		Exemption for EMD is not applicable as NPCI is not a Government organization. All bidders who are participating has to submit EMD amount either online transfer or in the form of Bank Guarantee
2	Section -1 Bid Cost	8	12	Bid Cost	We are the MSME Company and would request for the bid document cost exemption.		Exemption for Bid cost is not applicable as NPCI is not Government Organization. All bidders who are participating in EOI has to submit BID cost
3	Bid Security	8	13	Bid Security (EMD)	We are the MSME Company and would request for the EMD submission exemption.		Exemption for EMD is not applicable as NPCI is not a Government organization. All bidders who are participating has to submit EMD amount either online transfer or in the form of Bank Guarantee
4	A - Fundamental Requirements	37	A.7	Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc.	We request NPCI to clarify if they are also looking for DNS primary/secondary solutions with DNS security from the DDOS bidder.		Refer to Corrigendum 3
5	Additional clarification required	-	-	-	NPCI should also ask for PoP outside India supporting Anycast, this will enable in case of disaster scenarios. The SAAS Solution should be running out of over 20+ PoP with all PoPs running in ANYCAST in order to ensure Global Availability		No change in EOI Terms
6	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 EOI Terms
7	A - Fundamental Requirements	37	A.7	The Proposed solution must not modify MAC or IP addresses of passed frames.	We request NPCI to clarify if this is relevant for cloud based SAAS service. This technical point is usually applicable to on-prem layer 2 deployments of hardware devices for DDOS		Refer to Corrigendum 3
8	A - Fundamental Requirements	38	A.16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a SaaS service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
9	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 EOI Terms
10	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 EOI Terms
11	Additional clarification required	-	-	-	Does NPCI want SAAS Platform to support unlimited data transfer		No change in EOI Terms
12	A - Fundamental Requirements	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	We request NPCI to revise this point and change it to 99.99% of higher as it is dependent on external factors as well.		uptime has to be 100% availability
13	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 EOI Terms
14	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to support behavioral based malicious user detection for low and slow attacks and potential misbehavior. The platform should have option to define client IP or query parameter or header name or cookie or TLS finger print as unique identifier to define individual endpoint.		No change in EOI Terms

NPCI/EOI/2023-24/IT/03 dated 24th January 2024
INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE
RESPONSES TO PRE-BID QUERIES

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
15	B – Security / DDoS Feature	38	B.8	The proposed Solution should support DNS query source validation, DNS Query, per-Source Flooding.	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a saas service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
16	B – Security / DDoS Feature	39	B.9	The proposed Solution should support Flowspec.	We request NPCI to clarify if the requirement is pure SAAS based DDOS offering or a hybrid approach where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		SaaS with always on
17	Additional clarification required	-	-	-	Does NPCI want SaaS platform to be able to consume Openapi spec/Swagger V2 and V3 file for API endpoint confg and should support positive security configuration for published apis.		No change in EOI Terms
18	Additional clarification required	-	-	-	Does NPCI need System should report Malicious user dashboard		No change in EOI Terms
19	C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Being a SaaS platform, many intergrations are based on API which is a standard across multiple OEM's. So we request NPCI to modify this point as follows. "DDOS solution should integrate with existing SIEM engine seamlessly through syslog or API "		Refer to Corrigendum 3
20	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to have ability to define Circuit Breaker configuration - this should provide mechnism for watching failures in upstream connections or requests and if the failures reach a certain threashold , automatically fail subsequent requests which allows to apply back pressure on downstream quickly		No change in EOI Terms
21	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 EOI Terms
22	Additional clarification required	-	-	-	Does NPCI looking forward to have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.		No change in EOI Terms
23	C – Integration Capabilities	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
24	Additional clarification required	-	-	-	Does NPCI need Proposed SaaS Solution to provide Organization capability to restrict usages of specific PoPs only by Bring your own IP services (/24 Pool)		No change in EOI Terms
25	Additional clarification required	-	-	-	Does NPCI need OEM PoP services only which will have better SLA and not any Public Cloud to avoid dependency of cloud providers SLA		No change in EOI Terms
26	Eligibility Criteria	11	4	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	Do you mean the bidder should have reference for similar setup or just experience of managing DDoS solution		should have Similar setup implementation

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
27	Query	-	-	-	Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection		No change in EOI Terms
28	Additional points to consider	-	-	-	SaaS must support following Violation Detections		No change in EOI Terms
					- Apache Whitespace		
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		
29	Additional clarification required	-	-	-	Does NPCI want the proposed platform to also provide protection based on a variety of threat intel sourced from the real world campaigns to attack and/or take over resources. The Threat Campaign protection should be based on current “in-the-wild” attacks. These signatures contain contextual information about the nature and purpose of the attack.		No change in EOI Terms
30	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 EOI Terms
31	A - Fundamental Requirements	37	A.7	Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc.	We request NPCI to clarify if they are also looking for DNS primary/secondary solutions with DNS security from the DDOS bidder.		Refer to Corrigendum 3
32	Additional clarification required	-	-	-	NPCI should also ask for PoP outside India supporting Anycast, this will enable in case of disaster scenarios. The SAAS Solution should be running out of over 20+ PoP with all PoPs running in ANYCAST in order to ensure Global Availability		No change in EOI Terms
33	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 EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
34	A - Fundamental Requirements	37	A.7	The Proposed solution must not modify MAC or IP addresses of passed frames.	We request NPCI to clarify if this is relevant for cloud based SAAS service. This techical point is usually applicable to on-prem layer 2 deployments of hardware devices for DDOS		Refer to Corrigendum 3
35	A - Fundamental Requirements	38	A.16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a SaaS service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
36	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 EOI Terms
37	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 EOI Terms
38	Additional clarification required	-	-	-	Does NPCI want SAAS Platform to support unlimited data transfer		No change in EOI Terms
39	A - Fundamental Requirements	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	We request NPCI to revise this point and change it to 99.99% of higher as it is dependent on external factors as well.		uptime has to be 100% availability
40	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 EOI Terms
41	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to support behavioral based malicius user detction for low and slow attacks and potential misbahaviour. The platform should have option to define client IP or query parameter or header name or cookie or TLS finger print as unique identifier to define individual endpoint.		No change in EOI Terms
42	B – Security / DDoS Feature	38	B.8	The proposed Solution should support DNS query source validation, DNS Query, per-Source Flooding.	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a saas service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
43	B – Security / DDoS Feature	39	B.9	The proposed Solution should support Flowspec.	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		SaaS with always on
44	Additional clarification required	-	-	-	Does NPCI want SaaS platform to be able to consume Openapi spec/Swagger V2 and V3 file for API endpoint confg and should support positive security configuration for published apis.		No change in EOI Terms
45	Additional clarification required	-	-	-	Does NPCI need System should report Malicous user dashboard		No change in EOI Terms
46	C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Being a SaaS platform, many intergrations are based on API which is a standard across multiple OEM's. So we request NPCI to modify this point as follows. "DDOS solution should integrate with existing SIEM engine seamlessly through syslog or API "		Refer to Corrigendum 3
47	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to have ability to define Circuit Breaker configuration - this should provide mechnism for watching failures in upstream connections or requests and if the failures reach a certain threashold , automatically fail subsequent requests which allows to apply back pressure on downstream quickly		No change in EOI Terms
48	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 EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
49	Additional clarification required	-	-	-	Does NPCI looking forward to have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.		No change in EOI Terms
50	C – Integration Capabilities	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
51	Additional clarification required	-	-	-	Does NPCI need Proposed SaaS Solution to provide Organization capability to restrict usages of specific PoPs only by Bring your own IP services (/24 Pool)		No change in EOI Terms
52	Additional clarification required	-	-	-	Does NPCI need OEM PoP services only which will have better SLA and not any Public Cloud to avoid dependency of cloud providers SLA		No change in EOI Terms
53	Eligibility Criteria	11	4	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	Do you mean the bidder should have reference for similar setup or just experience of managing DDoS solution		Similar setup is more advantage
54	Query	-	-	-	Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection		No change in EOI Terms
	Additional points to consider	-	-	-	SaaS must support following Violation Detections		No change in EOI Terms
					- Apache Whitespace		
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		
55	Additional clarification required	-	-	-	Does NPCI want the proposed platform to also provide protection based on a variety of threat intel sourced from the real world campaigns to attack and/or take over resources. The Threat Campaign protection should be based on current “in-the-wild” attacks. These signatures contain contextual information about the nature and purpose of the attack.		No change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
56	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 EOI Terms
57	A - Fundamental Requirements	37	A.7	Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc.	We request NPCI to clarify if they are also looking for DNS primary/secondary solutions with DNS security from the DDOS bidder.		NPCI is looking for always on DDOS protection
58	Additional clarification required	-	-	-	NPCI should also ask for PoP outside India supporting Anycast, this will enable in case of disaster scenarios. The SAAS Solution should be running out of over 20+ PoP with all PoPs running in ANYCAST in order to ensure Global Availability		No change in EOI Terms
59	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 EOI Terms
60	A - Fundamental Requirements	37	A.7	The Proposed solution must not modify MAC or IP addresses of passed frames.	We request NPCI to clarify if this is relevant for cloud based SAAS service. This techical point is usually applicable to on-prem layer 2 deployments of hardware devices for DDOS		Refer to Corrigendum 3
61	A - Fundamental Requirements	38	A.16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a SaaS service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
62	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 EOI Terms
63	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 EOI Terms
64	Additional clarification required	-	-	-	Does NPCI want SAAS Platform to support unlimited data transfer		No change in EOI Terms
65	A - Fundamental Requirements	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	We request NPCI to revise this point and change it to 99.99% of higher as it is dependent on external factors as well.		uptime has to be 100% availability
66	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 EOI Terms
67	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to support behavioral based malicius user detction for low and slow attacks and potential misbahaviour. The platform should have option to define client IP or query parameter or header name or cookie or TLS finger print as unique identifier to define individual endpoint.		No change in EOI Terms
68	B – Security / DDoS Feature	38	B.8	The proposed Solution should support DNS query source validation, DNS Query, per-Source Flooding.	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a saas service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
69	B – Security / DDoS Feature	39	B.9	The proposed Solution should support Flowspec.	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
70	Additional clarification required	-	-	-	Does NPCI want SaaS platform to be able to consume Openapi spec/Swagger V2 and V3 file for API endpoint confg and should support positive security configuration for published apis.		No change in EOI Terms
71	Additional clarification required	-	-	-	Does NPCI need System should report Malicous user dashboard		No change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
72	C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Being a SaaS platform, many intergrations are based on API which is a standard across multiple OEM's. So we request NPCI to modify this point as follows. "DDOS solution should integrate with existing SIEM engine seamlessly through syslog or API "		Refer to Corrigendum 3
73	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to have ability to define Circuit Breaker configuration - this should provide mechnism for watching failures in upstream connections or requests and if the failures reach a certain threashold , automatically fail subsequent requests which allows to apply back pressure on downstream quickly		No change in EOI Terms
74	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 EOI Terms
75	Additional clarification required	-	-	-	Does NPCI looking forward to have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.		No change in EOI Terms
76	C – Integration Capabilities	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
77	Additional clarification required	-	-	-	Does NPCI need Proposed SaaS Solution to provide Organization capability to restrict usages of specific PoPs only by Bring your own IP services (/24 Pool)		No change in EOI Terms
78	Additional clarification required	-	-	-	Does NPCI need OEM PoP services only which will have better SLA and not any Public Cloud to avoid dependency of cloud providers SLA		No change in EOI Terms
79	Eligibility Criteria	11	4	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	Do you mean the bidder should have reference for similar setup or just experience of managing DDoS solution		Similar setup is more advantage
80	Query	-	-	-	Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection		No change in EOI Terms
81	Additional points to consider	-	-	-	SaaS must support following Violation Detections		No Change in EOI Terms
					- Apache Whitespace		
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
82	Additional clarification required	-	-	-	Does NPCI want the proposed platform to also provide protection based on a variety of threat intel sourced from the real world campaigns to attack and/or take over resources. The Threat Campaign protection should be based on current “in-the-wild” attacks. These signatures contain contextual information about the nature and purpose of the attack.		No Change in EOI Terms
	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 EOI Terms
83	Confidentiality	19	6.6	Information relating to the examination, clarification and comparison of the proposals shall not be disclosed to any Bidders or any other persons not officially concerned with such process until the identification process is over. The undue use by any Bidder of confidential information related to the process may result in rejection of its proposal. During the execution of the project except with the prior written consent of the NPCI, the Bidder and its personnel shall not at any time communicate to any person or entity any confidential information acquired in the course of the proposal	We request, this clause to be made mutual		No Change in EOI Terms
84	Design Ownership	19	6.7	The Bidder shall indemnify the NPCI from all actions, costs, claims, demands, expenses and liabilities, whatsoever, resulting from any actual or alleged infringement as aforesaid and at the expenses of the Bidder. NPCI shall be defended in the defence of any proceedings which may be brought in that connection.	We request addition of the following clause: With respect to all claims including those for intellectual property claims, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent twelve (12) months of charges collected by Bidder pursuant to the applicable PO/Order giving rise to the liability		No Change in EOI Terms
85	Scope of Work	9	Chapter 3	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.	Understanding is that NPCI is expecting a Cloud-based solution and not a Hardware based solution. Please confirm.		Refer to Corrigendum 3
86	Scope of Work	10	Chapter 3	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. 17. Bidders are expected to provide the onsite support post implementation if the technical issues are not remotely resolved.	Since the DDoS solution required is Cloud based, kindly specify the activities expected from the resource on site.		Refer to Corrigendum 3
87	Scope of Work	9	Chapter 3	5. Integrate the solution with On-prem NPCI’s Active Directory system for authentication & other application based on rest APIs.	Kindly specify any use case that calls for integration with NPCI's AD.		Refer to Corrigendum 3
88	Scope of Work	10	Chapter 3	10. Bidder should support the migration of the existing DDOS solution policies and features and building new policies required by organization for the proposed solution during the implementation phase.	Please specify: 1. Existing DDoS solution OEM 2. Count of existing policies and features to be migrated		This will be shared separately with the requester
89	Scope of Work	11	Chapter 3	35.SupportModel: -24x7 and 365 days Service Coverage. (Email/Phone/Portal) -Technical Account Manager -Escalation Matrix -Periodic Health Checks	Please specify the frequency of periodic health checks?		Monthly

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
90	ANNEXURE M - Technical Specifications	37	A.2	DDOS solution should provide 6GBPS of clean traffic distributed across 3 locations, i.e., 2 GBPS clean traffic per location.	Kindly specify the names of the locations and address where the DDoS service is required.		We have 3 sites(Hyderabad-Narsingi,Chennai-Siruseri,Chennai-STT)
91	ANNEXURE M - Technical Specifications	37	A.2	DDOS solution should provide 6GBPS of clean traffic distributed across 3 locations, i.e., 2 GBPS clean traffic per location.	Kindly specify the Internet link provider name and bandwidth of each link at each location to be considerd for DDoS mitigation.		Solution should be agnostic to the Internet link provider
92	ANNEXURE M - Technical Specifications	37	A.2	DDOS solution should provide 6GBPS of clean traffic distributed across 3 locations, i.e., 2 GBPS clean traffic per location.	Please specify the number of Public IPs and subnets to be protected.		Solution should be agnostic to the public ip subnets
93	ANNEXURE M - Technical Specifications	37	A.2	DDOS solution should provide 6GBPS of clean traffic distributed across 3 locations, i.e., 2 GBPS clean traffic per location.	Are all the links at each location active-active or active-passive?		All location will have Active Internet access at all time
94	ANNEXURE M - Technical Specifications	37	A.2	DDOS solution should provide 6GBPS of clean traffic distributed across 3 locations, i.e., 2 GBPS clean traffic per location.	Do the NPCI WAN routers support GRE configuration?		Yes GRE is supported
95	General	General	General	General	In case there are Hardware footprints required to achieve full capability, will the client provide space to install the DDoS hardware components.		Solution should be SaaS based with no hardware requirement
96	D- Monitoring & Dashboard	39	D.3	Solution should provide DDoS attacks log backup and Filterable /Exportable Attack Log	Please specify the duration of log backup that is required.		30 days log minimum should be minimum available from cloud based solution
97	EOI	7	6	Last date and time for Bid Submission - 05.02.2024 5:30 PM	Requesting for extension of 1 week for the submission		Refer to Corrigendum 3
98	EOI	10	13	The bidder shall provide 24*7*365 basis post implementation technical support for the components supplied.	Requesting for How many years for the Maintanacne		3 years
99	EOI	10	10	Bidder should support the migration of the existing DDOS solution policies and features and building new policies required by organization for the proposed solution during the implementation phase	Requesting for Share the existing network infrastructure,topology and policies Details.Are there any constraints or limitations on exisiting bandwidth usage?How are the network resources distributed across different locations?what are the exisiting critical services running with DDOS protection.? is it hosted on Prem or in Public cloud platform?		Currently F5 On Prem is used as DDOS solution further details will be given once bidder is finalized
100	EOI	10	10	Bidder should support the migration of the existing DDOS solution policies and features and building new policies required by organization for the proposed solution during the implementation phase	Requesting share the details of Exiting Router, Firewall Interface , Number of Used Ports , What is your current bandwidth capacity, and throughput ? Type of Ports details		Currently F5 On Prem is used as DDOS solution further details will be given once bidder is finalized
101	A - Fundamental Requirements	37	A.7	Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc.	We request NPCI to clarify if they are also looking for DNS primary/secondary solutions with DNS security from the DDOS bidder.		Refer to Corrigendum 3
102	Additional clarification required	-	-	-	NPCI should also ask for PoP outside India supporting Anycast, this will enable in case of disaster scenarios. The SAAS Solution should be running out of over 20+ PoP with all PoPs running in ANYCAST in order to ensure Global Availability		No Change in EOI Terms
103	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 EOI Terms
104	A - Fundamental Requirements	37	A.7	The Proposed solution must not modify MAC or IP addresses of passed frames.	We request NPCI to clarify if this is relevant for cloud based SAAS service. This techical point is usually applicable to on-prem layer 2 deployments of hardware devices for DDOS		Refer to Corrigendum 3
105	A - Fundamental Requirements	38	A.16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a SaaS service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
106	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 EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
107	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 EOI Terms
108	Additional clarification required	-	-	-	Does NPCI want SAAS Platform to support unlimited data transfer		No Change in EOI Terms
109	A - Fundamental Requirements	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	We request NPCI to revise this point and change it to 99.99% of higher as it is dependent on external factors as well.		Refer to Corrigendum 3
110	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 EOI Terms
111	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to support behavioral based malicius user detction for low and slow attacks and potential misbahaviour. The platform should have option to define client IP or query parameter or header name or cookie or TLS finger print as unique identifier to define individual endpoint.		No Change in EOI Terms
112	B – Security / DDoS Feature	38	B.8	The proposed Solution should support DNS query source validation, DNS Query, per-Source Flooding.	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a saas service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
113	B – Security / DDoS Feature	39	B.9	The proposed Solution should support Flowspec.	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
114	Additional clarification required	-	-	-	Does NPCI want SaaS platform to be able to consume Openapi spec/Swagger V2 and V3 file for API endpoint confg and should support positive security configuration for published apis.		No Change in EOI Terms
115	Additional clarification required	-	-	-	Does NPCI need System should report Malicous user dashboard		No Change in EOI Terms
116	C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Being a SaaS platform, many intergrations are based on API which is a standard across multiple OEM's. So we request NPCI to modify this point as follows. "DDOS solution should integrate with existing SIEM engine seamlessly through syslog or API "		Refer to Corrigendum 3
117	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to have ability to define Circuit Breaker configuration - this should provide mechnism for watching failures in upstream connections or requests and if the failures reach a certain threashold , automatically fail subsequent requests which allows to apply back pressure on downstream quickly		No Change in EOI Terms
118	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 EOI Terms
119	Additional clarification required	-	-	-	Does NPCI looking forward to have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.		No Change in EOI Terms
120	C – Integration Capabilities	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
121	Additional clarification required	-	-	-	Does NPCI need Proposed SaaS Solution to provide Organization capability to restrict usages of specific PoPs only by Bring your own IP services (/24 Pool)		No Change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
122	Additional clarification required	-	-	-	Does NPCI need OEM PoP services only which will have better SLA and not any Public Cloud to avoid dependency of cloud providers SLA		No Change in EOI Terms
123	Eligibility Criteria	11	4	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	Do you mean the bidder should have reference for similar setup or just experience of managing DDoS solution		Similar setup is more advantage
124	Query	-	-	-	Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection		No Change in EOI Terms
125	Additional points to consider	-	-	-	SaaS must support following Violation Detections		No Change in EOI Terms
					- Apache Whitespace		No Change in EOI Terms
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		
126	Additional clarification required	-	-	-	Does NPCI want the proposed platform to also provide protection based on a variety of threat intel sourced from the real world campaigns to attack and/or take over resources. The Threat Campaign protection should be based on current “in-the-wild” attacks. These signatures contain contextual information about the nature and purpose of the attack.		No Change in EOI Terms
127	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 EOI Terms
128	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	9	6	Integrate the solution with On-prem NPCI’s Active Directory system for authentication & other application based on rest APIs.	Kindly provide details on the specific use cases that NPCI is seeking post-integration with On-prem NPCI's Active Directory, considering the multitude of policies associated with users. Additionally, please confirm the list of applications for authentication integration, specifying those reliant on REST APIs.		syslog or API
129	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	9	7	Integrate the solution with the NPCI’s SMTP, BMC, SIEM/SOAR, TIP.	Please share information on which SIEM/SOAR, TIP solutions should be integrated with the proposed solution.		Integrate the solution with the NPCI’s SMTP, BMC Software, SIEM/SOAR-log rhythm, TIP-cyware.

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
130	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	8	Bidder should update and maintain all supplied equipment to correctly reflect actual state of the setup at any point in time during the warranty period.	As NPCI is exploring a Managed DDoS Protection Service, the solution is intended to be delivered as a SAAS/PAAS, eliminating the need for any appliance delivery. NPCI exclusively seeking a cloud-based solution?		Yes, seeking for Cloud-Based solution
131	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	9	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.	Given that the solution will be offered on the cloud and the OEM will handle the complete implementation remotely, as it is their platform and they have full access, there may not be a necessity for individuals to visit onsite. Kindly grant permission for remote implementation.		Refer to Corrigendum 3
132	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	10	Bidder should support the migration of the existing DDOS solution policies and features and building new policies required by organization for the proposed solution during the implementation phase.	I kindly request you to share the specifics of the current DDoS solution, including details on the original equipment manufacturer (OEM), models, and the type of deployment in use.		Currently F5 On Prem is used as DDOS solution further details will be given once bidder is finalized
133	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	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.	As NPCI is considering a Managed DDoS Protection Service, the solution will be provided as SAAS/PAAS. Consequently, there will be no requirement for any monitoring and management software or database licenses.		Okay
134	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	16	Bidder should assign technical experienced person to NPCI for deployment of Always ON DDOS with minimum of 2+ years on experience. Resumes of the team members to be shared to NPCI as part of RFP response.	Since the solution is a platform-based cloud solution and will be wholly managed and implemented by the OEM, they will allocate resources accordingly. Consequently, we kindly request that you avoid engaging the technical personnel of bidders, as the OEM will be overseeing the process.		Implementation done by OEM or Partner must have 2+ years of experience on proposed solution/technology.
135	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	21	Bidders are expected to provide the onsite support post implementation if the technical issues are not remotely resolved.	Since there will be no on-site deployment and the solution will be provided as a SaaS/PaaS service, I kindly request you to omit the clause regarding on-site support.		Refer to Corrigendum 3
136	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	24	OEM should provide Technical Training to all the Operation support staff and administrators of NPCI.	Please provide information on the number of individuals from NPCI for whom the training needs to be conducted.		3 Batches of atleast 8 to 10 people for a week
137	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	28	The selected Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly layout the overall steps from initiation to closure of this engagement.	What is the duration of the contract?		3 years
138	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	32	The Bidder will have to provide all the MIS reports as per the requirements of the NPCI.	Kindly specify whether the dedicated EMS tool should be regarded as a distinct consideration.		OEM or Bidder should can provide weekly and monthly reports on mail
139	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	33	Bidder should provide soft copy and hard copies of Training material	We only provide soft copies as we do not produce any hard copies.		Ok
140	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	35	SupportModel: -24x7 and 365 days Service Coverage. (Email/Phone/Portal) -Technical Account Manager -Escalation Matrix -Periodic Health Checks -Monthly reports & Governance Meetings -Onsite visits as required -Proactive Invitations to Beta programs has context menu Compose Paragraph	As the solution is entirely owned and managed by the OEM, is it acceptable if onsite visits are not conducted by the bidder's technical team?		fine,Even OEM or bidder technical team presence is required .

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
141	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	32	Annexure-H B2 Eligibility criteria	The bidder should have reported minimum annual turnover of Rs. 20 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (2020-21, 2021-22 and 2022-23). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	We kindly request NPCI to consider a vendor profitability acceptance period of 2 years instead of 3 years, given the one-year loss incurred during the COVID-19 year.		No Change in EOI Terms
142	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 3	OEM Infrastructure should have multiple scrubbing centers (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	Should each of the multiple scrubbing centers have a dedicated scrubbing capacity of 10 TBPS individually, or is the capacity meant to be combined?		OEM Infrastructure should have capacity to absorb High volume DDOS attack from India location scrubbing centre
143	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 5	Proposed solution should be agnostic to the Internet Service Provider (ISP) solutions and protect all Internet facing applications of NPCI	Who are your link providers, and what is the link capacity in each of the data centers?		This information will be provided to successful bidder
144	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 6	Proposed product/solution should Protect from multiple attack vectors on different layers with frontline responders (Managed Services) available 24X7 to optimize DDOS mitigation and incident Response	Is it an option for the OEM to opt out of providing managed services for commercial viability, as it is Good to have requirement?		OEM Operations/Support team has to monitor NPCI traffic 24X7 and alert if any abnormality in Traffic . Refer to corrigendum 3
145	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 11	The System must have an updated IP reputation feed that describes suspicious traffic Blacklisted IPs, botnets, Phishing. It should be updated every minute to block and protect the network against active attackers. The System should have options for Blacklist and Whitelist IOC as per NPCI requirement. System also should restrict the IP address from specific segments like from malicious sources.	Is the expectation to deploy a network cloud firewall before the traffic undergoes scrubbing in the scrubbing center? Is it ok if cloud firewall solution does not have IP reputation feed but it still be able to identify suspicious traffic, blacklisted IPs, botnets, phishing attempts, and enforce policies defined by the OEM in accordance with NPCI requirements?		Requirement is to have an integration with IP reputation/Black list so that it can prevent access from known malicious sources
146	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 12	The proposed solution should support integration of third-party external Threat Intelligence Platform.	The solution refrains from ingesting feeds from any Threat Intelligence Platform, as ingestion is not allowed to preserve the integrity of the platform. However, threats reported by NPCI are incorporated into the platform only after a detailed analysis by the OEM's threat team. If the clause implies sharing threat intelligence with the Threat Intelligence Platform, in such instances, we share it in syslog format with the Threat Intelligence Platform.		Ask is for tool to have capability to have threat feed ingested in the system
147	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 15	The proposed solution detects and mitigate application layer DDOS attacks (Flood attacks, Protocol attacks and Volumetric attacks) instantly with zero second SLA.	The Zero Second SLA can be triggered for Flood attacks and Volumetric attacks. However, in the case of protocol-based incidents, the SLA might be extended, as there could be a requirement to inspect the packets further. We trust that our understanding is evident?		This understanding is in line with expectations

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
148	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	Could you provide the total number of NPCI Top-Level Domains (TLDs)/Zones? What is the expected capacity for DNS DDoS mitigation? Additionally, should DNS DDoS service be offered with 100% availability ?		This information will be provided once bidder is finalized, expectation is 100% availability for DNS DDOS service
149	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 20	The proposed solution should support TLS1.2 and above based traffic.	For Layer 7 protection, the solution can safeguard against flood/volumetric attacks such as HTTP GET & POST floods and HTTPS GET & POST floods. However, it is understood that NPCI does not anticipate SSL decryption to be performed by the solution. This is to avoid introducing latency and duplicating the efforts of the existing WAAP (Web Application and API Protection) solution. It's worth noting that implementing SSL decryption on the DDoS solution would require NPCI to propagate SSL keys to all scrubbing centers, which may raise compliance considerations. If NPCI consents to avoiding SSL decryption on the DDoS solution, then there is no requirement for the solution to support traffic based on TLS 1.2 and above.		Refer to Corrigendum 3
150	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	Does the clause need to be included in the contract, or would a mail communication confirming 100% availability suffice for NPCI?		Refer to Corrigendum 3
151	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 22	The proposed solution should be able to block traffic based on Geo location with periodical update on regular time automatically for lists of IPs, option should be there to block based on temporary (Hours, few hours) or permanently.	Temporary blocking can be achieved with the assistance of managed SOC services provided by the OEM. The block will be automatically removed once the criteria are met by the SOC, and no system policies will be created. We hope NPCI finds this acceptable as it aligns with the objectives of the clause.		No Change in EOI Terms
152	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	B. 3	The proposed solution must have an updated threat feed that describes new malicious traffic (botnets, phishing)	The solution is custom-designed and consistently updated for DDoS mitigation, incorporating pertinent threat feeds like TCP flood, UDP flood, and invalid traffic segments. Nevertheless, it will not incorporate feeds for Web Application threats such as botnets and phishing. Hope understanding is correct ?		Refer to Corrigendum 3
153	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	B. 7	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.	Is it anticipated that the solution team should inform NPCI of the attack, simultaneously initiate the scrubbing/mitigation process, and ensure that this dual action does not impact the response time, with no involvement required from the NPCI team in the mitigation process?		Refer to Corrigendum 3
154	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	B. 9	The proposed Solution should support Flowspec	Flowspec (Flow Specification) is a feature designed for appliances to perform traffic filtering and rate-limiting based on specific flow characteristics, such as source and destination IPv4 and IPv6 addresses, IP protocol, source and destination ports, and more. Considering NPCI's interest in an always-on DDoS cloud solution, there may be no need to concern ourselves with the parameters inspected in Flowspec. Instead, it is suggested to utilize FBM (Flow-Based Monitoring), which aids in detecting behavioral anomalies and irregularities in traffic flow. We hope that the FBM mechanism is acceptable to NPCI.		Refer to Corrigendum 3
155	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	C. 1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	What SIEM is presently in use?		Refer to Corrigendum 3

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
156	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	C. 2	DDOS solution should provide RESTAPI based integration for automation of action taken, reporting, analytics and various other purposes like SOAR, etc	Is NPCI using HTTPgrid, Postman, or any other API client? Furthermore, will NPCI work in conjunction with OEM to acquire API keys and integrate the provided OEM code into the existing API client?		Standard REST API based integration is required
157	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	D. 2	The solution must support the generation of CSV, PDF and e-mail reports. Also, should provide Web-based, live dashboards reports.	Web-based, live dashboards reports will only have logs for 30 days, hope is fine with NPCI ?		30 days log minimum should be minimum available from cloud based solution
158	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	D. 10	DDOS solution should integrate with Network performance & monitoring solution.	Can the existing network performance and monitoring solution establish a connection with the OEM-provided API ?		API based integration is fine
159	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Can you provide the total number of routers per data center, along with their make and model details?		This information will be provided once bidder is finalized
160	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Could you provide the total number of /24 subnets per data center, along with the locations of the data centers?		This information will be provided once bidder is finalized
161	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Which data centers are configured as Active/Active, and which data centers operate in an Active/Passive configuration?		This information will be provided once bidder is finalized
162	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Can you provide details on each router, including information about the respective ISPs and bandwidth specifications?		This information will be provided once bidder is finalized
163	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	9	6	Integrate the solution with On-prem NPCI's Active Directory system for authentication & other application based on rest APIs.	Kindly provide details on the specific use cases that NPCI is seeking post-integration with On-prem NPCI's Active Directory, considering the multitude of policies associated with users. Additionally, please confirm the list of applications for authentication integration, specifying those reliant on REST APIs.		OEM can connect with Azure AD
164	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	9	7	Integrate the solution with the NPCI's SMTP, BMC, SIEM/SOAR, TIP.	Please share information on which SIEM/SOAR, TIP solutions should be integrated with the proposed solution.		Integrate the solution with the NPCI's SMTP, BMC Software, SIEM/SOAR-log rhythm, TIP-cyware.
165	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	8	Bidder should update and maintain all supplied equipment to correctly reflect actual state of the setup at any point in time during the warranty period.	As NPCI is exploring a Managed DDoS Protection Service, the solution is intended to be delivered as a SAAS/PAAS, eliminating the need for any appliance delivery. NPCI exclusively seeking a cloud-based solution?		Yes, seeking for Cloud-Based solution
166	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	9	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.	Given that the solution will be offered on the cloud and the OEM will handle the complete implementation remotely, as it is their platform and they have full access, there may not be a necessity for individuals to visit onsite. Kindly grant permission for remote implementation.		Refer to Corrigendum 3
167	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	10	Bidder should support the migration of the existing DDOS solution policies and features and building new policies required by organization for the proposed solution during the implementation phase.	I kindly request you to share the specifics of the current DDoS solution, including details on the original equipment manufacturer (OEM), models, and the type of deployment in use.		Currently F5 On Prem is used as DDOS solution further details will be given once bidder is finalized
168	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	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.	As NPCI is considering a Managed DDoS Protection Service, the solution will be provided as SAAS/PAAS. Consequently, there will be no requirement for any monitoring and management software or database licenses.		Okay
169	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	16	Bidder should assign technical experienced person to NPCI for deployment of Always ON DDOS with minimum of 2+ years on experience. Resumes of the team members to be shared to NPCI as part of RFP response.	Since the solution is a platform-based cloud solution and will be wholly managed and implemented by the OEM, they will allocate resources accordingly. Consequently, we kindly request that you avoid engaging the technical personnel of bidders, as the OEM will be overseeing the process.		Implementation done by OEM or Partner must have 2+ years of experience on proposed solution/technology.
170	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	21	Bidders are expected to provide the onsite support post implementation if the technical issues are not remotely resolved.	Since there will be no on-site deployment and the solution will be provided as a SaaS/PaaS service, I kindly request you to omit the clause regarding on-site support.		Refer to Corrigendum 3

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
171	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	24	OEM should provide Technical Training to all the Operation support staff and administrators of NPCI.	Please provide information on the number of individuals from NPCI for whom the training needs to be conducted.		3 Batches of atleast 8 to 10 people for a week
172	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	10	28	The selected Bidder should follow a suitable methodology for delivering the requirements of the RFP for the entire contract period. Accordingly, the Bidder should factor for necessary effort and team deployment. The methodology should clearly layout the overall steps from initiation to closure of this engagement.	What is the duration of the contract?		3 years
173	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	32	The Bidder will have to provide all the MIS reports as per the requirements of the NPCI.	Kindly specify whether the dedicated EMS tool should be regarded as a distinct consideration.		OEM or Bidder should can provide weekly and monthly reports on mail
174	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	33	Bidder should provide soft copy and hard copies of Training material	We only provide soft copies as we do not produce any hard copies.		Ok
175	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	11	35	SupportModel: -24x7 and 365 days Service Coverage. (Email/Phone/Portal) -Technical Account Manager -Escalation Matrix -Periodic Health Checks -Monthly reports & Governance Meetings -Onsite visits as required -Proactive Invitations to Beta programs has context menu Compose Paragraph	As the solution is entirely owned and managed by the OEM, is it acceptable if onsite visits are not conducted by the bidder's technical team?		fine,Even OEM or bidder technical team presence is required .
176	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 3	OEM Infrastructure should have multiple scrubbing centers (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	Should each of the multiple scrubbing centers have a dedicated scrubbing capacity of 10 TBPS individually, or is the capacity meant to be combined?		OEM Infrastructure should have capacity to absorb High volume DDOS attack from India location scrubbing centre
177	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 5	Proposed solution should be agnostic to the Internet Service Provider (ISP) solutions and protect all Internet facing applications of NPCI	Who are your link providers, and what is the link capacity in each of the data centers?		This information will be provided to successful bidder
178	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 6	Proposed product/solution should Protect from multiple attack vectors on different layers with frontline responders (Managed Services) available 24X7 to optimize DDOS mitigation and incident Response	Is it an option for the OEM to opt out of providing managed services for commercial viability, as it is Good to have requirement?		OEM Operations/Support team has to monitor NPCI traffic 24X7 and alert if any abnormality in Traffic . Refer to corrigendum 3
179	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 11	The System must have an updated IP reputation feed that describes suspicious traffic Blacklisted IPs, botnets, Phishing. It should be updated every minute to block and protect the network against active attackers. The System should have options for Blacklist and Whitelist IOC as per NPCI requirement. System also should restrict the IP address from specific segments like from malicious sources.	Is the expectation to deploy a network cloud firewall before the traffic undergoes scrubbing in the scrubbing center? Is it ok if cloud firewall solution does not have IP reputation feed but it still be able to identify suspicious traffic, blacklisted IPs, botnets, phishing attempts, and enforce policies defined by the OEM in accordance with NPCI requirements?		Solution reputaRequirement is to have an integration with IP reputation/Black list so that it can prevent access from known malicious sourcestion has to be upto date (zero day).
180	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 12	The proposed solution should support integration of third-party external Threat Intelligence Platform.	The solution refrains from ingesting feeds from any Threat Intelligence Platform, as ingestion is not allowed to preserve the integrity of the platform. However, threats reported by NPCI are incorporated into the platform only after a detailed analysis by the OEM's threat team. If the clause implies sharing threat intelligence with the Threat Intelligence Platform, in such instances, we share it in syslog format with the Threat Intelligence Platform.		Ask is for tool to have capability to have threat feed ingested in the system
181	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	37	A. 15	The proposed solution detects and mitigate application layer DDOS attacks (Flood attacks, Protocol attacks and Volumetric attacks) instantly with zero second SLA.	The Zero Second SLA can be triggered for Flood attacks and Volumetric attacks. However, in the case of protocol-based incidents, the SLA might be extended, as there could be a requirement to inspect the packets further. We trust that our understanding is evident?		This understanding is in line with expectations

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
182	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	Could you provide the total number of NPCI Top-Level Domains (TLDs)/Zones? What is the expected capacity for DNS DDoS mitigation? Additionally, should DNS DDoS service be offered with 100% availability ?		This information will be provided once bidder is finalized, expectation is 100% availability for DNS DDOS service
183	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 20	The proposed solution should support TLS1.2 and above based traffic.	For Layer 7 protection, the solution can safeguard against flood/volumetric attacks such as HTTP GET & POST floods and HTTPS GET & POST floods. However, it is understood that NPCI does not anticipate SSL decryption to be performed by the solution. This is to avoid introducing latency and duplicating the efforts of the existing WAAP (Web Application and API Protection) solution. It's worth noting that implementing SSL decryption on the DDoS solution would require NPCI to propagate SSL keys to all scrubbing centers, which may raise compliance considerations. If NPCI consents to avoiding SSL decryption on the DDoS solution, then there is no requirement for the solution to support traffic based on TLS 1.2 and above.		Refer to Corrigendum 3
184	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	Does the clause need to be included in the contract, or would a mail communication confirming 100% availability suffice for NPCI?		Refer to Corrigendum 3
185	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	A. 22	The proposed solution should be able to block traffic based on Geo location with periodical update on regular time automatically for lists of IPs, option should be there to block based on temporary (Hours, few hours) or permanently.	Temporary blocking can be achieved with the assistance of managed SOC services provided by the OEM. The block will be automatically removed once the criteria are met by the SOC, and no system policies will be created. We hope NPCI finds this acceptable as it aligns with the objectives of the clause.		No Change in EOI Terms
186	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	B. 3	The proposed solution must have an updated threat feed that describes new malicious traffic (botnets, phishing)	The solution is custom-designed and consistently updated for DDoS mitigation, incorporating pertinent threat feeds like TCP flood, UDP flood, and invalid traffic segments. Nevertheless, it will not incorporate feeds for Web Application threats such as botnets and phishing. Hope understanding is correct ?		Refer to Corrigendum 3
187	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	38	B. 7	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.	Is it anticipated that the solution team should inform NPCI of the attack, simultaneously initiate the scrubbing/mitigation process, and ensure that this dual action does not impact the response time, with no involvement required from the NPCI team in the mitigation process?		Refer to Corrigendum 3
188	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	B. 9	The proposed Solution should support Flowspec	Flowspec (Flow Specification) is a feature designed for appliances to perform traffic filtering and rate-limiting based on specific flow characteristics, such as source and destination IPv4 and IPv6 addresses, IP protocol, source and destination ports, and more. Considering NPCI's interest in an always-on DDoS cloud solution, there may be no need to concern ourselves with the parameters inspected in Flowspec. Instead, it is suggested to utilize FBM (Flow-Based Monitoring), which aids in detecting behavioral anomalies and irregularities in traffic flow. We hope that the FBM mechanism is acceptable to NPCI.		Refer to Corrigendum 3
189	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	C. 1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	What SIEM is presently in use?		Refer to Corrigendum 3

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
190	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	C. 2	DDOS solution should provide RESTAPI based integration for automation of action taken, reporting, analytics and various other purposes like SOAR, etc	Is NPCI using HTTPgrid, Postman, or any other API client? Furthermore, will NPCI work in conjunction with OEM to acquire API keys and integrate the provided OEM code into the existing API client?		Standard REST API based integration is required
191	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	D. 2	The solution must support the generation of CSV, PDF and e-mail reports. Also, should provide Web-based, live dashboards reports.	Web-based, live dashboards reports will only have logs for 30 days, hope is fine with NPCI ?		30 days log minimum should be minimum available from cloud based solution
192	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	39	D. 10	DDOS solution should integrate with Network performance & monitoring solution.	Can the existing network performance and monitoring solution establish a connection with the OEM-provided API ?		API based integration is fine
193	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Can you provide the total number of routers per data center, along with their make and model details?		This information will be provided once bidder is finalized
194	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Could you provide the total number of /24 subnets per data center, along with the locations of the data centers?		This information will be provided once bidder is finalized
195	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Which data centers are configured as Active/Active, and which data centers operate in an Active/Passive configuration?		This information will be provided once bidder is finalized
196	EOI Reference No: NPCI/EOI/2023-24/IT/03 dated 24th January 2024	NA	NA	Fundamental Queries	Can you provide details on each router, including information about the respective ISPs and bandwidth specifications?		This information will be provided once bidder is finalized
197	B] Other than start-ups:	13	7	Bid earnest money (EMD)	We are the MSME Company and would request for the EMD submission exemption.		Exemption for EMD is not applicable as NPCI is not a Government organization. All bidders who are participating has to submit EMD amount either online transfer or in the form of Bank Guarantee
					- Apache Whitespace		No Change in EOI Terms
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		
198	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	Suggestion-100% is unrealistic and decision should be also made based on SLA granularity Hence requesting you to make changes in this point as below: 99.999% SLA in-line with SLA Asked in DDoS		Refer to Corrigendum 3

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
199	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	38	B.7	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 (with minimum guidance of Minimal time as suggested.	Suggestion-The SLA of the DDoS is critical and important and it should include uptime including Consistency of Mitigation etc. Hence requesting you to add this additional point in existing one: Consistency of Mitigation should be within 20 seconds and minimum of 95%.		Refer to Corrigendum 3 yes Solution should protect zero day attack ,Should send alert to NPCI
200	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	37	A.3	OEM Infrastructure should have multiple scrubbing centers (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	Suggestion-There should be no dependency on the Bidder & OEM provided service on an 3rd Party to have best Solution, ownership of the solution by the Bidder & OEM. Hence requesting you to change the point as below: OEM with Own Cloud Scrubbing center should be able to not only detect but also mitigate attacks.The scrubbing center shouldn't be using any public cloud offering and it should be a dedicated center owned by OEM.		OEM is required to have own scrubbing centre located in India geography
201	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	37	A.5	Proposed solution should be agnostic to the Internet Service Provider (ISP) solutions and protect all Internet facing applications of NPCI	Suggestion- If NPCI is using or might start using ISP given IPs for existing or any new location, the proposed DDoS solution should be capable to offer the protection for these IPs. Hence requesting you to add below point: Cloud DDoS Solution should have capability to protect, whenever needed, organization's IP address assets which are non DNS-addressable or using ISP IP addresses. We recommend NPCI to look for capability to protect ASN as well as ISP owned IP.		No Change in EOI Terms
202	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	39	B.13	The proposed Solution must be able to detect and block HTTP GET/POST Flood and should support mechanisms to avoid False Positives.	Suggestion-The solution should be capable to not only protect HTTP but also HTTPS flood given most of traffic in use now days is encrypted. Hence requesting you to kindly change the point as below: The proposed Solution must be able to detect and block HTTP/S GET/POST Flood and should support mechanisms to avoid False Positives.		Refer to Corrigendum 3
203	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	Query-Integration with RADIUS & TACACS is done for on-premise solution. This is not necessary for cloud based solution. Kindly elaborate if any specific use case		Refer to Corrigendum 3
204	Managed DDoS Protection Service NPCI/EOI/2023-24/IT/03	39	C.4	Solution should support MFA capabilities including FIDO2/Web Authentication, OATH (TOTP/HOTP) for access management.	Query-SAML is commonly used for integration and achieve MFA capabilities. Hence requesting you to add SAML too.		Refer to Corrigendum 3
205	4.2 Eligibility Criteria for Bidders	12	2	The bidder should have reported minimum annual turnover of Rs. 20 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (2020-21, 2021-22 and 2022-23).	Request you to change the clause for NON MSME bidder as well The bidder should have reported minimum annual turnover of Rs. 8 crores and should have reported profits (profit after tax) as per audited financial statements in at least **2 out of last 3 financial years** (2020-21, 2021-22 and 2022-23).		No Change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
206	Additional Points	-	-	-	Suggestion- Behavioral analysis is needed to protect against application DDoS and misuse attacks. Those attacks are harder to detect and appear like legitimate traffic so they can go unnoticed without a behavioral analysis tool. Hence requesting you to add below point: System should provide zero-day attack protection based on learning baseline / behavioural analysis of normal traffic, zero-day attacks are identified by deviation from normal behaviour by employing advanced echnique of generating signatures in real time within 19 seconds.		No Change in EOI Terms
207	Additional Points	-	-	-	Suggestion-Soluton should be able to detect and protect organization have protection against high-volume SSL-based attacksand it should be able to inspect traffic without SSl certificates. Hence requesting you to add below point: Solution should be able to detect and protect against SSL-based attacks without any need from customer to provide original SSL certificates and the solution should not add latency in peacetime and attack time for decrypting the HTTPs traffic for inspection.		No Change in EOI Terms
208	Additional Points	-	-	-	Suggestion- DDoS scrubbing centers should ensure date protection, availability and integrity by providing relevant compliances		No Change in EOI Terms
					Hence requesting you to add below point: Cloud DDoS Scrubbing Center should have following Quality & Security Standards:		Not required
					ISO 27032:2012		
					ISO 27002:2013		
					ISO 27017:2015		
209	Additional Points	-	-	-	Suggestion-There should be option available to have different deployment mode including Hybrid for future purpose from same OEM. Hence requesting you to add below point: The proposed cloud solution should support hybrid deployment mode from same OEM		No Change in EOI Terms
210	Additional Points	-	-	-	Sugestion-It is recommended that the OEM should consist of multiple option for future consideration. Given if all GRE links capacity is exhausted, GRE load balancing becomes very much necessary. Hence requesting you to add below point: Solution should support GRE Load-Balancing with no restriction on GRE Capacity.		No Change in EOI Terms
211	Scope of work	-	-	-	Please specify the model and version of Active Directory to check the compatibility between your AD and the proposed solution		azure ad connect (windows 2016 on premise)
212	Scope of work	-	-	-	Please specify the OEM, model and version of SMTP, BMC, SIEM/SOAR, TIP to check the compatibility between your AD and the proposed solution		Integrate the solution with the NPCI's SMTP, BMC Software, SIEM/SOAR-log rhythm, TIP-cyware.
213	Scope of work	-	-	-	Instead of OEM, can the bidder provide post-implementation technical support? Also, bidders have support centers based in India		Yes, bidders can also provide support post implementation
214	Scope of work	10	15	Implementation of the solution and migration of policies from existing solution to be done by Bidder/OEM directly.	Please help us with the details of the existing solution used by NPCI		Currently F5 On Prem is used as DDOS solution further details will be given once bidder is finalized
215	ANNEXURE M - Technical Specifications -> A - Fundamental Requirements	37	A.12	The proposed solution should support integration of third-party external Threat Intelligence Platform.	Please help us with the details of the existing Threat Intelligence Platform solution used by NPCI		Details will be shared with successful bidder
216	ANNEXURE M - Technical Specifications -> A - Fundamental Requirements	38	A.18	The proposed solution must not have any limitations in handling the number of concurrent sessions for DDoS attack traffic.	Please specify how many concurrent sessions are looking for. Based on that we can proposed a right solution for NPCI		The limitation should only be on the amount of clean traffic expected by NPCI.

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
217	ANNEXURE M - Technical Specifications -> B – Security / DDoS Feature	38	B.1	The proposed solution must be able to block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped. Solution should also support packet Anomaly Protection.	What do you mean by invalid packets, can you please elaborate more on this?		Traffic that does not conform to standard RFC rules
218	ANNEXURE M - Technical Specifications -> C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Please help us with the details of the existing SIEM solution used by NPCI		Refer to Corrigendum 3
219	ANNEXURE M - Technical Specifications -> C – Integration Capabilities		C.3	DDOS solution should Integration with TACACS+ and RADIUS	Please specify the model and version of the TACACS+ and RADIUS server used by the NPCI to check the compatibility between your server and the proposed solution		Refer to Corrigendum 3
220	ANNEXURE M - Technical Specifications ->D-Monitoring & Dashboard	39	D.10	DDOS solution should integrate with Network performance & monitoring solution.	Please help us with the details of the existing Network performance & monitoring solution used by NPCI		API based integration is fine
221	A - Fundamental Requirements	37	A.7	Solution should support to pass traffic on various layer 7 and layer 4 protocols like HTTP, HTTPS, DNS, GRPC, GRE traffic etc.	We request NPCI to clarify if they are also looking for DNS primary/secondary solutions with DNS security from the DDOS bidder.		Refer to Corrigendum 3
222	Additional clarification required	-	-	-	NPCI should also ask for PoP outside India supporting Anycast, this will enable in case of disaster scenarios. The SAAS Solution should be running out of over 20+ PoP with all PoPs running in ANYCAST in order to ensure Global Availability		No Change in EOI Terms
223	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 EOI Terms
224	A - Fundamental Requirements	37	A.7	The Proposed solution must not modify MAC or IP addresses of passed frames.	We request NPCI to clarify if this is relevant for cloud based SAAS service. This techical point is usually applicable to on-prem layer 2 deployments of hardware devices for DDOS		Refer to Corrigendum 3
225	A - Fundamental Requirements	38	A.16	The proposed solution should provide protection from DNS queries-based attacks and protect the name servers of organization	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a SaaS service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
226	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 EOI Terms
227	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 EOI Terms
228	Additional clarification required	-	-	-	Does NPCI want SAAS Platform to support unlimited data transfer		No Change in EOI Terms
229	A - Fundamental Requirements	38	A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	We request NPCI to revise this point and change it to 99.99% of higher as it is dependent on external factors as well.		Refer to Corrigendum 3
230	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 EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
231	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to support behavioral based malicius user detction for low and slow attacks and potential misbahaviour. The platform should have option to define client IP or query parameter or header name or cookie or TLS finger print as unique identifier to define individual endpoint.		No Change in EOI Terms
232	B – Security / DDoS Feature	38	B.8	The proposed Solution should support DNS query source validation, DNS Query, per-Source Flooding.	We request NPCI to clarify where the Namesservers are hosted currently, if NPCI is already using a saas service for NS records will it allow for the change in delegation.		Details will be shared with successful bidder
233	B – Security / DDoS Feature	39	B.9	The proposed Solution should support Flowspec.	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
234	Additional clarification required	-	-	-	Does NPCI want SaaS platform to be able to consume Openapi spec/Swagger V2 and V3 file for API endpoint confg and should support positive security configuration for published apis.		No Change in EOI Terms
235	Additional clarification required	-	-	-	Does NPCI need System should report Malicous user dashboard		No Change in EOI Terms
236	C – Integration Capabilities	39	C.1	DDOS solution should integrate with existing SIEM engine seamlessly through syslog	Being a SaaS platform, many intergrations are based on API which is a standard across multiple OEM's. So we request NPCI to modify this point as follows. "DDOS solution should integrate with existing SIEM engine seamlessly through syslog or API "		Refer to Corrigendum 3
237	Additional clarification required	-	-	-	Does NPCI want proposed SaaS platform to have ability to define Circuit Breaker configuration - this should provide mechnism for watching failures in upstream connections or requests and if the failures reach a certain threashold , automatically fail subsequent requests which allows to apply back pressure on downstream quickly		No Change in EOI Terms
238	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 EOI Terms
239	Additional clarification required	-	-	-	Does NPCI looking forward to have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.		No Change in EOI Terms
240	C – Integration Capabilities	39	C.3	DDOS solution should Integration with TACACS+ and RADIUS	We request NPCI to clarify if the requirment is pure SAAS based DDOS offering or a hybrid approch where the bidder can combine on-prem + Cloud based scrubbing. This technical clause is more applicable towards on-prem devices		Refer to Corrigendum 3
241	Additional clarification required	-	-	-	Does NPCI need Proposed SaaS Solution to provide Organization capability to restrict usages of specific PoPs only by Bring your own IP services (/24 Pool)		No Change in EOI Terms
242	Additional clarification required	-	-	-	Does NPCI need OEM PoP services only which will have better SLA and not any Public Cloud to avoid dependency of cloud providers SLA		No Change in EOI Terms
243	Eligibility Criteria	11	4	The bidder should have successfully implemented a minimum of one (1) innovative idea and should provide client reference for the same	Do you mean the bidder should have reference for similar setup or just experience of managing DDoS solution		Similar setup is more advantage
244	Query	-	-	-	Kindly confirm how many L 7 apps/Subdomains are to be factored for layer 7 protection		No Change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
245	Additional points to consider	-	-	-	SaaS must support following Violation Detections		No Change in EOI Terms
					- Apache Whitespace		
					- Bad HTTP Version		
					- Bad HTTP Header Value		
					- Bad Multipart parameter Parsing		
					- CRLF Character before request start		
					- Content Length should be positive number		
					- Directory Traversal		
					- Disallowed file upload content detected		
					- Disallowed file upload content in body detected		
					- Illegal File types		
					- Illegal Method		
					- Malformed JSON data		
					- Malformed XML data		
					- Malformed Request		
					- Mandatory HTTP header missing		
					- Modified Cookie		
					- Multiple HOST header		
					- Multiple Decoding		
					- No HTTP host headerin HTTP1.1 Request		
					- Null in request		
					- Request length exceed defined buffer size		
					- Unparsable Request content		
					- Several Content Length Headers		
246	Additional clarification required	-	-	-	Does NPCI want the proposed platform to also provide protection based on a variety of threat intel sourced from the real world campaigns to attack and/or take over resources. The Threat Campaign protection should be based on current “in-the-wild” attacks. These signatures contain contextual information about the nature and purpose of the attack.		No Change in EOI Terms
247	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 EOI Terms
248	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point: A.21	The committed uptime of the proposed solution should be 100% availability on yearly basis at each site.	Suggestion: 100% is more of a Marketing Gimick and having detailed & granular SLA with realistic figures is Suggested to have Best Players Participate. Hence requesting you to make changes in this point as below: 99.999% SLA in-line with SLA Asked in DDoS		uptime has to be 100% availability

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
249	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point: B.7	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 (with minimum guidance of Minimal time as suggested.	Suggestion: The SLA of the DDoS is critical and commited and it should include not just uptime but also Time to Mitigate to have Robust service for NPCI. Hence requesting you to add below point: Time to Mitigate (TTM) for any kind of attack should not be more than 30 Seconds		Refer to Corrigendum 3
							yes Solution should protect zero day attack ,Should send alert to NPCI
250	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	37	Point A.5	Proposed solution should be agnostic to the Internet Service Provider (ISP) solutions and protect all Internet facing applications of NPCI	Query: Please confirm that NPCI has their own ASN to offer ISP agnostic IP? Also requesting you to please specify number of IP subnets?		This information will be provided once bidder is finalized
251	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point A.17	The proposed DDoS solution should not reach End of Support within 5 years from the date of submission of bid. If this happens, the bidder is bound to provide the then prevalent higher model at no additional cost to NPCI.	Query: For NPCI, the solution requested is always-on cloud DDoS. However the point of providing higher model doesn't seem relevant. Hence requesting you to remove this point		Ask is current version shouldn't reach EOS within next 5 years
252	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point A.23	The proposed solution should support mitigation of Burst Attacks, the specific mitigation strategies the solution employs, such as traffic filtering, rate limiting, and IP blocking.	Suggestion: DDoS solution should be capable enough to mitigate advanced attacks accurately without need of any manual intervention to provide best of protection solution for NPCI Hence requesting you to change the point as below: The proposed solution should support capabilities to mitigate any kind of attack which is not limited to traffic filtering, rate limiting, IP blocking, real-time signature generation but also have advanced machine learning engine which can work on its own real-time threat detection and mitigation ability		Our ask is to mitigate all types of attacks automatically
253	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	39	Point B.11	The proposed Solution should support for all protocols at layer 3.	Suggestion: Covering all layers will ensure full protection including encrypted attacks Hence requesting you to change the point as below: The proposed Solution should support all protocols at L3/4/7 including TLS/SSL, DNS, RPS etc.		Refer to Corrigendum 3
254	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point B.9	The proposed Solution should support Flowspec.	Query: Flowspec is mainly used whenever on-premise solution is considered. Here, since the consideration is for cloud based solution, kindly elaborate need for Flowspec		SaaS with always on
255	INVITATION FOR EXPRESSION OF INTEREST (EOI) – MANAGED DDOS PROTECTION SERVICE	38	Point A.12	The proposed solution should support integration of third-party external Threat Intelligence Platform.	Query: OEMs have their own threat intelligence tool. Please elaborate what is NPCI expectation for integration of 3rd party Threat Intelligence platform		our ask is to feed/ingest data/IOC received from NPCI TIP to solution

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
256	Suggestions	-	-	-	Suggestion: Behavioral analysis is needed to protect against application DDoS and misuse attacks. Those attacks are harder to detect and appear like legitimate traffic so they can go unnoticed without a behavioral analysis tool. Hence requesting you to add below point: The proposed DDoS Solution must have Positive Security Model supporting advanced behavior-analysis technologies to separate malicious threats from legitimate traffic with advanced capability to generate real-time signatures within 20 seconds to combat zero-day attacks.		zero day attack 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.
257	Suggestions	-	-	-	Suggestion: DDoS solution should be capable to protect organization from high-volume, encrypted or very short duration threats including emerging network multi-vector attacks, phantom floods and other types of cyberattacks. Hence requesting you to add below point: System should support for below methodology for handling SSL or encrypted traffic: ▪ Ability to detect SSL flood attacks without need to use any SSL Certificate and rate-limit suspected source ▪ Ability to challenge only first request of suspected SSL attack source as well as all Sources and bypass authenticated or legit sources from DDoS solution to limit latency on SSL traffic for legit users ▪ Ability to inpsect with vulnerability for only suspected DDoS attack traffic with SSL decryptor ▪ Ability to conduct full SSL inspection for all sources for complete traffic inspection		The proposed Solution should support for all protocols at layer 3 to layer 7
258	Suggestions			-	Suggestion: DDoS scrubbing centres owned by OEM should follow various compliances and certifications for organization like NPCI, standards like PCI DSS ensures security of payment card information and SOC-2 Type II ensures availability, integrity, confidentiality and privacy Hence requesting you to please add below point: Security Related standards for OEM owned DDoS Scrubbing Center Service Datacenter PCI-DSS v3.2 US SSAE16 SOC-2 Type II		Not required
259	EOI Schedule	8	12	Bid cost of 11800	As this is EOI could the Bid fee be exempted as we would again have to pay the bid fee when the RFP is released. OR Make it refundable		Exemption for Bid cost is not applicable as NPCI is not Government Organization. All bidders who are participating in EOI has to submit BID cost
260	EOI Schedule	8	13	EMD of 500000	As this is EOI could the EMD be exempted as we would again have to pay the EMD while bidding the RFP.		Exemption for EMD is not applicable as NPCI is not a Government organization. All bidders who are participating has to submit EMD amount either online transfer or in the form of Bank Guarantee
261	Eligibility Criteria (Other than Start-ups)	32	8	Self declaration to be provided along with customer references	This clause is applicable to the OEM or Bidder - Please clarify		MAF to be provided by OEM as per Annexure I
262	Technical Specification - Annexure M	36	A.3	OEM Infrastructure should have multiple scrubbing centers (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	Even if the only Meta Data is sent outside India geo. Is it not permissable. No data is sent outside, only Meta Data		No, data should be sent outside to INDIA geography

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
263	ANNEXURE M - Technical Specifications	38	Point: B.7	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 (with minimum guidance of Minimal time as suggested.	Suggestion: The SLA of the DDoS is critical and important and it should include not just uptime but also, Time to Detect, Time to Mitigate, Consistency of Mitigation, Notification etc. to have Robust service for NPCI.		Zero delay
					Hence requesting you to add below point: • Time to Alerts: 2 Minutes via SMS/E-mail Notification, 15 Minutes via Phone Call Notification		Refer to Corrigendum 3
					• Time to Mitigate: 20 Seconds		Time to mitigate should be minimal
					• Consistency of Mitigation: Minimum 95%.		Not required
					• DDoS Protection service Uptime: 99.999%.		Uptime can be 99.99999
264	ANNEXURE M - Technical Specifications	37	Point A.3	OEM Infrastructure should have multiple scrubbing centers (local to INDIA geography) to absorb HIGH DDOS attack and decrease the latency.	**Suggestion:** There should be no dependency on the Bidder & OEM provided service on any 3rd Party to have best Solution, ownership of the solution by the Bidder & OEM. **Hence requesting you to add below point:** OEM should have Own Cloud Scrubbing Capability that can be used for detection, mitigation and reporting all should be provided by OEM directly and not from the 3rd party. Also, the Scrubbing should be dedicated facility & not using any Public Cloud offering / Infrastructure.		need clarity from partner
265	ANNEXURE M - Technical Specifications	37	Point A.5	Proposed solution should be agnostic to the Internet Service Provider (ISP) solutions and protect all Internet facing applications of NPCI	**Suggestion:** This is important as NPCI today might be using own ASN but if in future uses ISP provided IP's for any / future location the solution should have capability to offer DDoS protection for the same. **Hence requesting you to add below point:** Cloud DDoS Solution should have capability to offer protection if required in future which will help organization to protect IP addresses assets that are not DNS-addressable or using ISP IP's and not NPCI ASN. This should be agnostic to any ISP NPCI use today or in future.		This information will be provided once bidder is finalized
266	ANNEXURE M - Technical Specifications	39	Point D.1	Proposed solution should have centralized management system that helps to manage, monitor, and maintain all, DDoS setup.	**Suggestion:** It is important to list minimum requirement for the solution so that they offer minimum listed capability and not just the High level to Comply. **Hence requesting you to add below point:** Proposed solution should have centralized management system that helps to manage, monitor, and maintain all, DDoS setup and at least to have:		No Change in EOI Terms
					• Asset Management and Site provisioning		Asset has to be completely managed by OEM
					• User Management – including roles		Solution can integrate with Azure AD through API
					• Traffic statistics – Attack vs. clean traffic		No Change in EOI Terms
					• Attack alerts and information – Including attack vector, source, target, bandwidth, and so on.		No Change in EOI Terms
					• Attack distribution – By source/destination/vector		No Change in EOI Terms
					• Attack status – Under attack/peacetime/diverted/cool-down		No Change in EOI Terms
					• Peace-Time Analytics of Network, Traffic, Geo-Traffic distribution, attack, Top-Source, Top Destination etc. for better Visibility & Analytics.		No Change in EOI Terms

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
267	ANNEXURE M - Technical Specifications	38	Point A.18	The proposed solution must not have any limitations in handling the number of concurrent sessions for DDoS attack traffic.	**Suggestion:** It is important and recommended to have mitigation Closer to source of the attack rather than target during an high volume attack campaign. **Hence requesting you to add below point:** The proposed solution must not have any limitations in handling the number of concurrent sessions, PPS, Attack volume for DDoS attack traffic and should have Global "Anycast" capability to use Global Mitigation Capacity of 10+ Tbps.		Solution should protect and handles all
268	ANNEXURE M - Technical Specifications	38	Point A.23	The proposed solution should support mitigation of Burst Attacks, the specific mitigation strategies the solution employs, such as traffic filtering, rate limiting, and IP blocking.	**Suggestion:** To have efficient & DDoS mitigation with efficicay & accuracy the system should be advanced enough to have no dependency on Manual Intervention, analysis of PCAPS etc. for best protection for NPCI. **Hence requesting you to add below point:** The proposed solution should support mitigation of Burst Attacks, the specific mitigation strategies the solution employs, such as traffic filtering, rate limiting, IP blocking and real time Signature capability and no dependency on Manual Intervention.		No Change in EOI Terms
269	ANNEXURE M - Technical Specifications	39	Point B.11	The proposed Solution should support for all protocols at layer 3.	**Suggestion:** It is important to cover layer 3, layer4 and layer 7 to ensure better protection. **Hence requesting you to add below point:** The proposed Solution should support for all protocols at layer 3, 4 & 7 including TLS/SSL, DNS, RPS etc.		Refer to Corrigendum 3
270	ANNEXURE M - Technical Specifications	39	Point B.13	The proposed Solution must be able to detect and block HTTP GET/POST Flood and should support mechanisms to avoid False Positives.	**Suggestion:** Given most of the traffic now days is secured, it is important to detect and block not only HTTP but also HTTPS flood attacks. **Hence requesting you to add belowpoint:** The proposed Solution must be able to detect and block HTTP/S GET/POST Flood and should support mechanisms to avoid False Positives.		Refer to Corrigendum 3
271	ANNEXURE M - Technical Specifications	38	Point A.17	The proposed DDoS solution should not reach End of Support within 5 years from the date of submission of bid. If this happens, the bidder is bound to provide the then prevalent higher model at no additional cost to NPCI.	**Query:** As per RFP ask it is understood that NPCI is looking for Cloud Based Always-On Solution and not On-prem. So the Question of Higher Model point is irrelevent. Please clarify & Elaborate.		Ask is current version shouldn't reach EOS within next 5 years
272	Recommendation			-	**Suggestion:** Should have protection against SSL-based attacks without requiring customers to provide original SSL certificates and solution should not add latency in peacetime & attack time for decrypting the HTTPs traffic for inspection **Hence requesting you to add below points:** Should have protection against SSL-based attacks without requiring customers to provide original SSL certificates and solution should not add latency in peacetime for decrypting the HTTPs traffic for inspection		As we are remove L7 this point is irrelevant

Sr. No.	Document reference	Page No	Clause No	Description in EOI	Clarification Sought	Additional Remarks (if any)	Response
273	Recommendation			-	**Suggestion:** This is crtitical to have a robust Integration and best mitigation required in Future. The Cloud Vendor should atleast have this option for future available. **Hence requesting you to add below point:** The proposed cloud solution should be able to integrate with on premise DDoS solution in future if required and it should be from same OEM		NA
274	Recommendation		-	-	**Suggestion:** This is important that the vendor should have multiple option as may be required in future. Also for a sceanerio when all links / subnets are under attack and capacity of GRE required to be distributed across links the GRE Load balancing is critical & important. **Hence requesting you to kindly add below point:** The Services must offer multiple ways to route clean traffic towards data center (On-premises/Cloud) which includes via cross-connection, GRE tunnel, Direct connect, VRF based. Also, solution should support GRE Load-Balancing with no restriction on GRE Capacity.		No change in EOI Terms
275	Recommendation		-	-	**Suggestion:** It is important to make these consideration and have Best Environment of Critical Infra / Traffic of NPCI where it is processed. Also maintaining such certifications calls for rigorous adherence of Processes and Investments and the solution which is serving NPCI should have minimum level of Benchmarks. **Hence requesting you to add below point:** Cloud DDoS Scrubbing Center should have following Quality & Security Standards:		As we already mentioned Scrubbing center has be in INDIA and compliance of all BFSI standards.
					a. PCI DSS v3.2 (Payment Card Industry Data Security Standard)		Not required
					b. ISO 27002:2013 (Information Security Management Systems)		
					c. ISO 27017:2015 (Information Security for Cloud Services)		
					d. US SSAE16 SOC-2 Type II		
					e. ISO 27032:2012 (Security Techniques — Guidelines for Cybersecurity)		
					f. ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain)		