



Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

Response to Pre Bid Queries: Request for Proposal (RFP) for Procurement and Management of Cyber Security Component

SI No.	RFP Page No	RFP Clause No	RFP Clause	Existing Clause in RFP		Revised Clause in RFP	
				Criteria/ Clause	Marks	Criteria/ Clause	Marks
1.	Corrigendum I page 90	Annexure XI(B)	Scoring Methodology	Bidder's experience of Designing of Information Security architecture/ System integration of IT Security solution/ Information security components/SOC in India in Scheduled Commercial Banks in India with minimum 2 Lakh crore business (as on FY 2021-22 / FY 2020-21) (For three years of experience 3 marks will be awarded. 1 mark will be awarded for every additional year of experience)	5 (Max)	Bidder's experience of Designing of Information Security architecture/ System integration of IT Security solution/ Information security components/SOC in India in RBI or Scheduled Commercial Banks in India with minimum 1.4 Lakh crore business (as on FY 2021-22 / FY 2020-21) within the last 5 years. (For three years of experience 3 marks will be awarded. 1 mark will be awarded for every additional year of experience)	5 (Max)
2.	Corrigendum I page 38	Annexure XI(A) SL No.37	TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	8X 10G ports (SFP + Fiber port), 4x 40G (QSFP + Fiber port) ports 2 x 1G RJ45 Management Port. Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achieved through software by pass at interface level	1 (Max) (Mandatory)	Appliance should have sufficient port to cater current and future requirements. however bidder to factor minimum ports as given below : 8X10G ports (SR/LR Fiber) or (SFP + Fiber port) and 2X40G (SR/LR Fiber) or (QSFP + Fiber port) bypass ports And 2 x 1G RJ45 Management Port. Fail to wire switch along with proposed device with minimum 4 bypass segment/ or can be achieved through additional external switch populated with same interfaces capacity to achieve fail over or Achieved through software/hardware by pass at interface level	1 (Max) (Mandatory)

3.	Corrigendum I page 33	Annexure XI(A) SI No. 40	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Bidder has to provide threat intel solution from the OEMs of proposed systems for internal device consumption, in addition to the same bidder has to provide third party dedicated Threat Intelligence Feed from reputed OEMs. Third party Threat Intelligence Feed should able to provide analysis report/network graph analysis relation report based on historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity, actors involved in the past incidences around the world), exploits run from the detected IPs, provide extensive context and malware analysis in addition to the threat indicators and any other valuable information. Search option should be available for minimum 5 analysts . Bidder has to factor necessary hardware/software/database etc for hosting above system in DC and DR if required. External threat intelligence system should be from renowned OEMs.	5 Analysts- 2 Marks 6-7 Analysts-3 Marks More than 7 Analysts- 5 Marks	Bidder has to provide threat intel solution from the OEMs of proposed systems for internal device consumption	2 (Max) (Mandatory)
4.	Addition of new clause	Annexure XI(A) SI No. 40.1	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Addition of new clause		Bidder has to provide third party dedicated Threat Intelligence Feed from reputed OEMs. Third party Threat Intelligence Feed should able to provide analysis report/network graph analysis relation report based on historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity, actors involved in the past incidences around the world), exploits run from the detected IPs, provide extensive context and malware analysis in addition to the threat indicators and any other valuable information. Search option should be available for minimum 5 analysts. Bidder has to factor necessary hardware/software/database etc for hosting above system in DC and DR if required. External threat intelligence system should be from renowned OEMs. Separate line item for the same	5 Analysts- 3 Marks 6- 7Analysts- 6 Marks More than 7 Analysts- 10 Marks (Mandatory)

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

						has been defined in the Commercial.	
5.	Corrigendum I page 33	Annexure XI(A) , SL No. 41	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and should support third party threat feeds in industry standard STIX & TAXII format.	1 (Max) (Mandatory)	The DDOS Appliance should support inbuilt Threat intelligence Gateway (TIG) feature for outbound threat blocking and if feasible should support third party threat feeds in industry standard STIX & TAXII format.	1 (Max) (Mandatory)
6.	Corrigendum I page 38	Annexure XI(A) , SL No. 42	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections.	1 (Max) (Mandatory)	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections OR Proposed DDoS product/solution should be stateless in nature	1 (Max) (Mandatory)
7.	Corrigendum I page 37	Annexure XI(A) , SL No. 44	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Inspection and Mitigation: 40 Gbps (without additional hardware) Layer 4: 40 Gbps with 100 Million Hardware sync DDoS Flood Attack Prevention Rate: 35 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet). DDoS Cloud Mitigation: 20 Gbps	1 (Max) (Mandatory)	Inspection and Mitigation: 40 Gbps (without additional hardware) Attack Prevention Rate: 39 Mpps without hardware change (This performance figure must be mentioned in public facing datasheet) DDoS Cloud Mitigation: 20 Gbps	1 (Max) (Mandatory)
8.	Corrigendum I page 39	Annexure XI(A) , SL No. 48	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	a) Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 3Million IOC's for inline blocking (URL, domain and IP address subnet) b) The solution has Inbuilt mechanism to inspect traffic with external threat intelligence feed and shall support at least 3Million hash for inline blocking	Both a & b - 5 Marks (Max) Only a - 2 Marks	Inbuilt mechanism to inspect traffic with external threat feed and shall support at least 1 Million IOC's for inline blocking (URL, domain and IP address subnet)	2 (Max) (Mandatory)
9.	Corrigendum I page 39	Annexure XI(A), SL No. 51	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	1 (Max) (Mandatory)	OPTIONAL: Support integration of external Threat Intelligence Platform (TIP) and Support Threat Intelligence Feed	Yes-5 (Max) No-0 Marks (Weightage)
10.	Corrigendum I page 39	Annexure XI(A), SL No. 62	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time	Supports CAPTCHA- 5 Marks (Max)	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time through inbuilt Captcha	Supports CAPTCHA- 5 Marks (Max)

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

			NS OF THE SOLUTION	through inbuilt Captcha Mechanism or HTTP Authentication	Supports HTTP – 2 Marks	Mechanism or HTTP Authentication/Equivalent	Supports HTTP or Equivalent – 2 Marks
11.	Corrigendum I page 40	Annexure XI(A), SL No. 71	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Inspect SSL traffic for both RSA and ECC base key. Device should have support minimum 100,000 SSL TPS without session reuse for ECC & 2048 key RSA from day one and scalable up to 200,000 SSL TPS without hardware change	1 (Max) (Mandatory)	Clause stands deleted	
12.	Corrigendum I page 57	Annexure XI(A), SI No. 272	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Form Factor 1RU (Preferably)	1 (Max) (Mandatory)	Form Factor 1RU/2RU(Preferebly)	1RU/2RU – 1 Marks (Max) Others -0 Mark (Weightage)
13.	Corrigendum I page 57	Annexure XI(A), SI No. 276	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Always on management & LED to initial configuration.	1 (Max) (Mandatory)	Always ON management to initial configuration	1 (Max) (Mandatory)
14.	Corrigendum I page 59	Annexure XI(A) , SL No. 304	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Power on demand: Dual AC/DC supply with hot swappable units, with always on management & LED to initial configuration	1 (Max) (Mandatory)	Power on demand: Dual AC/DC supply with hot swappable units, with always on management to initial configuration	1 (Max) (Mandatory)
15.	Corrigendum I page 60	Annexure XI(A) , SL No.321	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Form Factor: 1RU (Preferably) 1(Max)	1 (Max) (Mandatory)	Form Factor: 1RU/2RU (Preferably)	1RU/2RU (Preferably) - 2 (Max) Others-0 Mark (Max) (Weightage)

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

16.	Corrigendum I page 65	Annexure XI(A) , SL No.377	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link.	Yes- 5 Mark(Max) No- 0 Mark (Weightage)	The solution should provide online troubleshooting and traffic analysis tool where customer can take snapshot of appliance configuration and upload it on OEM's web based diagnostic tool to check the health and vulnerability of appliance with recommended solution provided on knowledge base link OR The solution should provide troubleshooting and traffic analysis tool. Proposed OEM should have dedicated online portal for knowledge and learning	Yes- 5 Mark(Max) No- 0 Mark (Weightage)
17.	Corrigendum I page 77	Annexure XI(A), SL No.518	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The ADC shall be manageable by SSH , HTTP , HTTPS, API, Console	1 (Max) (Mandatory)	The ADC shall be manageable by SSH , HTTPS, API, Console	1 (Max) (Mandatory)
18.	Corrigendum I page 77	Annexure XI(A) , SL No.523	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication. Device should have inbuilt SSL VPN capability.	1 (Max) (Mandatory)	The solution must support Reverse proxy or full proxy (Forward Proxy & Reverse Proxy) architecture for HTTP1.1 & HTTP/2 based application traffic. Support IPv6 for Reverse Proxy deployments, IPv4 to IPv6 and IPv6 to IPv4 Dual Stack communication.	2 (Max) (Mandatory)
19.	Corrigendum I page 36	Annexure XI(A) , SL No.19	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	24/48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	1 (Max) (Mandatory)	48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	1 (Max) (Mandatory)
20.	Corrigendum I page 43	Annexure XI(A) , SL No. 116(e)	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Advanced DoS detection with "self-learning" for more accurate and fewer false positives	1 (Max) (Mandatory)	Clause stands deleted	
21.	Corrigendum I page 73	Annexure XI(A) , SL No. 466	Annexure XI(A) TECHNICAL AND	Store minimum 15(Fifteen) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum	1 (Max) (Mandatory)	Store minimum 7(seven) days full Raw packets and 90(ninety) Days of indexed Meta data, having usable disk capacity of minimum 300 TB for raw packets &	2 (Max) (Mandatory)

			FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	300 TB for raw packets & 100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement		100 TB for indexed metadata separately, after RAID configurations respectively having minimum 4 Ports (2 X 1Gbps Copper and 2X10 Gbps Fiber) on capture appliance. Bidder may factor additional storage as per the requirement. Bidder also ensure to replay the data of 7(seven) days in seamless manner.	
22.	Corrigendum I page 45	Annexure XI(A) , SL No. 147	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Storage: Minimum 400 GB SSD for system and 2 TB SSD for Logging capability	Storage Capacity 200% or more than proposed minimum – 3 Marks(Max) Else 1 Mark (Mandatory)	Storage: Minimum 2 TB SSD for Logging capability	Storage Capacity 200% or more than proposed minimum – 5 Marks(Max) Else 2 Marks (Mandatory)
23.	Corrigendum I page 46	Annexure XI(A) , SL No. 152	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Ports: 12X10 Gig SFP/SFP+ ports with respective SR transceivers & 2 x 40G/100G QSFP28 ports with respective transceivers Console Management USB Port 4 X 1/10 Gig Ethernet	2X100G - 5 Marks(Max) 2X40G - 2 Marks (Mandatory)	Ports: 12X10 Gig SFP/SFP+ ports with respective SR transceivers & 2 x 40G/100G QSFP28 ports with respective transceivers Console Management USB Port 2 X 1 Gig Ethernet	2X100G - 5 Marks(Max) 2X40G-2 Marks (Mandatory)
24.	Corrigendum I page 46	Annexure XI(A) , SL No. 156	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Form factor: Within 5U(Preferably) in standard 42U Rack	5U or less -2 Marks (Max) Others-0 Mark (Weightage)	Clause stands deleted	
25.	Corrigendum I page 47	Annexure XI(A) , SL No. 164	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Dashboard view and reporting of CPU usage (including real-time graph) for management activities and data plane CPU for other activities.	1 (Max) (Mandatory)	Dashboard view and real-time graph of CPU, Memory, Session usage activity. Dashboard should have the option to view the CPU and memory usages for management activities for other activities.	1 (Max) (Mandatory)

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

26.	Corrigendum I page 48	Annexure XI(A) , SL No. 165	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Mandatory: Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID, AVC , NGIPS, Anti-Virus, Anti-Malware, Anti-Spyware and logging enabled should be 30 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA.. Optional : The device may also have support for zero day attack prevention and file blocking security threat prevention features	Supports Optional Feature along with mandatory features - 5 Marks(Max) Supports only mandatory feature – 2 Marks	Mandatory: Minimum NG Threat prevention throughput in real world/production/Application Mix environment (by enabling and measured with Application-ID/AVC , NGIPS, Anti-Virus, Anti-Malware, Anti-Spyware and logging enabled should be 30 Gbps. The bidder shall submit the performance test report reference from public documents or from Global Product Engineering department / Global Testing Department/ Global POC team of OEM certifying the mentioned performance and signed by person with PoA. Optional : The device may also have support for zero day attack prevention and file blocking security threat prevention features	Supports Optional Feature along with mandatory features - 5 Marks(Max) Supports only mandatory feature – 2 Marks
27.	Corrigendum I page 48	Annexure XI(A) , SL No. 166	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Support for both Client as well client less VPN. Must support Split tunnelling based on destination domain, client process, and video streaming application . Solution must support App for endpoints running Windows, Linux and macOS and also should support Mobile app for endpoints running iOS, Android, Chrome OS , and Windows 10.	1 (Max) (Mandatory)	a) Support for both Client as well client less VPN. Must support Split tunnelling based on destination domain. Solution must support App for endpoints running Windows, Linux and macOS and also should support Mobile app for endpoints running iOS, Android and Windows 10. b)Optional: Support for Chrome OS	Both a and b- 5 Marks (Max) Only-a 2 Mark (Mandatory)
28.	Corrigendum I page 48	Annexure XI(A) , SL No. 174	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet and byte count	Yes-5 Marks(Max) No-0 (Weightage)	GUI based packet capture utility within its management console with capability of creating packet capture filters for IPv4 and IPv6 traffic and ability to define the packet or byte count	Yes-5 Marks(Max) No-0 (Weightage)
29.	Corrigendum I page 50	Annexure XI(A) , SL No. 197	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Should have Host inspection profiling and it should collect information about the host it is running on. The VPN client should submit host information to the gateway upon successful connection. The gateway should match this information with HIP profiles on the NGFW and accordingly NGFW should enforce the corresponding security policy.	1 (Max) (Mandatory)	Should have Host inspection profiling and it should collect information about the host it is running on. The VPN client should submit host information to the gateway/ Client management server upon successful connection. The gateway should match this information with HIP profiles on the NGFW or Client Management server and accordingly NGFW should enforce the corresponding security policy.	1 (Max) (Mandatory)

30.	Corrigendum I page 51	Annexure XI(A) , SL No. 201	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following: <input type="checkbox"/> Automatically identify and block phishing sites <input type="checkbox"/> Prevent users from submitting credentials to phishing sites <input type="checkbox"/> Prevent the use of stolen credential	Yes-5 Marks(Max) No-0 (Weightage)	The NGFW should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials and the following: ·Automatically identify and block phishing sites ·Prevent users from submitting credentials to phishing sites	Yes-5 Marks(Max) No-0 (Weightage)
31.	Corrigendum I page 52	Annexure XI(A) , SL No. 222	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	The solution must be able to use AV and zero day signatures based on payload and not just by hash values and it should support bare metal analysis if required using hybrid setup.	1 (Max) (Mandatory)	Clause stands removed	
32.	Corrigendum I page 55	Annexure XI(A) , SL No. 254	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog , Terminal Services, XFF Headers , Server Monitoring , AND client probing	1 (Max) (Mandatory)	Acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Terminal Services	1 (Max) (Mandatory)
33.	Corrigendum I page 69	Annexure XI(A) , SL No. 421	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Analysis engine must support micro-tasking within Dynamic Analysis O.S VM's (Windows, Macintosh & Linux environments), such as analysis using different versions and service packs of operating systems and different versions of applications by performing the analysis in parallel (i.e. To use multiple virtual machines in parallel) with all licenses and dependencies included in the platform.	1 (Max) (Mandatory)	MANDATORY: Analysis engine must support micro-tasking within Dynamic Analysis O.S VM's (Windows & Linux environments), such as analysis using different versions and service packs of operating systems and different versions of applications by performing the analysis in parallel (i.e. To use multiple virtual machines in parallel) with all licenses and dependencies included in the platform. OPTIONAL: Support for MacOS	Both mandatory and Optional features available: 3-marks(Max) Only Mandatory feature available: 1 Mark (Mandatory)

)
34.	Corrigendum I page 72	Annexure XI(A) , SL No. 462	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Solution must have a dedicated on premises Malware Analysis engine with purpose built platform having windows, Linux and MAC O.S environments. Bidder may size the system as per the best available option.	1 (Max) (Mandatory)	MANDATORY: Solution must have a dedicated on premises Malware Analysis engine with purpose built platform having Windows and Linux OS environments. Bidder may size the system as per the best available option. OPTIONAL: Support for MacOS	Both mandatory and Optional features available: 3- marks(Max) Only Mandatory feature available: 1 Mark (Mandatory)
35.	Corrigendum I page 73	Annexure XI(A) , SL No. 471	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Solution should Include O.S environment support for Windows, Linux and MacOS X systems, completely on-premise. No Submissions should require to be submitted on cloud or 3rd party. All requirements, updates, upgrades, patches must be provided for the solution by the bidder to run for entire project period	1 (Max) (Mandatory)	MANDATORY: Solution should Include O.S environment support for Windows and Linux systems, completely on-premise. No Submissions should require to be submitted on cloud or 3rd party. All requirements, updates, upgrades, patches must be provided for the solution by the bidder to run for entire project period OPTIONAL: Support for MacOS	Both mandatory and Optional features available: 3- marks(Max) Only Mandatory feature available: 1 Mark (Mandatory)
36.	Corrigendum I page 77	Annexure XI(A) , SL No. 516	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO	Damping Sudden Surge in traffic so it does not overwhelm the servers by tracking the number of connections to the server, and adjust the rate of new connections to the server	1 (Max) (Mandatory)	Clause stands deleted	

			NS OF THE SOLUTION			
37.	Corrigendum I page 77	Annexure XI(A) , SL No. 520	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	The ADC solution shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950	1 (Max) (Mandatory)	Clause stands deleted
38.	Corrigendum I page 77	Annexure XI(A) , SL No. 521	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	The ADC solution shall conform to EN 55022 Class A/B or EN 55032 Class A/B or CISPR22 Class A/B or CISPR32 Class A/B or CE Class A/B or FCC Class	1 (Max) (Mandatory)	Clause stands deleted
39.	Corrigendum I page 46	Annexure XI(A) , SL No. 149	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Inspection throughput- 100 Gbps IPsec VPN - 30 Gbps(AES256-SHA256) Sessions- 1,000,000 per second Concurrent Sessions - 50M	Inspection Throughput 150 Gbps or more - 10 Marks (Max) Else 5 Marks	Inspection Throughput 150 Gbps or more - 3 Marks (Max) Else 1 Mark
40.	Corrigendum I page 42	Annexure XI(A) , SL No. 104	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Bandwidth should be dedicated and not shared. Connectivity required, if any, will have to be arranged and factored by the bidder.	1 (Max) (Mandatory)	Bidder/MSSP/ISP/OEM shall provide scrubbing services to mitigate unlimited number of attacks and has to ensure that the required legitimate throughput should always be available for the Bank. 2 (Max) (Mandatory)
41.	Corrigendum I page 42	Annexure XI(A) , SL No. 106	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Service should be always on	1 (Max) (Mandatory)	Service should be always on or On-Demand Protection 2 (Max) (Mandatory)
42.	Corrigendum I page 35	Annexure XI(A) , SL No. 4	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Ports: 12x1/10GE WAN ports, 2X40GE and 2X40/100GE SPF/SPF+ base ports	1 (Max) (Mandatory)	Ports: Minimum 12X10GE WAN ports, 2X40GE and 2X100GE SPF/SPF+ base ports 1 (Max) (Mandatory)

			NS OF THE SOLUTION				
43.	Corrigendum I page 35	Annexure XI(A) , SL No. 6	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	RAM: 16GB and upgradable to 32 GB	1 (Max) (Mandatory)	RAM: 16GB and upgradable to atleast 64 GB. Bidder has to upgrade to atleast 64 GB if utilization reaches threshold (70%)	2 (Max) (Mandatory)
44.	Corrigendum I page 35	Annexure XI(A) , SL No. 7	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Form factor: 1U(Preferably) in standard 42U Rack	1 (Max) (Mandatory)	Form factor: Upto 10U(Preferably) in standard 42U Rack	Upto 10U – 2 Marks(Max) More than 10U-0 Mark (Weightage)
45.	Corrigendum I page 35	Annexure XI(A) , SL No. 8	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Protocols: IPv4, IPv6, Static routes, RIP and RIPv2, OSPFv3, EIGRP , BGP, IGMPv3, IKE, ACL, DHCP, HSRP, RADIUS, AAA, IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPsec, MAC-Sec , SSHv2, SNMPv2c , SNMPv3, NTP, RADIUS, TACACS+.	1 (Max) (Mandatory)	Protocols: IPv4, IPv6, Static routes, RIP and RIPv2, OSPFv3, BGP, IGMPv3, IKE, ACL, DHCP, RADIUS, AAA, IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPsec, SSHv2, SNMPv3, NTP, RADIUS, TACACS+	1 (Max) (Mandatory)
46.	Corrigendum I page 35	Annexure XI(A) , SL No. 9	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Encapsulations: GRE, Ethernet, 802.1q VLAN, PPP, HDLC, PPPoE	1 (Max) (Mandatory)	Clause stands removed	1 (Max) (Mandatory)
47.	Corrigendum I page 35	Annexure XI(A) , SL No. 10	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Encryptions/ Authentication: DES, 3DES, AES-128, AES-256, MD5, MD5, SHA, SHA-256, SHA-384, SHA-512	1 (Max) (Mandatory)	Clause stands removed	
48.	Corrigendum I page 36	Annexure XI(A) , SL No. 14	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Supports SDWAN with IPSec Throughput – 30 Gbps	Yes-5 Marks(Max) No-1 Mark (Weightage)	Clause stands removed	

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

			NS OF THE SOLUTION			
49.	Corrigendum I page 36	Annexure XI(A) , SL No. 19	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Ports: 24/48 nos. 25G/40G SFP/SFP+/QSFP based ports with 100G SFP/SFP+/QSFP+ based uplink Ports	1 (Max) (Mandatory)	Ports: 48x10/25 SFP+ ports with 8X100G ports 1 (Max) (Mandatory)
50.	Corrigendum I page 36	Annexure XI(A) , SL No. 20	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	RAM: 16 GB	1 (Max) (Mandatory)	16GB and upgradable to 64GB and above. Bidder has to upgrade to 64 GB if utilization reaches threshold(70%) 1 (Max) (Mandatory)
51.	Corrigendum I page 36	Annexure XI(A) , SL No. 22	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Protocols: IPv4, IPv6, static routing, RIP, PIM, OSPF, VRRP, PBR, QoS, BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP, SSHv2, SNMPv2c, SNMPv3, NTP, RADIUS, TACACS+.	1 (Max) (Mandatory)	Protocols: IPv4, IPv6, static routing, RIP, PIM, OSPF, VRRP, PBR, QoS, BGPv4, BGPv6 , MPLS, VRF, VXLAN, IS-ISv4, OSPFv3, MP-BGP, SSHv2, SNMPv3, NTP, RADIUS, TACACS+ 1 (Max) (Mandatory)
52.	Corrigendum I page 36	Annexure XI(A) , SL No. 24	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Other Features: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z & 1588v2.	1 (Max) (Mandatory)	Other Features: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.. 1 (Max) (Mandatory)
53.	Corrigendum I page 37	Annexure XI(A) , SL No. 25	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Other Features: IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbour Discovery Inspection and IPv6 Source Guard.	1 (Max) (Mandatory)	Clause stands removed
54.	Corrigendum I page 37	Annexure XI(A) , SL No. 31	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE SOLUTION	Other Features: HA Active-Active/Active-Passive with Clustering	Yes-5 Marks(Max) No-0 Marks	Clause stands removed

PUNJAB NATIONAL BANK
Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001
Email: itdhw@pnb.co.in Tel: 011-23311452

55.	Corrigendum I page 41	Annexure XI(A) , SL No. 84	Annexure XI(A) TECHNICAL AND FUNCTIONAL SPECIFICATIO NS OF THE SOLUTION	Cloud signalling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation.	1 (Max) (Mandatory)	The proposed DDoS Solution must support cloud signaling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for Volumetric DDoS attack mitigation. The on- premise DDoS appliance should integrated with at- least 4 ISP's Scrubbing center solution in India, appropriate proof needs to be submitted	1 (Max) (Mandatory)
56.	Corrigendum page 4, SI No. 13	Eligibility Criteria, Annexure III	SL No. 5	Bidder should have minimum 5 years' experience in implementing Information Security Products and Services either as security integrator or as security implementer including deployment of SOC in large financial institutions which has its offices/branches in atleast 2 of the Metro cities- Delhi NCR, Mumbai , Chennai, Bangalore, Kolkata and Hyderabad with wide area network, intranet and internet as well as demilitarized zone and security equipment's like (atleast 3) Next Generation Firewalls, NIPS, Application delivery controller(ADC), Web Application Firewall(WAF) etc. Out of 5 years' experience, at least 3-year experience (as on the date of publishing this RFP) should be in a Scheduled Commercial Banks with minimum 1.4 Lakh Crores total business in FY 2020-21 or 2021-22 or RBI	Bidder should have minimum 5 years' experience in implementing Information Security Products and Services either as security integrator or as security implementer including deployment of SOC in RBI or large financial institutions which has its offices/branches in atleast 2 of the Metro cities- Delhi NCR, Mumbai , Chennai, Bangalore, Kolkata and Hyderabad with wide area network, intranet and internet as well as demilitarized zone and security equipment's like (atleast 3) Next Generation Firewalls, NIPS, Application delivery controller(ADC), Web Application Firewall(WAF) etc. Out of 5 years' experience, at least 3-year experience (as on the date of publishing this RFP) should be in a RBI or Scheduled Commercial Banks with minimum 1.4 Lakh Crores total business in FY 2020-21 or 2021-22.		
57.	Page 114-117	Annexure X(A) and X(B)	MAF and UNDERTAKING	Revised MANUFACTURER'S (OEM) AUTHORIZATION FORM (MAF).(ANNEXURE-XA) and UNDERTAKING FOR BEING the OEM of the OFFERED DEVICES for SUPPLY OF CYBER SECURITY COMPONENTS....(ANNEXURE-XB)			
58.	Page 180-181	ANNEXU RE XXIV	Checklist	Revised Checklist			

MANUFACTURER'S (OEM) AUTHORIZATION FORM (MAF)

(To be provided on the Letter head of the OEM duly signed & stamped by their Authorized Signatory.)

To
The Assistant General Manager
I T Procurement Department
Punjab National Bank
I.T. Division, Head Office
New Delhi

Dear Sir,

Reg.: RFP FOR PROCUREMENT AND MANAGEMENT OF CYBER SECURITY COMPONENTS.

We hereby submit the following: -

We, M/s _____ who are the established and reputable manufacturers of the following equipment/components/devices/solution/services (as per table A below) having factories at _____ do hereby authorize M/s _____ (who is the vendor submitting it's bid pursuant to the Request for Proposal issued by Punjab National Bank) to offer their quotation, negotiate and conclude a contract with you against the above bid invitation with our products.

Table-A

SL No.	Components/ devices/ solution/ equipment/services Name	Model No.	Components/ devices/ solution/ equipment/services conforms to all the technical specifications and requirements mentioned in this RFP

(Add as many rows as required)

We hereby extend our guarantee and warranty as per the terms and conditions of this RFP and it's subsequent Corrigendum and/or Clarifications, if any, and the contract for the equipment/component/solution/device and services offered against this invitation by the above mentioned Bidder. We also hereby undertake to perform the obligations as set out in the RFP in respect of such equipment and services.

In case the bidder i.e. M/s _____ is not able to perform the obligations as per RFP during the contract period (like if bidder ceases to exist from the ICT Industry, stops services or support to the Bank, terminates contract due any reasons with Bank or due to any other reason), we will perform the said obligations, as per given scope of work of RFP, either directly or through mutually agreed third party/any other authorized Partner of ours.

With reference to all the components/parts/assemble/software used inside the company products being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/software shall be original new components / parts / assembly / software only and that no refurbished, duplicate, second hand components, parts, assembly are being supplied.

Date:

Place:

Yours faithfully
Signature of Authorized Signatory
Name of Signatory:
Designation:
Email ID:
Mobile No:
Telephone No.:
Seal of Company

UNDERTAKING FOR BEING the OEM of the OFFERED DEVICES for SUPPLY OF CYBER SECURITY COMPONENTS

To
The Assistant General Manager
I. T. Procurement Department
Punjab National Bank
I.T. Division, Head Office, New Delhi

Sir
Reg: RFP for Procurement and Maintenance of Cyber Security Component.
We hereby submit the following: -

We, M/s_____ are the OEM of the devices/components/solution/services (as per Table A) having factories at _____ do hereby offer our quotation against the above bid invitation with our products.

Table A

SL No.	Components/ devices/ solution/ equipment/services Name	Model No.	Components/ devices/ solution/ equipment/services conforms to all the technical specifications and requirements mentioned in this RFP

We hereby extend our guarantee and warranty as per the terms and conditions of this RFP and its subsequent Corrigendum and/or Clarifications, if any, and the contract for the equipment/component/solution/device and services offered against this invitation. We also hereby undertake to perform the obligations as set out in the RFP in respect of such equipment and services.

With reference to all the components/parts/assemble/software used inside the company products being quoted by us vide your tender cited above, we hereby undertake that all the components / parts / assembly used inside the company products/software shall be original new components / parts / assembly / software only and that no refurbished, duplicate, second hand components, parts, assembly are being supplied.

Date:

Place:

Yours faithfully

Signature of Authorized Signatory

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company

ANNEXURE XXIV

CHECKLIST

Sl No.	Particulars	Compliance (Yes/No)
1.	Proof of RFP Cost	
2.	Proof of EMD	
3.	Terms and Conditions (Annexure-I)	
4.	UNDERTAKING FROM THE BIDDER.....(ANNEXURE-II)	
5.	ELIGIBILITY CRITERIA OF THE BIDDER.....(ANNEXURE-III)	
6.	BIDDER'S INFORMATION.....(ANNEXURE-IV)	
7.	COMPLIANCE STATEMENT.....(ANNEXURE-V)	
8.	PERFORMANCE CERTIFICATE.....(ANNEXURE-VI)	
9.	LITIGATION CERTIFICATE.....(ANNEXURE-VII)	
10.	UNDERTAKING FOR NON- BLACKLISTED.....(ANNEXURE - VIII)	
11.	TURNOVER CERTIFICATE.....(ANNEXURE-IX)	
12.	MANUFACTURER'S (OEM) AUTHORIZATION FORM (MAF).....(ANNEXURE-XA)	
13.	UNDERTAKING FOR BEING the OEM of the OFFERED DEVICES for SUPPLY OF CYBER SECURITY COMPONENTS.....(ANNEXURE-XB)	
14.	TECHNICAL AND FUNCTIONAL SPECIFICATIONS OF THE APPLICATION.....(ANNEXURE-XI(A))	
15.	SCORING METHODOLOGY.....(ANNEXURE-XI(B))	
16.	PERFORMA FOR INTEGRITY PACT.....(ANNEXURE - XIII)	
17.	Performa for the Bank Guarantee.....(ANNEXURE- XIV)	
18.	Certificate regarding RFP FOR PROCUREMENT AND MANAGEMENT OF CYBER SECURITY COMPONENTS.....(ANNEXURE- XV(A))	
19.	Certificate regarding RFP FOR PROCUREMENT AND MANAGEMENT OF CYBER SECURITY COMPONENTS.....(ANNEXURE- XV(B))	
20.	Complete Bill of Material of Offered Solution/Hardware (BOM).....(ANNEXURE- XVI)	

21.	NDA (Non-Disclosure Agreement).....(ANNEXURE XVII)	
22.	UNDERTAKING OF INFORMATION SECURITY FROM THE BIDDER.....(ANNEXURE - XVIII)	
23.	Escalation Matrix (Both OEM & Bidder with its parent Company).....(ANNEXURE- XIX)	
24.	Undertaking for Labour Law Compliance.....(ANNEXURE- XX)	
25.	DECLARATION THAT THE FIRMWARE/SOFTWARE IS FREE FROM BUGS/ VULNERABILITY.....(Annexure XXI)	
26.	DETAILS OF OFFERED SOLUTION.....(Annexure XXII)	
27.	LIST OF ITEMS ALREADY DEPLOYED IN THE BANK.....(Annexure XXIII)	
28.	Power of Attorney if applicable and Copy of Board Resolution of the Bidder and all the OEMs involved in the Bid	

Date: _____

Place: _____

Signature of Authorized Signatory

Name of Signatory:

Designation:

Email ID:

Mobile No:

Telephone No.:

Seal of Company