NHPC LIMITED
(A Govt. of India Enterprise)
NHPC Office Complex, Sector-33, Faridabad-121003, Haryana (India)

CIN: L40101HR1975GOI032564

Dated: 05.04.2024

Replies to Bid queries alongwith Amendment No. 1

Description of Work: **Procurement of Cyber Security Equipment.**

GeM Bid No.: GEM/2024/B/4705638 dated 15.03.2024

In reference to subject tender, please find enclosed herewith the replies of the queries of the prospective bidders annexed as Appendix-I (Technical) alongwith Amendment No. 1 to the tender document.

Encl.: i) Amendment No. 1 (1 page)

ii) Appendix-I (Reply to Bid queries) (3 pages)

For & on behalf of NHPC Ltd.

Sd/-

General Manager (E)
Contracts (E&M)-IV Division

NHPC Limited
(A Govt. of India Enterprise)

Dated:05.04.2024

Amendment No.1

Name of Work: Procurement of Cyber Security Equipment.

GeM Bid No: GEM/2024/B/4705638 dated 15.03.2024

In reference to subject tender, the following amendments are hereby authorized to be incorporated in the tender document:

Sl. no.	Clause No.	Tender Provision	Amendment
Special Terms & Conditions (STC)			
1.	Annexure-A, Sr. No. 5 Security Information and Event Management (SIEM), Generic Points	The SIEM solution should be software based with a clear logical and physical separation of the collection module, logging module and correlation module.	The SIEM solution should be software based with a clear logical or physical separation of the collection module, logging module and correlation module.

Except above, all other terms & conditions and Scope of Work & Technical specifications of the tender document shall remain unchanged.

Sd/-
General Manager (E)
Contracts (E&M)-IV Division

Appendix-1

NHPC LIMITED
(A Govt. of India Enterprises)

Replies to Bid Queries

Name of Work: Regarding Procurement of Cyber Security Equipment.

GeM Bid Number: GEM/2024/B/4705638 dated 15.03.2024

SN	Page No.	Clause No.	Vendor's Query / Comment	NHPC Reply
1			Relaxation is requested in Prior Experience criteria from bidder to OEM/Bidder so that NHPC can get good participation from authorized vendors. Already there are OEM specification criteria and only OEM authorized bidders are allowed to quote. Therefore it is requested to make Prior experience to bidder /OEM.	Bid conditions are clear in this regard. Please adhere with bid condition.
2			"Section Name & No" - "5. Security Information and Event Management (SIEM) Generic Points", Page No. 37 "Clarification Required" - Kindly confirm the number of locations the Central SIEM deployed in DC needs to monitor (if any remote locations/ isolated network or similar).	Number of locations the Central SIEM needs to monitor is 2.
3	8 and Web Application firewall	Layer 7 requests per second: 900,000	WAF is used for L7 protection and L7 RPS plays an important role in terms of performance, it is requested by the honorable committee to increase the L7 RPS. It is suggested to amend the clause as "Layer 7 requests per second: 5 M"	Bid conditions are clear in this regard. Please adhere with bid condition.

4	8 and Web Application firewall	The proposed appliance should support the below metrics: Minimum Misses, Hash, Persistent Hash, Tunable Hash, Least Connections, Least connections per service, Round-Robin, Response Time, Bandwidth.	Specification clearly mentioned that the requirement is of Web Application Firewall. The feature asked in this Clause is relevant for Load Balancer NOT for a Web Application Firewall. Hence, we requested to the committee kindly delete this clause.	Bid conditions are clear in this regard. Please adhere with bid condition.
5	8 and Web Application firewall	DNSSEC should be supported in the proposed device from Day 1	Specification clearly mentioned that the requirement is of Web Application Firewall. The feature asked in this Clause is relevant for Load Balancer NOT for a Web Application Firewall. Hence, we requested to the committee kindly delete this clause.	Bid conditions are clear in this regard. Please adhere with bid condition.
6	9 and Web Application firewall	Addition of this clause	To ensure the stability of participating OEM we requested that the committee kindly add this clause as "Minimum 50Cr turnover in any of the last 3 financial years and proof to be submitted"	Bid conditions are clear in this regard. Please adhere with bid condition.

7	9 and Web Application firewall	Addition of this clause	The anti-defacement features monitors your web sites for defacement attacks. If it detects a change, it can automatically reverse the damage. we requested to the committee for the addition of this clause "The WAF should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client. It should returns the cached original web page to make the anti-defacement effects unnoticeable or returns a 503 error page to the client to end the service".	Bid conditions are clear in this regard. Please adhere with bid condition.
8	9 and Web Application firewall	Addition of this clause	"Considering the asked 5 Virtual Instances from Day 1 and scalable up to 10 Virtual Instances. and dedicated allocation of parameters per virtual instance, RAM and Hard disk are important parameters for multiple functions, however, there is no RAM and Hard disk parameter mentioned in the specification hence, this is requested to be included within the specification. It is suggested to the addition of the clause"" The proposed Appliance must have the below configuration A. Should have minimum 4 TB hard disk and 128 GB RAM."""	Bid conditions are clear in this regard. Please adhere with bid condition.
9			"We would like to inform you that we have ISO/IEC 15408-1:2022 Certificate which is Indian equivalent Certificate to Common criteria certificate. Apart we also have other industry standard certificate like CE, ROHS, UL, FCC, IEC 60068-2-27:2008, IEC 60068-2-31:2008, IEC 61967-1:2018, IEC 62151:2000, IEC 60215:2016, EN 300 386 V2, 2.1:2022, EN 50121-4:2016+A1:2019, EN 55022:2010, EN 60950-1:2005 certificates. Kindly let us know the exact name of the Indian Certificate which will be acceptable in the bid."	"As per bid conditions, Common criteria/any Indian Certificate is required. ISO/IEC 15408-1:2022 Certificate is also acceptable."

NHPC LIMITED
(A Govt. of India Enterprise)
NHPC Office Complex, Sector-33, Faridabad-121003, Haryana (India)

CIN: L40101HR1975GOI032564

Dated: 10.04.2024

Replies to Bid queries alongwith Amendment No. 2

Description of Work: **Procurement of Cyber Security Equipment.**

GeM Bid No.: GEM/2024/B/4705638 dated 15.03.2024

In reference to subject tender, please find enclosed herewith the replies of the queries of the prospective bidder annexed as Appendix-II (Technical) alongwith Amendment No. 2 to the tender document.

Encl.: i) Amendment No. 2 (10 pages)

ii) Appendix-II (Reply to Bid queries) (3 pages)

For & on behalf of NHPC Ltd.

Sd/-

General Manager (E)
Contracts (E&M)-IV Division

NHPC Limited
(A Govt. of India Enterprise)

Dated: 10.04.2024

Amendment No.2

Name of Work: Procurement of Cyber Security Equipment.

GeM Bid No: GEM/2024/B/4705638 dated 15.03.2024

In reference to subject tender, the following amendments are hereby authorized to be incorporated in the **Special Terms & Conditions (STC)** of tender document:

Sl. no.	Clause No.	Tender Provision	Amendment
1	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), Performance & Scalability	Appliance must have one Console port, dedicated one management Port, one USB port and redundant power supply. The device should have 8 x 1G Copper ports, 6 x 10G SFP+ port from day 1. The device should have provision of adding 8 x 1G copper ports in future without changing hardware. Appliance should have 900 GB Storage from day 1. Appliance should support 15 Gbps or more Firewall throughput & 10 Gbps or more IPS throughput. Appliance should support 9 Gbps or more Threat Protection throughput. The device should have Concurrent Sessions: 4 million or higher & New connection/Sec: 100,000 or higher. Firewall Should support at least 3 Gbps or more IPsec VPN throughput and 1000 IPsec Site-to-Site VPN tunnels & 2000 IPsec VPN clients.	Appliance must have one Console port, dedicated one management Port, one USB port and redundant power supply. The device should have 8 x 1G Copper ports, 6 x 10G SFP+ port from day 1. The device should have provision of adding 8 x 1G copper ports in future without changing hardware. Appliance should have 900 GB Storage from day 1. Appliance should support 15 Gbps or more Firewall throughput & 10 Gbps or more IPS throughput. Appliance should support 9 Gbps or more Threat Protection throughput. The device should have Concurrent Sessions: 4 million or higher & New connection/Sec: 100,000 or higher. Firewall Should support at least 3 Gbps or more IPsec VPN throughput and 1000 IPsec Site-to-Site VPN tunnels & 2000 IPsec VPN clients.

Sl. no.	Clause No.	Tender Provision	Amendment
		Firewall Should support at least 5 Gbps or more TLS/SSL inspection & decryption throughput and 100 SSL VPN clients. The appliance should have 100,000 SSL DPI connections.	Firewall Should support at least 5 Gbps or more TLS/ SSL inspection & decryption throughput and 100 SSL VPN clients. **The appliance should support SSL DPI inspection.**
2	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), General Firewall Features	Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy-based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic. Should support BGP, OSPF, RIP v1/v2 routing protocol and Ipv4 & Ipv6 functionality. Firewall should support manual NAT and Auto-NAT, Static NAT, Dynamic PAT, PAT etc. Should have Layer 2 bridge or transparent mode/ Wire mode/Sniffer mode /Tap mode. Should support Zero-Touch registration & provisioning using Web/ mobile App. solution should support policy-based routing, Application based routing and Multi Path routing. Application Control: The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500 application signatures. Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP and others.	Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy-based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone traffic. Should support BGP, OSPF, RIP v1/v2 routing protocol and Ipv4 & Ipv6 functionality. **Firewall should support manual NAT, Static NAT, PAT etc.** Should have Layer 2 bridge or transparent mode/ Wire mode/Sniffer mode /Tap mode. **Should support Zero-Touch registration/minimal human intervention & provisioning using Web/ mobile App.** solution should support policy-based routing, Application based routing and Multi Path routing. Application Control: The proposed system shall have the ability to detect, log and take action against network traffic based on over 3500 application signatures. Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP and others.

Sl. no.	Clause No.	Tender Provision	Amendment
		Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy. Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found. The Firewall should Support for TLS 1.3 to improve overall security on the firewall. This should be implemented in Firewall Management, SSL VPN/DPI. Firewall should support client/clientless SSL VPN technology or an easy to manage IPsec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms. Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback. Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate-based authentication connection tunnel. Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly rerouting traffic between endpoints through alternate routes.	**Firewall should support Link aggregation to provide additional level of redundancy.** Firewall should support static routing, Dynamic Routing and WAN load balancing for redundant or backup Internet connections. Should support deep packet SSL to decrypt HTTPS traffic for scanning (IPS, Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found. **The Firewall should Support for TLS 1.3 to improve overall security on the firewall.** Firewall should support client/clientless SSL VPN technology or an easy to manage IPsec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms. Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback. Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate-based authentication connection tunnel. Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly rerouting traffic between endpoints through alternate routes.

Sl. no.	Clause No.	Tender Provision	Amendment
		Solution should support Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, Route-based VPN over OSPF, RIP, BGP. Proposed solution must support application inspections on following protocols DNS, FTP, H.323, SMTP, NetBIOS, TFTP, SNMP etc. Solution should support User identification and activity available through seamless AD/LDAP/Citrix/Terminal Services SSO integration. Should have secure SD-WAN that enables organizations to build, operate and manage secure, high-performance networks across remote sites for exchanging traffic using low-cost internet services without adding any additional components or hardware. Vendors not having SDWAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1. Firewall should have Pictorial view of a particular access rule, NAT and Routing rule.	Solution should support Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, Route-based VPN over OSPF, RIP, BGP. **Proposed solution must support application inspection**. Solution should support User identification and activity available through seamless AD/LDAP/ Citrix/Terminal Services SSO integration. Should have secure SD-WAN that enables organizations to build, operate and manage secure, high-performance networks across remote sites for exchanging traffic using low- cost internet services without adding any additional components or hardware. Vendors not having SD-WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1. ~~Firewall should have Pictorial view of a particular access rule, NAT and Routing rule.~~
3	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), Firewall Security Features	Firewall should scan for threats in both traffic for malware in files of unlimited length and size across all ports and TCP streams by GAV /Cloud AV. The proposed firewall should support raw TCP inspection that scans raw TCP streams on any port to detect and prevent threats.	**Firewall should scan for threats in inbound traffic for malware in files of unlimited length and size across all ports by GAV /Cloud AV.** ~~The proposed firewall should support raw TCP inspection that scans raw TCP streams on any port to detect and prevent threats.~~

Sl. no.	Clause No.	Tender Provision	Amendment
		Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc. Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations and can be applied on common protocols as well as raw TCP streams. Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture. Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 5000 IPS Signatures or 20K DPI signatures or 50 million Cloud AV signatures from day 1. Should protect against DdoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DdoS through UDP/ICMP flood protection and connection rate limiting. Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management. URL database should have at least 15-20 million sites and 55 + categories.	Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc. **Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations and can be applied on common protocols**. Solution should have single-pass DPI architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture. Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 5000 IPS Signatures or 20K DPI signatures or 50 million Cloud AV signatures from day 1. **Should protect against DdoS/DoS attack using Layer 3 SYN/ Layer 2 SYN**. It protects against DOS/ DdoS through UDP/ICMP flood protection and connection rate limiting. Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management. **URL database should have**

Sl. no.	Clause No.	Tender Provision	Amendment
		Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. Should have advanced QoS that guarantees critical communications on the network. Firewall should support SQL injection Protection, Crosssite scripting Protection (XSS) & DNS security. Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. Solution should support on premise/ cloud based Multi-engine Sandboxing for preventing zero-day threats. The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel	**at least million sites and 55 + categories**. Shall be able to configure traffic shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy. Should have advanced QoS that guarantees critical communications on the network. Firewall should support SQL injection Protection, Crosssite scripting Protection (XSS) & DNS security. Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. **Solution should support on premise/ cloud based Sandboxing for preventing zero-day threats**. The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side

Sl. no.	Clause No.	Tender Provision	Amendment
		attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc. Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multibrowser environments. Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. Deep packet SSL should be available on the same platform & License for DPI SSL should be along with appliance. The Firewall solution should have detection and prevention capabilities for Command & Control communications and data exfiltration. Firewall Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.	Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc. **Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android**. Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined. Deep packet SSL should be available on the same platform & License for DPI SSL should be along with appliance. The Firewall solution should have detection and prevention capabilities for Command & Control communications and data exfiltration. Firewall Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.

Sl. no.	Clause No.	Tender Provision	Amendment
4	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), Visibility and Monitoring	Should provide real-time monitoring and visualization provides a graphical representation of top applications, top address, top users and intrusion by sessions for granular insight into traffic across the network. The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status. Solution should have real-time visibility of critical attacks & observed threats. Any license required for this should be enabled from day 1.	**Should provide real-time monitoring provides a graphical representation of top applications, top address, top users and intrusion by sessions/hit count for granular insight into traffic across the network.** The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status. Solution should have real-time visibility of critical attacks & observed threats. Any license required for this should be enabled from day 1.
5	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), Management & Reporting Feature	The management platform must be accessible via a web-based interface and without any additional client software. Firewall should support management via CLI, SSH, GUI and support for SNMPv2/3. The solution should support Centralize management which includes configuration, monitoring performed by the Management Centre On-prem / on cloud. The Centralize management platform should support multidevice firmware upgrade, global policy template to push config across multiple firewalls in single click. The Centralize management platform should support account lockout security & account access control.	The management platform must be accessible via a web-based interface and without any additional client software. Firewall should support management via CLI, SSH, GUI and support for SNMPv2/3. The solution should support Centralize management which includes configuration, monitoring performed by the Management Centre On-prem / on cloud. **The Centralize management platform should support multidevice firmware upgrade, policy to push config across multiple firewalls in single click/ minimal human intervention**. The Centralize management platform should support account lockout security & account access control.

Sl. no.	Clause No.	Tender Provision	Amendment
		The on prem Centralize management platform should support closed network deployment. The solution should store syslog in local storage or remote appliance. OEM can offer individual solution for logging and reporting based architecture to meet the requirements. Firewall should have reporting facility to generate reports on virus detected, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks in different formats such as PDF/TEXT/ CSV. The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address. Analytics platforms support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem. The solution should support Cloud-based/ On Prem configuration backup. The solution should support IPFIX or NetFlow protocols for real-time and historical monitoring and reporting. The solution should support Application Visualization and Intelligence – should show historic and real-time reports of what applications are being	The on prem Centralize management platform should support closed network deployment. **The solution should store logs in local storage or remote appliance.** Firewall should have reporting facility to generate reports on virus detected, top sources for viruses, destination for viruses, top viruses etc. Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks in different formats such as PDF/TEXT/ CSV. The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address. Analytics platforms support Real-time risk monitoring and analysis of all network and user traffic that passes through the firewall ecosystem. The solution should support Cloud-based/ On Prem configuration backup. **The solution should support IPFIX or NetFlow protocols or OEM standard for real-time and historical monitoring and reporting**. The solution should support Application Visualization and Intelligence – should show historic and real-time reports of what applications

Sl. no.	Clause No.	Tender Provision	Amendment
		used, and by which users. Reports should be completely customizable. Logging and reporting solution should be supported. The solution shall have readymade templets to generate reports like complete reports or attack reports.	are being used, and by which users. Reports should be completely customizable. Logging and reporting solution should be supported. The solution shall have readymade templets to generate reports like complete reports or attack reports.
6	Annexure-A, Next Generation Firewall (10 Gbps IPS Throughput), Certification, Warranty, Installation, Testing and Commissioning	Proposed Solution should support 24x7x365 telephone, email and web-based technical support. OEM should have TAC / R&D Centre in INDIA. Common criteria/ Any Indian certificate. Manufacturer's warranty should be mentioned minimum 05 (five) years. warranty including all services like GAV, IPS, Antispyware or antimalware, Application control, BoT protection, ATP, Patch & Firmware upgrade. Bidder must carry out on site installation, testing and commissioning.	**Proposed Solution should support 24x7x365 telephone, email or web-based technical support**. OEM should have TAC / R&D Centre in INDIA. Common criteria/ Any Indian certificate. Manufacturer's warranty should be mentioned minimum 05 (five) years. warranty including all services like GAV, IPS, Antispyware or antimalware, Application control, BoT protection, ATP, Patch & Firmware upgrade. Bidder must carry out on site installation, testing and commissioning.

Except above, all other terms & conditions and Scope of Work & Technical specifications of the tender document shall remain unchanged.

Sd/-
General Manager (E)
Contracts (E&M)-IV Division

Appendix-II

NHPC LIMITED
(A Govt. of India Enterprises)

Replies to Bid Queries

Name of Work: Regarding Procurement of Cyber Security Equipment.

GeM Bid Number: GEM/2024/B/4705638 dated 15.03.2024

SN	Page No.	Clause No.	Vendor's Query / Comment	NHPC Reply
1	15	Scope of Work	As per the mentioned clause, there are three locations, Request you to kindly confirm are three locations where deployment is required or two locations DC and DR, please specify the DC and DR location as well	Deployment is required at NHPC Faridabad/BSNL Data Centre Faridabad.
2	15 and 23	b) The Bidder shall implement the Firewalls in HA mode at BSNL DC Faridabad and DR- NICSI Delhi. c) Make offered for BoQ item No. 1- Firewall 32 Gbps should be different from make offered for BoQ item No. 2-Firewall 10 Gbps."	The scope of work is not matching the BOQ, as per scope of work there should be 4 internal firewalls (2 at DC and 2 at DR) and similarly 4 Nos of external firewall (2 at DC and 2 at DR), However the as per BOQ only 2 firewall of each type (Internal & External) is mentioned. Request to kindly clarify the same. do we need to supply 4 at DC and 4 at DR which include both type firewalls as you are looking in HA mode.	As per BoQ, 2 nos. firewall in HA for DC and 02 nos. firewall in HA for DR are required.
3	23	PAM, SIEM, MFA, DLP, NAC	Kindly confirm whether these components needs to be deployed at DC only or DC and DR both.	NHPC Faridabad/ BSNL DC only

4	General Query		Supporting network components in not mentioned in the RFP, request you to kindly confirm do we need propose the supporting network components (switches, SFPs, Passive cabling etc.) or we have to deploy it in the existing network.	Existing network
5	General Query		If we need to deploy it in the existing architecture, request you to kindly share the existing network architecture with port connection type and speed and availability.	Architecture shall be provided during implementation
6	General Query		Do we need to consider the infra required like compute, virtualization, OS , DB , storage etc. required to deploy the solution like SIEM/MFA Etc.	No
7	General Query		How much log retention period is required for SIEM and how much should be online and how much should be in archival.	Already mentioned in bid document as 06 month online and 01 year offline.
8	General Query		Is DC-DR replication required for logs.	No
9	General Query		What is connectivity between DC and DR and how much bandwidth available	Not applicable
10	General Query		In case some additional component is required to run the solution like compute , switches ,do these components also required to meet the MII.	All components should meet MII requirement as applicable.
11	General Query		Kindly confirm whether rackspace will be provided by the NHPC or we need to propose the rack also.	Rackspace shall be provided by NHPC
12	General Query		Kindly allow site survey before bidding so that appropriate solution can be proposed by the bidder.	Please adhere to bid conditions
13	General Query		MII firewalls with 60% LC OEMs (eg. Gajshield) are not fully complying in this RFP , request you to plesase	Please refer amendment

			ammend the specifications so that MII OEMs could also comply , attached is the Queries of MII OEM also.	
14	General Query		Some of the OEMs may not the Form1 and Form1-A but providing 60% local content declaration, In that case request you to kindly consider the declaration also.	Please adhere to bid conditions