

Response to the Pre-Bid Queries

S. No.	Volume of the RFP (I/II/III)	RFP document reference(s) (Section, page number & Clause No.)	Actual Clause in the RFP	Clarification Sought	Response
1	Volume I	Section 3.1, Technical Qualification Criteria, A1 Core Banking Solution, Page 38	The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and allied products within the last five (5) years from the date of bid submission , with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally.	The Bidder /or Wholley owned subsidiary from Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and allied products within the last five (5) years from the date of bid submission (or date of publishing bid), with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally.	As per RFP

Response to the Pre-Bid Queries

2	Annexure N	Secured Internet Access	Solution should facilitate remote users to securely access Internet and internal applications through Web Browsers, Desktop Clients, Mobile Clients, and Secured Browser etc.	Request to Modify (VENDOR-SPECIFIC BIAS): This requirement bundles 'Secured Browser' alongside standard access methods (Web Browsers, Desktop Clients, Mobile Clients). This is technically incorrect and appears to favor specific vendors: (1) TECHNICAL ISSUE: A unified SSE agent/client already provides comprehensive internet security for ALL traffic (browser and non-browser) across all applications. Adding 'Secured Browser' as a separate mandatory access method is redundant when a unified endpoint client is deployed. (2) VENDOR BIAS: Only certain vendors offer standalone 'Secure Browser' products, while industry-leading SSE solutions provide holistic security through unified clients that protect ALL endpoint traffic, not just browser traffic. (3) RECOMMENDATION: Request to modify to 'Solution should facilitate remote users to securely access Internet and internal applications through unified endpoint clients supporting Web Browsers, Desktop applications, and Mobile devices.'	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

3	AnnexureN	Secured Internet Access	The solution must have file encryption capabilities to encrypt the files downloaded from the sensitive applications accessed via Secured Browser or Remote Browser Isolation.	Request to Drop (VENDOR-SPECIFIC & TECHNICALLY REDUNDANT): This requirement should be dropped for the following reasons: (1) TECHNICALLY REDUNDANT: Modern SSE solutions provide superior alternatives: (a) Browser Isolation renders sensitive content as pixel-streams without actual file download, this ensures superior security and abide by zero trust . (b) DLP policies can block/allow downloads based on sensitivity. 2) VENDOR-SPECIFIC: File encryption for downloads specifically via 'Secured Browser' is a niche capability offered by very specific vendor, restricting fair competition. This requirement appears to be tailored for specific vendor products. Request to either DROP this requirement or modify to , 'The solution must have capabilities to protect sensitive data in files accessed via Browser Isolation, view-only rendering, or equivalent data protection controls'	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

4	AnnexureN	Secure Browser - General	Multiple references to 'Secure Private Browser' as mandatory component throughout the RFP including in Secure Internet Access section.	All 'Secure Browser' capabilities (SSL inspection, URL filtering, threat protection, DLP) are ALREADY covered in 'Secure Internet Access' section which mandates Unified SSE Agent. Creating separate section: • Duplicates requirements already specified • Creates evaluation confusion • Adds unnecessary complexity (4) VENDOR-SPECIFIC BIAS: Mandating a dedicated 'Secure Private Browser' as separate installable product: • FAVORS only vendors with proprietary browser products (specific vendor) • EXCLUDES industry-leading SSE vendors who provide comprehensive unified agents • EXCLUDES vendors providing Browser Isolation (superior security) This restricts competition without providing better security - in fact, it provides WORSE security. (5) INDUSTRY STANDARD: Per Gartner SSE framework, the recommended architecture is: • Unified SSE Agent for complete endpoint internet security (ALL traffic)	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

			• Browser Isolation for high-risk scenarios (no installation). • NOT a separate installable browser that only protects itself because installing a browser is creating another attack surface in the endpoint, the browser can itself get compromised which can itself lead to loss of security REQUEST: DROP the entire 'Secure Private Browser' section (S.No. 1-71) because: • It creates a FALSE SENSE OF SECURITY while leaving major gaps • It DOES NOT PROTECT DoP users completely • It is a SUBSET of Secure Internet Access (already covered). • It FAVORS single vendor without security justification • It is against INDUSTRY STANDARD architecture This provides COMPLETE protection for DoP users, not partial protection through a single browser.	

Response to the Pre-Bid Queries

5	Annexure N	DLP Section - General (S.No. 1-48)	Entire DLP section with 48 requirements covering: Data Visibility & Classification (S.No. 1-33) and Web Protection Security (S.No. 34-48)	Request to DROP 'DLP Section' (VENDOR-SPECIFIC & REDUNDANT): (1) ARCHITECTURAL REDUNDANCY WITH SECURE INTERNET ACCESS: • DLP is ALREADY covered extensively in 'Secure Internet Access' section • SSL Inspection, Content Filtering, URL Filtering - ALREADY in Secure Internet Access • Unified SSE solutions provide INLINE DLP as integral component, not separate product Creating a separate DLP section with overlapping requirements causes evaluation duplication. (2) WEB PROTECTION SECURITY (S.No. 34-48) IS DUPLICATE: • S.No. 34-48 asks for: Proxy, SSL Inspection, URL Filtering, Content Filtering, Malware Protection, Social Media Controls • ALL of these are ALREADY specified in 'Secure Internet Access' section • This is NOT DLP - this is Secure Web Gateway functionality duplicated Request to REMOVE S.No. 34-48 entirely as duplicate. (3) VENDOR-SPECIFIC	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

				BIAS - • S.No. 40: Specific hardware specs (128GB RAM, 10G/25G ports, iDRAC, RAID 10) (4) INDUSTRY STANDARD - UNIFIED SSE: Per Gartner SSE framework, modern architecture is: • Unified SSE with integrated DLP (single platform) • NOT separate standalone DLP appliance Mandating separate DLP appliance is LEGACY architecture that: • Increases complexity and cost • Creates policy management silos • Contradicts Zero Trust unified approach (5) DSPM REQUIREMENTS NEED CLARIFICATION: S.No. 9-19 describe Data Security Posture Management (DSPM) for data-at-rest which is DISTINCT from inline DLP. If DSPM is required, it should be: • Clearly separated from inline DLP requirements • Evaluated as optional/separate component • Not bundled with web proxy requirements	

Response to the Pre-Bid Queries

				REQUEST: (a) DROP the entire 'Web Protection Security' sub-section (S.No. 34-48) as it is DUPLICATE of Secure Internet Access, (b) DROP the entire DLP section as it is duplicate and already present into 'Secure Internet Access' section. NOTE: Current DLP section structure favors legacy ,standalone vendors and EXCLUDES SSE leaders who provide superior unified DLP with SSE.	

Response to the Pre-Bid Queries

6	Volume II	5.2.5.10, Page Number 117, Point no 2	The solution must handle a sustained throughput of at least 20,000 transactions per second (TPS) with the capacity to scale up to 50,000 TPS to accommodate future growth over the contract period	1. It is written Sustained TPS of 20000 - or middleware should support upto 20000 TPS. Assumed this TPS is for WebSphere Application Server. Please confirm? 2. Please confirm the 20000 TPS is sustained on WebSphere Application Server as its not aligned with Annexure O - Where Online + Offline and TPS comes around to be 2000? 3. Please give me the expected TPS required for ESB and WebSphere Application Server sepearately?	The middleware is envisaged as the backbone of the entire POSB IT system where all the applications will communicate with each other through this Middleware. Hence, it is projected that the proposed middleware should be capable of handling 20,000 communications with scalability upto 50,000. As per Annexure O - TPS of 300 has been given for the online transactions initiated by the citizens as per current statistics which is bound to grow with launch of revamped Internet and Mobile Banking services, along with UPI (which may push the TPS to 500 and beyond). Bidders are required to propose the solution and the Hardware meeting the above requirements.

Response to the Pre-Bid Queries

7	Volume II	Annexure O	User Metrics	Can TPS advised for Online and Offline TPS be used for TPS for API Gateway?	The middleware is envisaged as the backbone of the entire POSB IT system where all the applications will communicate with each other through this Middleware. Hence, it is projected that the proposed middleware should be capable of handling 20,000 communications with scalability upto 50,000. As per Annexure O - TPS of 300 has been given for the online transactions initiated by the citizens as per current statistics which is bound to grow with launch of revamped Internet and Mobile Banking services, along with UPI (which may push the TPS to 500 and beyond). API Gateway for external integrations should be separate from API Gateway for internal integrations. Bidders are required to propose the solution and the Hardware meeting the above requirements.

Response to the Pre-Bid Queries

8	Volume II	Annexure J Middleware Tab	Cross-language client SDKs with support for programming languages including but not limited to Java, C, C++, C#, Ruby, Perl, Python, PHP, and VB6.	Assume Cross Language SDKs are required to develop microservices? Are you looking to modernize WebSphere Application Server Services to microservices on Kubernetes Environment?	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

9	Volume II	Annexure J Middleware Tab	Support for multiple messaging protocols including OpenWire, STOMP, AMQP, MQTT, and JMS.	Assume this requirement is for services running on WebSphere Application Server. Please confirm ? Also, Please specify the number of interfaces using these messaging protocols in current environment	There is no middleware being used currently for POSB. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

10	Volume II	Annexure J Middleware Tab	Support for pluggable transport protocols such as In-VM, TCP, SSL, NIO, UDP, multicast, JGroups, and JXTA.	Assume, this requirement is for services running on WebSphere Application Server. Please confirm? Also, if you can specify if you are willing to use it in microservices ?	Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11	Volume II	Annexure J Middleware Tab	The ESB shall allow integration with multiple programming environments, including Java, .NET (C#, VB, F#, etc.), PHP, ESQL, and C++.	Is there any requirement to run PHP In ESB or Can it be removed ?	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

12	Volume II	Annexure J Middleware Tab	Guaranteed and assured message delivery.	It seems there is requirement for IBM MQ. Can you please specify if you have MQ or needs to be supplied as part of middleware? If needs to be supplied then please specify the number of interfaces which will depend on MQ with approximate size of message	Bidder to propose.

Response to the Pre-Bid Queries

13	Volume II	Annexure J API Gateway Tab	It shall support active-active clustering to provide high availability and resiliency.	Assuming Active-Active DR is required and High Availability is being considered through Container native solutions ? Please confirm	Active-Passive clustering at Data Centre (DC) and Disaster Recovery (DR) sites.

Response to the Pre-Bid Queries

14	Volume II	Annexure J API Gateway Tab	Support for runtime policy enforcement, circuit breakers, hard timeouts, service discovery, and load balancing of microservices is required.	Do you need to implement circuit breaker on API Gateway ? Can you please explain the use case of Circuit breaker ?	To prevent a falling service from being overwhelmed by further requests, the API Gateway should be able to trip the circuit breaker in the event of a service failure.

Response to the Pre-Bid Queries

15	Volume II	Annexure J API Gateway Tab	It shall enable bi-directional data format conversion between multiple widely used formats such as ISO, JSON, XML, CSV, and flat files.	Can the conversion be achieved using ESB as supplementary tool for some complex scenarios?	Bidder to propose the solution to meet the requirements.

Response to the Pre-Bid Queries

16	Volume II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	Since the Middleware Server used as WebSphere Application Server along with ESB- (TIBCO). Can you please share the number of interfaces implemented on WebSphere Application Server and TIBCO separately?	Tibco is not used in the POSB IT system. There is no middleware being used currently for POSB.

Response to the Pre-Bid Queries

17	Volume II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	There are single specifications given for Middleware. Can you please help me with ESB Particulars?	As per RFP

Response to the Pre-Bid Queries

18	Volume I	Section 5.20, Page 98	Form A 20	Can the Manufacturers'/ Producers' Authorization Form be submitted in Standard OEM format	MAF has to be submitted as per RFP prescribed format. OEM format shall be considered only if all the prerequisites of the RFP MAF format are covered therein.

Response to the Pre-Bid Queries

19	Volume II	Section x, Page 38	Reports	We understand that data lake house setup is out of the scope for this RFP	Data lake house setup is not in scope. Bidder shall integrate with DoP implemented central data lakehouse.

Response to the Pre-Bid Queries

20	Volume II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	The Environments are not defined in Scope and Compliance Sheet. Do you require separate Environment for all these multiple Environments ?	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

21	Volume II	Annexure J Middleware Tab	Environments are not defined	Can I assume the environment similar to API Gateway tab? If yes, then can you please specify the TPS required for ESB	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

22	Volume II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	Can you please define TPS for these environments separately?	Bidder to propose

Response to the Pre-Bid Queries

23	Volume II	Annexure J API Gateway Tab	Facilities for seamless integration with developers' IDEs and support for issue resolution workflows must be provided.	Can you please specify the workflows for issue resolution in IDE? Do you mean API Debugging ?	The clause refers to support for API development, testing, troubleshooting, and issue resolution through integration with developer tools and lifecycle systems. It does not specifically mandate IDE-based debugging workflows.

Response to the Pre-Bid Queries

24	Volume II	Annexure J API Gateway Tab	Compliance with relevant regional, national, and international regulations such as the Reserve Bank of India (RBI) guidelines, ISO 27001, Financial Data Exchange (FDX), and data privacy laws including the Indian Personal Data Protection Bill (PDP Bill) shall be ensured.	This requirement should be for complete API Solution instead of just API Gateway. API Gateway may work with other products to implement these framework. Can you please update the statement according to API Gateway as API Gateway only store information as defined by the solution	This requirement is applicable for the entire RFP.

Response to the Pre-Bid Queries

25	Volume II	Annexure L Container mgmt	The container platform should be one that provides a developer portal, plugins, middleware and inbuilt integrated IDE for developers to easily work on the same container platform to bring consistence and faster application lifecycle.	There is a separate requirement of middleware in the rfp with API gateway and ESB. Are you also planning to leverage a separate middleware of the container platform?	The reference to “middleware” in the container platform clause is intended to denote platform-embedded capabilities (such as plugins, integrations and developer services) that improve the developer experience and application lifecycle on the container platform. The RFP requirement for middleware (API gateway and ESB) should be treated as an independent enterprise integration and API management layer. Bidders shall propose: The container platform's native middleware features to enhance developer productivity, and A separate middleware solution (API gateway and ESB) to meet the dedicated middleware requirement, provided that the proposal clearly distinguishes between the container platform capabilities and the standalone middleware components.

Response to the Pre-Bid Queries

26	Volume II	Annexure B	Microsoft Biztalk	Assuming all Biztalk interfaces can be migrated or modernized to new ESB Solution. Please confirm?	As per RFP

Response to the Pre-Bid Queries

27	Volume II	Infra- Software Pg 238	IBM WebSphere Application Server Network Deployment	Are you looking to modernize WASND runtime?	As per RFP

Response to the Pre-Bid Queries

28	Volume II	Annexure L Container mgmt		What is the total worker node core that you are expecting for container mgmt platform to manage?	Bidder to propose.

Response to the Pre-Bid Queries

29	Volume II	Annexure J Archival	SI must include and provide the Solution capacity sizing, which shall include sizing for Hardware and Software based on the requirement in Annexure- Bill of Material (BoM). For the Database, DoP shall provide Oracle licenses, and SI need not factor the cost for the database licenses.	Should Database not be considered for any of the module mentioned in the RFP? Will this be taken care by DoP?	Bidder to propose all components to effectively run and manage the solutions proposed as part of this RFP. The Oracle DB Licenses are for RISC servers catering to CBS. Bidders may refer to the Corrigendum for more details.

Response to the Pre-Bid Queries

30	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 1. Network Security	Furthermore, the framework requires specialized Operational Technology (OT) Security for industrial assets	Is the requirement for a separate IAM setup for the OT environment? If yes, please provide the following details: 1. Is there a separate air gapped Ot environment in POSB's environment for which a separate IAM setup is needed? Or does the POSB intend to leverage a central IAM setup for both IT and OT assets? 2. What are the use cases that are needed to be implemented for IAM in the OT environment? For e.g. JML automation, SoD, strong authentication, privileged access management, remote privileged access etc.) 3. Please provide the count of users for the following: a. Admin users b. Non-admin users/end users c. non-human privileged identities 3. What are the different OT assets to which the access has to be secured? SCADA/HMI/PLCs etc.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements..

Response to the Pre-Bid Queries

31	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 4. Identity Management	The solution is required to provide a comprehensive Identity & Access Management (IDAM) system to govern user identities.	Please provide the following details: 1. Count of users: a. Internal users/Employees b. External users (third party/contractors etc.) 2. Are there any legacy/in-house developed applications? Do these applications expose any APIs? If no, then do these applications support SCIM for provisioning/deprovisioning? 3. What is the authoritative source for the user identities? 4. What are the use cases that are needed to be implemented for identity management: For e.g. - a. User lifecycle management b. role based/attribute based access control c. role optimization d. access recertification campaigns e. role based/business activity based separation of duties f. access provisioning/deprovisioning to hosts, etc.	Details of existing setup: 1)a)DOP Users: 25 b)Vendors : 160 2) No 3) FS Division 4) User provisioning and lifecycle - Password management - Role based access control - Access provion/deprovision

Response to the Pre-Bid Queries

32	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 4. Identity Management	To balance security with user experience, the framework must support Single Sign-On (SSO) for seamless access across platforms, reinforced by Multi-Factor Authentication (MFA) to ensure robust identity verification before granting access.	1. What are the directories that POSB is currently using? AD/LDAP/databases etc. 2. Does POSB need to provide Federation as part of SSO/MFA? 3. Please provide the count of users: a. internal users b. external users (third party/customers) c. customers 4. Is API authentication to be implemented? 5. Is the solution expected to support consent management for consumers?	Currently POSB is using Fincore SSO. Bidder to propose for 4. and 5.

Response to the Pre-Bid Queries

33	Volume II	Annexure N - MFA & SSO, Item No. 21	Solution should be able to provide an option to enforce capturing of each step taken during a web session for selected users, without changing the code of the application, for audit purposes at least 50 license only.	Please confirm if this capability is required to be users for admin users only	For admin user only. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

34	Volume II	Annexure N - MFA & SSO, Item No. 22	Solution should allow captured recording to be filtered by type of actions without changing the code of the application	Please confirm if this capability is required to be users for admin users only	For admin user only. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

35	Volume II	Annexure N - MFA & SSO, Item No. 23	Solution should allow captured recordings to be searchable by keyword or date without changing the code of the application	Please confirm if this capability is required to be users for admin users only	For admin user only. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

36	Volume II	Annexure N - MFA & SSO, Item No. 35	Proposed services and sub-processors must be hosted in India for customer data protection	Does POSB want an on-prem solution for SSO/MFA or is looking for a SaaS based solution for this?	All solutions should be on-prem unless explicitly stated otherwise.

Response to the Pre-Bid Queries

37	Volume II	Annexure N - PAM, Item No. 3	Vendor must to rotate password, support authentication against AD,run account discovery and also function as RDP and SSH jumphost with ONLY ONE windows service.	Is there any specific need for mandating a single windows service or is the requirement just to simplify management of privileged access across all endpoints?	As per RFP

Response to the Pre-Bid Queries

38	Volume II	Annexure N - PAM, Item No. 10	The proposed solution must support but not limited to the major types of accounts for password changing out-of-the-box. Active Directory (All Account) Windows Local User & Administrative Accounts Linux Local User & Administrative Accounts (Any Distribution) Unix Local Users & Administrative Accounts (Any Distribution) Network System Accounts Out-of-Band Management Systems AWS IAM Access Keys MS Azure Office 365 SSH Keys Database Accounts LDAP Accounts.	Please provide the following details on the AWS IAM and SSH Keys: 1. Does POSB want the solution to act as a certificate authority for the AWS IAM keys and the SSH keys? 2. If yes, please provide the number of applications/clients that need access to these keys 3. Does POSB require the proposed solution to generate new keys as part of credential rotation? Or does the new key generation need to be handled by AWS IAM/POSB's Certificate Authority? 4. If POSB's existing Certificate Authority is to be leveraged, please share its name and version details.	The revised clause to be read as: The proposed solution must support but not limited to the major types of accounts for password changing out-of-the-box. Active Directory (All Account) Windows Local User & Administrative Accounts Linux Local User & Administrative Accounts (Any Distribution) Unix Local Users & Administrative Accounts (Any Distribution) Network System Accounts Out-of-Band Management Systems Database Accounts LDAP Accounts. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

39	Volume II	Annexure N - PAM, Item No. 102	Solution must support real-time reputation checking	Please elaborate on what do you mean by reputation checking	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

40	Volume II	Section 6.7 / Pg135/ 6.7.1	6.7.1	No.of Users for L1, L2, L3	As per RFP

Response to the Pre-Bid Queries

41	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Leverage AI/ML techniques with no-code/low-code interfaces, enabling business users and data scientists to develop and refine fraud detection models.	Does DoP expect business users to independently configure and retrain fraud models using no-code/low-code interfaces, or should such activities be restricted to SI or data-science teams? If yes then please confirm on the number of such developers from DOP.	The solution should provide no-code/low-code capabilities with appropriate role-based access controls. Bidders to size and propose for number of developers. Bidders to provision for 15 DoP Business users.

Response to the Pre-Bid Queries

42	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Support real-time case management features, including alert assignment, prioritized queues, case notes, attachments, escalation, reminders, and reporting.	DoP is expecting a full-featured case management system with configurable workflows, SLAs, escalations and document management system. Please confirm	As per RFP

Response to the Pre-Bid Queries

43	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	We understand that DoP expects EFRM reporting to be delivered via an embedded reporting layer, which should be a part of the overall solution. Please confirm	Bidder to propose.

Response to the Pre-Bid Queries

44	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm average and peak daily transaction volumes across all channels to enable accurate sizing of real-time fraud detection infrastructure.	Bidders may refer to the Corrigendum for more details.

Response to the Pre-Bid Queries

45	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Please indicate expected daily fraud alert volumes and number of concurrent investigation users for case management sizing(workflow management)	The solution should be scalable to handle the fraud alert volumes. SI to size for 50 concurrent users.

Response to the Pre-Bid Queries

46	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	What is the historical data window in years or TB expected to be provided for fraud model training and back-testing?	EFRM solution is not implemented. Bidder to analyze the given information.

Response to the Pre-Bid Queries

47	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm the expected number of dashboards, & reports to be created as a part of the solution	Approx 50 reports.

Response to the Pre-Bid Queries

48	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm on the total number of viewers, users, editors and administrators of such reports	Approx 250 viewers, 50 concurrent users and 15 administrators.

Response to the Pre-Bid Queries

49	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Incorporate continuous model lifecycle management, including development, deployment, monitoring, model governance, retraining, and scorecarding.	If AI/ML or Generative AI solutions are proposed, are there any specific governance, explainability, auditability or model-risk requirements expected by DoP beyond standard RBI, CERT-In and DPDP compliance?	Bidders to ensure compliance with RBI, CERT-In and DPDP and any other statutory and regulatory guidelines as applicable.

Response to the Pre-Bid Queries

50	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Does DoP intend to standardize document management, records retention and audit evidence on a centralized Enterprise Content Management (ECM) platform and scanning solution(for physical documents), or should existing document repositories continue without transformation? If a new solution is needed, kindly confirm on the average number of documents to be digitized and number of concurrent users for the platform.	Bidder to propose. Number of users is given in #48.

Response to the Pre-Bid Queries

51	Volume II	Section 5.2.5, Page number 116, Clause number NA	Application Development & Integration of new functionalities	For use cases involving forms, certificates, KYC documents or regulatory submissions, should the solution propose ntelligent Document Processing (OCR + AI classification and extraction) capabilities. If yes, then please confirm the average document volume to be extracted in a year.	Bidder to propose.

Response to the Pre-Bid Queries

52	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm the expected no. of machine learning or scoring models that will be deployed for the solution	The bidder shall ensure adequate model coverage for real-time and near real-time fraud detection across all identified fraud risk scenarios, including but not limited to transaction fraud, account takeover, mule activity, anomalous behavior, and channel-specific threats, etc.

Response to the Pre-Bid Queries

53	Volume II	Section 5.2.5, Page number 115, Clause number 5.2.5.9 EFRM	Rule Management and Scenario Tuning	Pleasee confirm on the concurrent number of rules which can be triggered for seamlessly running the various transactions related to eFRMS.	Bidder to propose as per the requirements given in the RFP.

Response to the Pre-Bid Queries

54	Volume II	Annexure N / Database Activity Monitoring	Solution should provide functionality to test policies before enabling	Ideal method to test security policies are in UAT enviornment and not on production setup , it is thus requested to remove the clause and leverage UAT for testing purpose	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

55	Volume II	Annexure N / Database Activity Monitoring	The solution should have an agentless DAM architecture that can monitor database activity without the need for deploying agents on the database servers or enabling native logging eliminating performance impacts on database.	We understand the expectation is to have solution which support both agent based and agent less solution. Since one method is required atleast for collection or generation of logs	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

56	Volume II	Annexure N / Database Activity Monitoring	The solution should be able to integrate with the existing Data Activity Monitoring and Governance solution into a consolidated dashboard.	Dam solution allow forwarding security logs to technology such as siem and ticketing solution to help in overall security monitoring and governance. Hope the same is acceptable to the client.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

57	Volume II	Annexure N / Database Activity Monitoring	The proposed consent management solution should be capable of being deployed On-prem.	Consent management is not part of the DAM solution it is thus requested to move this clause to the relevant solution such as IAM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

58	Volume II	Annexure N / Database Activity Monitoring	The solution SAAS platform should be hosted in India.	The RFP talks about On-prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

59	Volume II	Annexure N / Database Activity Monitoring	The SAAS platform must be SOC2 type 2,SOC type 3, ISO/IEC 27001:2022, 27018:2019 and 27017:2015 compliant	The RFP talks about On-prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

60	Volume II	5.1.2.3 Transition of Applications. Page 27	• Finacle Core Banking Solution (CBS) v10.2.13 and all associated customisations and interfaces. • Internet Banking, Mobile Banking, and other POS channel integrations. • Allied enterprise applications, Risk-Based Authentication (RBA), AML/CFT solution, Aadhaar Data Vault and eKYC, Cheque Truncation System (CTS), Middleware solutions, APIs, and batch processing systems.	Please confirm if PLI is under the scope of this RFP, as PLI is not specifically mentioned.	PLI application is not under the scope.

Response to the Pre-Bid Queries

61	Volume II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if the existing hardware will be used while performing the upgrade and during parallel run	Bidder to size and provision hardware accordingly, based on the details given in the RFP and corrigendum.

Response to the Pre-Bid Queries

62	Volume II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if PLI Application will also be part of this application upgrade. Since PLI is running on EOSL hardware, upgrade of hardware may require PLI application upgrade also, please confirm if PLI application version is EOSL or not, if under mainstream support, will it support the upgraded hardware.	Refer #60

Response to the Pre-Bid Queries

63	Volume II	Bill of Quantity, 1. Compute, Page 212	SI No 15 to 42, IBM Power Systems 780 & HMC - CR7 are EOSL	Please confirm if this hardware is under this RFP Scope & will be considered as part of SLA defined in this RFP as these are already EOSL hardware	As per RFP

Response to the Pre-Bid Queries

64	Volume II	7. Physical Server Details, Page 239	SL no - P780 - AMC Validity Status - 29-09-2026	AMC Validity Status for P780 is not matching with AMC Date specified on Page 212. Please confirm the correct AMC Vailidity Date. Please confirm the AMC type - Best Effort/Non SLA Based or Mainstream support as EOSL is already bypassed	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

65	Volume II	Annexure H – Specification of Existing Racks, Page 254	<<General Query>>	Please confirm the availability of Free Rack Space, PDU points & Power, incase any additional hardware needs to be provisioned during Track 1 in existing DC, especially during Finacle Upgrade	Currently, three (3) rack spaces are available across different rows within the existing Data Centre. These racks are provisioned with single-phase power supply. The existing cooling infrastructure is assessed to be adequate to support ongoing DC operations. Bidders may refer to the Corrigendum for more details.

Response to the Pre-Bid Queries

66	Volume II	5.1.4 Operations and Maintenance of Existing Applications	The entire system should meet the requirements detailed in the RFP. It should also meet the expected performance levels and desired uptime as per Section 5 – Service Level Agreement, with respect to various fault tolerance/DR practices envisaged in the RFP. With reference to this, below are the key requirements:	Please confirm if all applications will be under this RFP Scope & will be considered as part of SLA defined in this RFP, especially if any application (or hardware they are running on) are already EOSL.	As per RFP

Response to the Pre-Bid Queries

67	Volume II	ii. System Support	h. The SI shall be responsible for fixing all bugs and program errors, whether identified by DoP or detected by the SI during testing, operations, or monitoring — across both existing and newly developed modules.	Please confirm the scope and SLAs incase the application is running with EOSL version or running with hardware with EOSL, where OEM doesn't extend mainstream support	As per RFP

Response to the Pre-Bid Queries

68	Volume II	2.24 Procurement through Local Suppliers (Make in India)	<< General Query >>	Please provide exception for IBM Hardware (Power Systems) as DOP is already using Power Systems	No exception for any particular component. Bidder has to comply with Make in India Regulations as applicable on the Total Contract Value.

Response to the Pre-Bid Queries

69	Volume II	C. Ongoing Support Services, Page 45	10. The incumbent vendor, HPE, is currently responsible for the Operations and Maintenance of certain common infrastructure and security solutions deployed at the existing DC/DR locations, which are shared between POSB and PLI. The SI shall work in conjunction with HPE to maintain the existing IT infrastructure and services specific to POSB till the new DCF is setup and operational, post which the SI shall be responsible for providing the same as mentioned in the RFP. The details of the common solutions are listed in Annexure B.	Please clarify this point. If PLI is not under scope of this RFP, then how the shared resources will be divided between POSB & PLI	Refer #60

Response to the Pre-Bid Queries

70	Volume II	5.2.4 Detailed Scope of Work, Page 82	22. The SI is required to follow the below matrix for installing the application instances in DC, DR and NDR environments within the infrastructure.	Please confirm the current availability of - Development/SIT/PREPROD of CBS Resources in DC - Training/PREPROD/UAT of CBS Resources in DR	Bidder to analyze from the information given in RFP/Corrigendum.

Response to the Pre-Bid Queries

71	Volume II	Annexure L - RISC Server	Minimum one RISC processor module with 60 active compute cores, supporting simultaneous multithreading and hardware accelerators for encryption, compression, and isolation.	Please clarify if the server is asked with Single socket of 60 Cores or 60 Cores can be spread on multiple sockets but part of Single Unit/Module. Please change the word "hardware accelerators" with "hardware based capability for encryption & isolation"	The requirement is for a minimum of 60 active compute cores within a single processor module/unit. These cores may be provided on one or more sockets, provided they are part of the same physical module/chassis and are managed as a single logical unit as per the OEM's standard design. The revised clause to be read as: "Minimum one RISC processor module with 60 active compute cores, supporting simultaneous multithreading and hardware-based capability/accelerators for encryption, compression and isolation." The functional requirement for hardware-based offload/acceleration remains unchanged. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

72	Volume II	Annexure L - Server Rack	42U - Rack should be 800mm (Width) x -1200mm (Depth).	Please change this creteria to include 600 mm or more as width as certain manufacturers build compact rack to optimize space requirements	As per RFP

Response to the Pre-Bid Queries

73	Volume II	Annexure L - Server Rack	The 19" mounting angles should be provided 2 Nos. on the front and rear sides of the Rack. It should be adjustable full depth. 19" Mounting Angles made up of Steel 2mm Thickness, with better mounting flexibility and maximises usable mounting space.	Please remove the Point - "It should be adjustable full depth."	As per RFP

Response to the Pre-Bid Queries

74	Volume II	Annexure L - Server Rack	Each rack should have a provision for a horizontal cable manager.	Please remove this point as cable managers are usually provided alongwith component being installed based on specifications	Bidders may propose either rack-supplied cable managers or equivalent integrated cable-management accessories, but each rack must support and be supplied with at least one horizontal cable manager Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

75	Volume II	Annexure L - Server Rack	The Hexagonal Perforated Dual Rear Door will be Lockable, and a 3 Point Lock should be provided.	Please allow single Rear Door also with Lock & Key	The clause to be read as: “Provide perforated lockable rear door(s) with at least 80% perforation and a multi-point or equivalent locking mechanism.” Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

76	Volume II	Annexure L - Server Rack	Rack should be Castor wheels 4 Nos. (i.e. 2 front wheels with brake and 2 rear without brake) with adjustable levellers. The rack shall not have an External height >1991mm, including levelling legs and Castors.	Please allow External Hieght > 2050mm, wheels without brake (considering mechnism which restricts rack movement)	As per RFP

Response to the Pre-Bid Queries

77	Volume II	Annexure L - Server Rack	Minimum 2 × enterprise SSD (hot-plug) in RAID 1 or OEM-equivalent mirroring.	This point is contradictory with Point 5. Latest Generation Servers are equipped with NVMe Disks. Please delete this point as the requirement is fulfilled in Point 5 already	Revised clause to be read as: "Minimum 2 × enterprise-grade SSD (SAS/SATA or NVMe), hot-plug, configured in RAID 1 or OEM-equivalent mirroring for OS boot." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

78	Volume II	Annexure L - Server Rack	Integrated/optional RISC-compatible controller supporting RAID 0/1/5/6/10 or OEM equivalent.	NVMe protocol is PCI based protocol & doesn't support RAID, therefore change "RAID 0/1/5/6/10" to "OS Mirroring"	Revised clause to be read as: "Where SAS/SATA drives are used, an integrated/optional RAID controller shall support RAID 0/1/5/6/10 (or higher levels such as 50/60). Where NVMe boot disks are used, equivalent OS- or OEM-based mirroring shall be provided." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

79	Volume II	Annexure L - Server Rack	Server should have below security essentials and certificates: • shall include FIPS 140-2, TPM 2.0 v5 & UEFI with secure boot. • cryptographically verified trusted booting standards meeting basis NIST SP 800-147B, BIOS Integrity measurement proposed guidelines basis NIST SP 800-155, protection standards meeting NIST SP 800-193 and standards & secure media sanitization standards meeting NIST SP 800-88. • real time firmware security scanning to protect against firmware which executes before the OS boots. • maintain repository for firmware and should be able to rollback, if required. • configuration upgrades should be only with cryptographically signed firmware and software from the server OEM. • End-to-end supply chain controls to ensure component integrity, security, and vendor responsibility. • Secure Erase • Data at Rest Encryption (SEDs with local or external key mgmt) • Chassis Intrusion Detection • Server OEM Security bezel with lock function • CNSA • ASHRAE A3/A5	Please review these points as some of these points are either related to OEM Specific or Storage related like Data at Rest Encryption is storage term & chassis Intrusion Detection is more related to Blade/Chassis Servers. Please either delete this point or limit to standard RAS/security features like Quantum safe encryption etc.	The revised clause is read as: "Server should have below security essentials and certificates: 1. FIPS 140-3 validated cryptographic modules. 2. TPM 2.0, UEFI Secure Boot, NIST SP 800-147B/155/193 and 800-88 aligned controls 3. Secure erase, support for SEDs where used, 4. firmware integrity with signed updates and rollback. 5. supply-chain security 6. chassis intrusion detection 7. lockable front bezel 8. ASHRAE A3/A4/A5 compliance." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

80	Volume II	Annexure L - Server Rack	Integrated service processor with remote console; local VGA/DP/HDMI as supported.	Please add local with RJ45 connectivity also	The revised clause to be read as: “Integrated service processor with remote console, local VGA/DP/HDMI as supported, and a dedicated RJ-45 management port.” Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

81	Volume II	Annexure L - Server Rack	OEM need to submit latest and valid FCC Class A, Energy Star, CE Certification, OEM, BIS Certificate	Please allow some of them to be submitted incase any such is not valid for specific OEM/Country of Origin	The revised clause to be read as: "The OEM shall provide current and valid FCC Class A, Energy Star, CE, and BIS certifications for the offered server model, as applicable to both the country of origin and the country of destination. If any particular certification is not required or not applicable, the OEM shall instead provide an equivalent certification recognized in the relevant country, together with supporting documentation demonstrating compliance with Indian requirements" Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

82	Volume II	Annexure L, Page #- 260, Tape Library	Enterprise-class, rack-mountable, LTO-9 or higher, SAN integration	Enterprise class library consist of Drives & Slots in a Frame based architecture rather than rack-mountable design. Also, LTO 10 is the latest drive available in the industry. Request you to kindly amend this clause as "Enterprise-class, Frame based library, LTO-10 or higher, SAN integration"	As per RFP

Response to the Pre-Bid Queries

83	Volume II	Annexure L, Page #- 260, Tape Library	Native read/write speeds as per LTO gen; Data Rate Matching	Data Rate matching (DRM) terminology is for specific OEM, We offer "Speed Matching" Technique to achieve the same functionality. Request you to kindly amend this clause as "Native read/write speeds as per LTO gen; Data Rate Matching/Speed Matching"	The revised clause to be read as: Native read/write speeds as per LTO gen; Adaptive Tape Speed (ATS). Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

84	Volume II	Annexure L, Page #- 260, Tape Library	High-availability robotic subsystem; dual accessor preferred	Enterprise class library benefits with Dual accessor/robotics in terms of High Availability as well as load sharing. Keeping it is as "preferred" encourage the bidder to quote with single accessor. Request to amend this clause as "High-availability and load sharing robotic subsystem with dual accessor and dual gripper on each accessor "	As per RFP

Response to the Pre-Bid Queries

85	Volume II	Annexure L, Page #- 260, SAN Storage	Storage solution should provide the native capability to replicate data of existing storage between DC, DR and NDC without using any additional Hardware and software.	As per the industry standard, Same family of Storage can replicate with each other or must require additional Hardware or software for the same. Request you to kindly amend this clause as "Storage solution should provide the capability to replicate data of existing storage between DC, DR and NDC. If any additional Hardware and software required to achieve this capabilities shall be included in the solution."	The revised clause to be read as : Storage solution should provide capability to replicate data of existing storage between DC, DR and NDC with/without using any additional Hardware and software. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

86	Volume II	Annexure L, Page #- 260, SAN Storage	SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage without using external/3rd party hardware or Software.	Migration of data from existing storage to new storage would require to follow certain process and tools. Request you to kindly amend this clause as "SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage. ."	The revised clause to be read as :- SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage. Any required tools or software shall be included in the proposed solution. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

87	Volume II	Annexure L, Page #- 260, SAN Storage	Storage must be scalable to at least double capacity without adding any additional controllers with the same set of drives and RAID.	Base Controller enclosure has certain number of NVMe drives that saturate the performance of a storage and increasing the number of drives beyond base Controller enclosure would not help in linear capacity and performance increment. Also, Storage solution support Scale-out design that anyways help to increase the capacity. and performance by adding additional pair of controllers. Request you to kindly amend this clause as "Storage must be scalable to at least double capacity by adding any additional controllers with the same set of drives and RAID. "	As per RFP

Response to the Pre-Bid Queries

88	Volume II	Annexure L, Page #- 260, SAN Storage	The storage solution should be supplied with a three-phase power supply connectivity.	Power supply configuration depends on the storage power consumption and configuration. Request you to kindly amend this clause as "The storage solution should be supplied with a single-phase or three-phase power supply connectivity. . "	As per RFP

Response to the Pre-Bid Queries

89	Volume II	Annexure L, Page #- 260, SAN Storage	The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture with cache across configured controllers.	Each drive has only 2 physical ports that can connect to 2 controllers only that can work in HA mode by mirroring the cache of between 2 controllers. Spreading cache across more than 2 controllers would require to do cache virtualisation that will lead to cache coherency and reduce the performance drastically along with increase in the complexity of solution. Request you to kindly amend this clause as "The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture. "	The revised clause to be read as : The Storage system should be the latest generation Enterprise Storage product providing enterprise class data availability , end to end NVMe support and supporting zero data loss 3-way DR replication . Proposed storage must be an active-active multicontroller, scale up and scale out architecture. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

90	Volume II	Annexure L, Page #- 260, SAN Storage	The proposed Storage System should be Unified Storage (Block & File), capable of delivering 99.9999% uptime, with no single point of failure for active/passive components, supporting Block & File on a single platform with common management or redundant gateways.	We understand that the existing Storage is SAN storage which is meant for high performance. As per the best practice for core banking solution, SAN Storage is the preferred storage while for unstructure data for some other application can be storage on separate NAS/File storage. Keeping both SAN & NAS on same controller or stoarge would lead to no special benefit rather it lower the performance and increase complexity. Request you to kindly amend this clause as "The proposed Storage System should be SAN Storage, capable of delivering 99.9999% uptime, with no single point of failure for active/passive components"	As per RFP

Response to the Pre-Bid Queries

91	Volume II	Annexure L, Page #- 260, SAN Storage	Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes.	There are multiple type of NVMe drives available in like SLC, MLC, TLC, QLC with their own pros and cons in terms of performance and reliability. NVMe TLC has standard performance and Reliability as it supports 3-4K P/E Cycle while IBM invented their own NVMe drives (or Computational storage device) with leading chip manufacturer "Micron" that is know as FCM (FlashCore Module) that has P/E cycle of 15K i.e. ~5X better than traditional NVMe TLC drive with higher capacity of 9.6TB, 19.2TB & 38.4TB. Request you to kindly amend this clause as "Must support dual-port NVMe SSDs for not more than 40TB and mixing of drive sizes shall be possible."	As per RFP

Response to the Pre-Bid Queries

92	Volume II	Annexure L, Page #- 260, SAN Storage	Must support unified Block & File protocols (FC, iSCSI, NVMe-oF, NFS). In the absence of a native file, a redundant NAS gateway must be provided.	We understand that the existing Storage is SAN storage which is meant for high performance. As per the best practice for core banking solution, SAN Storage is the preferred storage while for unstructure data for some other application can be storage on separate NAS/File storage. Keeping both SAN & NAS on same controller or stoarge would lead to no special benefit rather it lower the performance and increase complexity. Request you to kindly amend this clause as "Must support SAN Block protocols (FC, iSCSI, NVMe-oF).	As per RFP

Response to the Pre-Bid Queries

93	Volume II	Annexure L, Page #- 260, SAN Storage	The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 256GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall dynamically support read and write i/o	As per the asked performance in Point no.1 i.e. 3 Lac scalable to 5 Lac can be easily maintained with Dual controller with all the consideration asked in the RFP in cost-effective way. Min. 4 controllers will increase the commercials as well as complexity to manage the same. Also, Cache for NDC site should be at least 25% of DC that too DRAM as in industry SSD Cache or PMEM is also available which is not true cache rather just a standard Flash drive that act as Cache and not recommended for CBS or critical applications. Request you to kindly amend this clause as "The proposed storage system must be configured with minimum Dual Controllers & cache sizes of 2TB DRAM at DC and DR and 512GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall	The revised clause to be read as: Proposed solution should support minimum 2 controllers each site from day 1 and scalable upto 4 controllers within same storage array at each site. Cache sizes of 2TB at DC & DR respectively and 256GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall dynamically support read and write i/o . Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

				dynamically support read and write i/o ". 	

Response to the Pre-Bid Queries

94	Volume II	Annexure L, Page #- 260, SAN Storage	DC/DR: min 16x 32/64Gb FC ports, 16x 25GbE ports,. NDC: min 8x 32/64Gb FC, 8x 25GbE for ISCSI /NAS	We understand that the SAN Switch has been asked in the RFP which is meant for FC connectivity only and 25G iSCSI is not require in this case. Also, NAS shall not be the part of SAN Stoarge requirement as justified in above points. Request you to kindly amend this clause as "DC/DR: min 16x 32/64Gb FC port,. NDC: min 8x 32/64Gb FC.	The revised clause to be read as: DC/DR: min 16x 32/64Gb FC ports, 8x 25GbE ports, NDC: min 8x 32/64Gb FC, 8x 25GbE for ISCSI/NAS Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

95	Volume II	Annexure L, Page #- 260, SAN Storage	Must support NVMe backend with PCIe drive connectivity.	Base Controller enclosure has certain number of NVMe drives that saturate the performance of a storage and increasing the number of drives beyond base Controller enclosure would not help in linear capacity and performance increment. Also, Storage solution support Scale-out design that anyways help to increase the capacity. and performance by adding additional pair of controllers. Request you to kindly amend this clause as Must support SAN backend connectivity.	As per RFP

Response to the Pre-Bid Queries

96	Volume II	Annexure L, Page #- 260, SAN Storage	Must support 10/25GbE connectivity for replication (native or external). Any extra HW must be bundled.	Recommend to use FCIP router for better reliability and faster data replication as it uses WAN Optimisation. Hence 10/25G ports are not required. Request you to kindly delete this clause.	As per RFP

Response to the Pre-Bid Queries

97	Volume II	Annexure L, Page #- 260, SAN Storage	Must integrate with VMware, Nutanix, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible).	Nutanix is a HCI appliance that uses internal disk of node to create SDS layer and don't use external storage. Request you to kindly amend this clause as Must integrate with VMware, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible).	The revised clause to be read as: Must integrate with VMware, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible). Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

98	Volume II	Annexure L, Page #- 260, X86 server	Intel Platinum/ AMD processor @ 2.0 GHz or higher 64 Cores in 2 Sockets	As per the current clause, AMD has an edge to quote any series of processor while Intel has to quote Platinum mandatorily which is not a level playing field. Request you to kindly amend this clause as Intel / AMD processor @ 2.0 GHz or higher 64 Cores in 2 Sockets	The revised clause to be read as: "Intel or AMD server-class processors @ Minimum 2.0 GHz or higher, providing a total of at least 64 physical cores across 2 sockets." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

99	Volume II	Annexure L, Page #- 260, X86 server	2 TB DDR5 RAM- Minimum 32 DDR5 DIMM slots RDIMMS 8TB Max, supporting speeds of min 4800MT/s	2TB RAM would require 8 x 256GB capacity per DIMM from Day 1 while the supply of 256GB is limited and commercial high and considering 64GB capacity per DIMM would consume all 32nos. of DIMM slots and would have no further scope of increment of RAM Capacity. Hence scalability is not possible. Request you to kindly amend this clause as 2 TB DDR5 RAM- Minimum 32 DDR5 DIMM slots RDIMMS, supporting speeds of min 4800MT/s	The revised clause to be read as: "2 TB DDR5 RAM- Minimum 24 DDR5 DIMM slots RDIMMS, supporting speeds of min 4800MT/s with Headroom of expansion" Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 0	Volume II	Annexure L, Page #- 260, X86 server	Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS doesn't work on Raid card and hence not applicable for SDS solution. Request you to kindly amend this clause as Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60 (Not applicable in case of SDS)	The revised clause to be read as: "Integrated/PCIe 4.0 or 5.0 SAS RAID Controller with 12 Gb/s or 24 Gb/s SAS, 8 GB cache, supporting RAID 0, 1, 5, 6, 10, 50, 60." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 1	Volume II	Annexure L, Page #- 260, X86 server	Dual Port 10/25 Gbps SFP+ SR ethernet adapter with minimum four SFP modules of 10Gbps and 25 Gbps each	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS require higher bandwidth. Request you to kindly amend this clause as Dual Port 10/25 Gbps SFP+ SR ethernet adapter with minimum four SFP modules of 10Gbps and 25 Gbps each (It should be Dual port of 100GbE in case of SDS Solution)	The revised clause to be read as: “Each server shall have at least one dual-port 10/25 GbE SFP+/SFP28 adapter with a minimum of four compatible SR transceivers. For nodes dedicated to SDS solutions, MSPs may propose higher-bandwidth adapters (e.g., dual-port 100 GbE) in addition to or in place of the 10/25 GbE adapter, as per SDS OEM sizing, provided the solution meets or exceeds the base requirement.” Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 2	Volume II	Annexure L, Page #- 260, X86 server	Dual port 64 Gbps Fiber Channel HBA	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and utilise internal drives only and hence not applicable for SDS solution. Request you to kindly amend this clause as Dual port 64 Gbps Fiber Channel HBA (Not applicable in case of SDS)	As per RFP

Response to the Pre-Bid Queries

10 3	Volume II	Annexure L, Page #- 260, X86 server	Integrated Graphics controller with at least 8MB of video frame buffer/ memory	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and utilise dedicated node of GPUs and hence not applicable for SDS solution. Request you to kindly amend this clause as Integrated Graphics controller with at least 8MB of video frame buffer/ memory (Not applicable in case of SDS)	As per RFP

Response to the Pre-Bid Queries

10 4	Volume II	Annexure L, Page #- 260, X86 server	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of NICs & system health	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS doesn't work on Raid card as well as External storage and hence not applicable for SDS solution. Request you to kindly amend this clause as Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of NICs & system health (RAID management, external storage management not applicable for SDS solution)	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 5	Volume II	Annexure L, Page #- 260, X86 server	The Offered server should have certification with latest OS version of Microsoft, VMWare, RHEL, UBUNTU and SUSE	We understand that the entire solution also include SDS (Software defined storage) and Virtualisation as well which will consume same x86 hardware and required these Host OS on either Bare metal or Virtualisation platform. Also, VMware is not OS rather its one type of Hypervisor layer. Request you to kindly amend this clause as The Offered server should have certification with latest OS version of Microsoft, RHEL, UBUNTU and SUSE as host OS in case of Bare metal OR Virtualisation platform.	The revised clause to be read as: "The offered server shall be certified with the latest supported versions of Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), Ubuntu and SUSE Linux Enterprise Server as host operating systems, and shall be listed on the Virtualisation Hardware Compatibility List (HCL) for the relevant ESXi versions where a virtualisation platform is proposed." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 6	Volume II	Annexure L, Page #- 260, SAN Director	The switch should support Virtual SAN and inter VSAN routing for sharing resources across VSAN. Switch should be able to deliver line-rate routing between any ports in a system or fabric without the need for external routing appliances.	Are we referring Vmware vSAN (SDS) here as it will limit the participations . Please clarify.	The revised clause to be read as: The switch should support Virtual SAN/fabric and inter VSAN/Line-rate routing for sharing resources across VSAN. Switch should be able to deliver line-rate routing between any ports in a system or fabric without the need for external routing appliances. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

10 7	Volume II	Annexure L, Page #- 260, Backup Solution	Disk-based backup appliances, SAN/NAS, VTL; Support for multi-site storage targets.	Tape library has been asked in the solution and that make recommended Backup strategy as D2D2T and hence VTL is not required. Request you to kindly amend this clause as Disk-based backup appliances, SAN/NAS, ; Support for multi-site storage targets.	As per RFP

Response to the Pre-Bid Queries

10 8	Volume II	Annexure L, Page #- 260, Backup Solution		DOP is already using IBM Storage protect backup perpetual licenses and all the backup is currently in its own format on tapes. Having different Backup solution procurement will lead to migrate all the existing data to new backup solution and also make commercial impact by not utilising the existing licenses. Request to kindly ask for additional capacity for existing licenses to avoid any migration efforts and economical solution.	Bidder to propose best solution , aligned with RFP functional and non-functional requirements.

Response to the Pre-Bid Queries

10 9	Volume II	Annexure J EMS	EMS must support Server Automation and Patch Management	Please provide the expectations/ requirements for server automation.	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 0	Volume II	Annexure J EMS	EMS must provide Centralised Log Management and a Unified Dashboard.	Our submission to please rephrase the clause as "EMS must provide Centralised Event Management and a Unified Event Dashboard."	As per RFP

Response to the Pre-Bid Queries

11 1	Volume II	Annexure J EMS	EMS OEM must be ISO 27034 certified; solution must have ISO 27001:2013 & ISO 9001 certification.	ISO27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. ISO 9001 certification validates an organization's ability to consistently provide quality products/services, meet customer needs, and adhere to regulations through a globally recognized Quality Management System (QMS) framework, enhancing efficiency, reducing errors, boosting customer confidence, and providing a competitive edge for businesses of any size or sector. However ISO 27034 is not OEM certifications as its provides only guidance to assist organizations in integrating security into the processes used for managing their applications. ISO27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

				Since this certification is for guidance only to assist the organisation who are running and managing the in house applications, they utilize the principles outlined within its broader security framework and offerings, particularly for application security management during their Software development Cycle (SDLC) but it's not mandatory for every OEM to certified their products under this certification. Our submission is to please rephrase this clause as : EMS OEM must have ISO 27001:2013 & ISO 9001 certification	

Response to the Pre-Bid Queries

11 2	Volume II	Annexure J EMS	EMS must support discovery mechanisms (Active Directory, DNS) and service discovery.	Our submission is to please rephrase the clause as "EMS should provide the ability to integrate with Active Directory and DNS and should provide the ability to monitor active directory as well."	As per RFP

Response to the Pre-Bid Queries

11 3	Volume II	Annexure J EMS	EMS must provide Runbook Automation, OOTB workflows (1000+), integration with CMDB, and intuitive workflow/dashboard creation.	While tools can provide OOTB workflows and also provide the capability to create new workflows; our submission is to remove the (1000+) as every customer environment is different and workflows should be designed and used as per the project requirement.	The revised clause to be read as: EMS must provide Runbook Automation, OOTB workflows based upon DoP requirement as much maximum, integration with CMDB, and intuitive workflow/dashboard creation. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 4	Volume II	Annexure J EMS	EMS must integrate with external systems (CyberArk, Systems Monitoring, RSA, PostgreSQL, Kerberos), support debugging, and process automation libraries.	Please provide the details of the systems monitoring tool to integrate with. Also, please share/ provide the detailed requirements/ expectation regarding each of the integrations asked within the clause.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

11 5	Volume II	Annexure J EMS	NMS must support wireless discovery, SD-WAN monitoring, security system monitoring, and telemetry-based data collection.	Please provide share OEM, Make and Model or Wireless Lan Controller.	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 6	Volume II	Annexure J EMS	NMS must support zero-touch automation via APIs, integration with NetDevOps (GitHub), and scheduled/ad-hoc scans.	Our submission is to please rephrase the clause as "NMS must support zero-touch automation via APIs/ scripts/ ansible playbooks, integration with NetDevOps (GitHub), and scheduled/ad-hoc scans." Please elaborate the requirement with a use case for integration with NetDevOps (Github).	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 7	Volume II	Page # 235 till 240	Annexure C – BoQ of Existing Licenses	We observed that many of the hardware's and Software's are out of AMC Support (31-Dec-2025) and we assume that AMC support will get extended by DOP on the existing Hardware's and Software's till the new solutions deployed . Please confirm the understanding.	Refer updated Infra details in Corrigendum. AMC support shall be extended by DoP wherever required. However, no EOL/EOSL hardware is to be used at new DCF.

Response to the Pre-Bid Queries

11 8	Volume II	Page # 227 till 230	Annexure B – Common Infra and Security solutions maintained by HPE	We observed that many of the hardware's are under EOSL and we assume that AMC support on these Hardwares will be taken care by DOP till the new solutions deployed . Please confirm the understanding.	Refer #117

Response to the Pre-Bid Queries

11 9	Volume II	Page # 231 till 234	Annexure B – Common Infra and Security solutions maintained by HPE	We assume Software's license utilization is within the available license count , this is to ensure the Software License Compliance. Please confirm the understanding.	As per RFP

Response to the Pre-Bid Queries

12 0	Volume II	Page # 231 till 234	Annexure B – Common Infra and Security solutions maintained by HPE	We observed that many of the Software Versions are bit older than to the latest Version and we assume that Software Version upgrades are not part of Scope . Please confirm the understanding.	As per RFP

Response to the Pre-Bid Queries

12 1	Volume II	Page # 218 till 221	3. Network:	We observed that many of the hardware's are under EOSL and we assume that AMC support on these Hardwares will be taken care by DOP till the new solutions deployed . Please confirm the understanding.	Refer #117

Response to the Pre-Bid Queries

12 2	Volume II	Page # 216	2. Storage:	We observed that storage components are out of AMC Support (30/08/2025) and we assume that AMC support will get extended by DOP on the existing storage components till the new solutions deployed . Please confirm the understanding.	Refer #117

Response to the Pre-Bid Queries

12 3	Volume II	Page # 212 till 215	1.Compute	We observed that servers are out of AMC Support (30/08/2025 & 31/12/2025) and we assume that AMC support will get extended by DOP on the existing Servers till the new solutions deployed . Please confirm the understanding.	Refer #117

Response to the Pre-Bid Queries

12 4	Volume II	Page # 209	Annexure A – Existing Infrastructure 2.Bandwidth Connectivity	We understand that , Network infrastructure is provided by NI and the same will be managed by DOP , Please confirm the understanding	Internet connectivity for WAN traffic and MPLS connectivity for data center locations should be provisioned by SI. It should be from two different service providers and shall be in Active-Active mode. The connectivity should be redundant from two different ISPs. Minimum MPLS & Internet links 2Gbps (each link), Replication link 1Gbps (each link). SI needs to size adequate network bandwidth as per their proposed solution which should be in-line with RPO/RTO requirements for replication of data among DC, NDC and DR sites. All the field locations bandwidth will be taken care by NI and managed by DoP. SI has to coordinate with NI for network connectivity and routing configuration.

Response to the Pre-Bid Queries

12 5	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	The proposed solution should support min 800+ OOB integration with 3rd party solutions and OOB Parser availability.	The proposed solution should support min 600+ OOB integration with 3rd party solutions and OOB Parser availability.	Bidders may refer to the Corrigendum Functional Requirements and the updated Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

12 6	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	Solution should be able to provide data visualization on a causality view page for raw telemetry on data models rules	Solution should be able to provide data visualization on a causality view page/dashboard for raw telemetry/event on data models rules. This Modification will allow good number of Participants	Clause is omitted. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

12 7	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	Solution should be able to advance to ML or Analytics to identify Logs where not collected from a data source for an abnormally long time	This Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Clause is omitted. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

12 8	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	The proposed solution shall have GUI based remote task manager as response capabilities. Live terminal should support features such as below : -File hash Information collection -Termination of the service -Download of binary -Addition of hash value to block list -Delete the file -Send the hash to get the verdict (TI integration) -Execute a python script -Execute a powershell script	This Compliance is specific to Core EDR feature , hence requesting DOP to delete this compliance from SIEM	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

12 9	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	Proposed solution should have capability to search and destroy to swiftly sweep across endpoint and eradicate threats.	This Compliance is specific to Core EDR feature , hence requesting DOP to delete this compliance from SIEM	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

13 0	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)	The proposed solution should support automatic collection of the following forensic information from windows/Mac machine for - further investigation purposes: Recent files (LNK files), Jump lists, OpenSavePidIMRU, ShellBags, WordWheelQuery, Amcache, Application Resource Usage (SRUM), Background Activity Monitor, CIDSizeMRU, LastVisitedPidIMRU, Prefetch, RecentFileCache, Shimcache, UserAssist, Windows Timeline, ARP cache, DNS cache, Hosts File, Network Connectivity Usage (SRUM), Network Data Usage (SRUM), Browser History (User), edirected or System generated traffic), Memory collection (Remote memory imaging & Full memory images including kernel memory, not just user-space)	This Compliance is specific to Core EDR feature , hence requesting DOP to delete this compliance from SIEM	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

13 1	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)		Kindly mention the EPS requirement and number of devices which needs to be integrated with proposed SIEM solution as no sizing parameters are mentioned in RFP.	As per RFP

Response to the Pre-Bid Queries

13 2	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)		The complete SIEM solution along with all its components like collectors and management servers should be on-premises and shall have ability to store the logs for a year as per Government guidelines.	As per RFP

Response to the Pre-Bid Queries

13 3	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Information and Event Management (SIEM)		The SIEM should provide a unified analytics interface that allows the same query language to analyse both log data and performance data inbuilt in the SIEM itself, without any 3rd party integration.	As per RFP

Response to the Pre-Bid Queries

13 4	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)		Kindly confirm number of concurrent analysts count required for SOAR solution with full read and write access with no limitation on number of actions/playbooks/connector s in a 24X7 SOC operations for POSB.	As per RFP

Response to the Pre-Bid Queries

13 5	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	The solution should support 800+ integrations out of the box. Integration packs should include pre-built usecases consisting of playbooks, automation actions, scripts that can be customised. The solution should have an integration store that is continuously updated with both OEM and Partner provided integration. Forensic tools, specify all products IT (e.g. AD, SAML...) Communication tools (e.g. email, Slack, Hipchat...) SIEM tools Endpoint Security Network Security Active Directory Threat Intelligence others	The solution should support 600+ integrations out of the box. Integration packs should include pre-built usecases consisting of playbooks, automation actions, scripts that can be customised. The solution should have an integration store that is continuously updated with both OEM and Partner provided integration. Forensic tools, specify all products IT (e.g. AD, SAML...) Communication tools (e.g. email, Slack, Hipchat...) SIEM tools Endpoint Security Network Security Active Directory Threat Intelligence others	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

13 6	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	Proposed solution should have built-in IDE that supports development of custom integrations via the console/UI and should support IDE plugins, SDK for rapid development.	This Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

13 7	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	The solution should have source code available for review for automations, playbooks, integrations	This Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

13 8	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	The solution should have a built-in credential manager for securely storing integration credentials. Credentials should be masked from view by admin and encrypted using AES-256 and hashed using SHA-512 as well as Bcrypt hashing algorithm.	This Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

13 9	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	The solution should map current and future CIRT processes and procedures to incident types	This Compliance is specific to OEM , hence requesting DOP to Change this compliance as below to have good Number of Participants " The solution should have integration to map current and future CIRT processes and procedures to incident types"	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

14 0	AnnexureN	SIEM, UEBA, SOAR, TI, NTA - Security Orchestration, Automation and Response (SOAR)	The solution should support sending out authenticated surveys to drive the investigation workflow	This Compliance is specific to OEM , hence requesting DOP to Change this compliance as below to have good Number of Participants " The solution should support sending out authenticated surveys/suggestions to drive the investigation workflow"	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

14 1	AnnexureN	External NGFW	NGFW Throughput (Application Visibility and Control/Application-Identification and Logging enabled considering webmix/appmix traffic flows): 50 Gbps or higher	Considering scalability of project and overall incoming volume it is recommended to have higher factored external firewall solution as 80 Gbps or higher from single appliance without any stacking/cluster solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 2	AnnexureN	External NGFW	NGTP Throughput (Enabling Firewall, IPS, URL filtering / Web Security Essentials, Application Control, Anti-Virus, Anti-Bot, DNS Security, Basic File Blocking and Logging enabled considering webmix/appmix flows): 30 Gbps or higher	Considering scalability of project and overall incoming volume it is recommended to have higher factored external firewall solution as 70 Gbps or higher from single appliance without any stacking/cluster solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 3	AnnexureN	External NGFW	Minimum Concurrent TCP Connections post enables Application Visibility and Control (AVC) or Concurrent http sessions: 500 million TCP or 5 million http	Minimum Concurrent TCP Connections post enables Application Visibility and Control (AVC) or Concurrent http sessions: 120 million at layer 4 or 40 million at layer 7 from single appliance without any stacking/cluster solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 4	AnnexureN	External NGFW	Minimum New TCP Connection per second post enable AVC or http sessions per second: 2,500,000 TCP or 250,000 http	Minimum New TCP Connection per second post enable AVC or http sessions per second: 900,000 at layer 4 or 400,000 at layer 7 from single appliance without any stacking/cluster solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 5	AnnexureN	External NGFW	10G RJ45 8 or higher	Requesting DOP to use 10G Fiber instead of copper	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 6	AnnexureN	External NGFW	10G SFP+ 10 or higher	Requesting to use 10G Fiber instead of copper as 10G SFP+ 20 or higher	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 7	Annexure N	External NGFW	There should have APT solution with following features:	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 8	AnnexureN	External NGFW	Cloud base unknown malware analysis service should be certified with SOC2 or any other Data privacy compliance certification for customer data privacy protection which is uploaded to unknown threat emulation and analysis	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

14 9	AnnexureN	External NGFW	Cloud base unknown malware analysis service should be able to perform dynamic threat analysis on such as EXEs, DLLs, ZIP files, PDF documents, Office Documents, Java, Android APKs, Adobe Flash applets, Web pages that include high-risk embedded content like JavaScript, Adobe Flash files. MAC OS and DMG file types. The proposed next generation security platform should be able to detect and prevent zero-day threats infection through HTTP, HTTPS, FTP, SMTP, POP3, IMAP use by any of application used by the users (eg: Gmail, Facebook, MS outlook)	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Clause is omitted. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 0	AnnexureN	External NGFW	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.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 1	Annexure N	External NGFW	Cloud base unknown malware analysis service with guaranteed protection signature delivery time not more than 5 minutes.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 2	AnnexureN	External NGFW	Advance unknown malware analysis engine should be able to creates automated high-fidelity signature for command and control (CnC) connections and spyware to inspect command and control http payload to create one to many payloads base signatures protection from multiple unknown spyware and command and control channels using single content base signature	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 3	AnnexureN	External NGFW	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 4	AnnexureN	External NGFW	The APT should assist the team in discovering the infected host by providing Detailed analysis of every detected malicious file and Session data associated with the delivery of the malicious file, including source, destination, application, User and URL etc.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 5	AnnexureN	External NGFW	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.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Refer #150

Response to the Pre-Bid Queries

15 6	AnnexureN	External NGFW	The protection signatures created base unknown malware emulation should be payload or content base signatures that cloud block multiple unknown malware that use different hash but the same malicious payload.	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Refer #153

Response to the Pre-Bid Queries

15 7	AnnexureN	External NGFW	Should protect against never-before-seen phishing and JavaScript attacks inline. Solution should be capable to use both signature based and ML based signature less technology	Sandbox is already been asked in the RFP as a separate dedicated solution , and this Compliance is specific to OEM , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 8	AnnexureN	External NGFW	Proposed model to have Trusted Platform Module (TPM) module for hardware and software integrity. The proposed appliance architecture should have Control Plane separated from the Data Plane in the Device architecture itself, whereby Control Plane should handle Management functions & Data Plane should handle Signature matching for Security processing	Proposed model to have Trusted Platform Module (TPM) module for hardware and software integrity. The proposed appliance architecture should have Control Plane separated from the Data Plane in the Device architecture itself, logically or physically whereby Control Plane should handle Management functions & Data Plane for Security processing	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

15 9	AnnexureN	External NGFW	The proposed firewall solution must support separation of management plane and data plane on firewall device with capability to allocate dedicated management resources (like CPU cores, interface) on gateway device and configure management domain, so that access to the firewall device management is guaranteed even in scenario of heavy traffic load on firewall device or threats like DoS attacks. Proposed Firewall should not use proprietary CPU & should be open architecture to protect & scale against dynamic latest security threats with minimum 24 core CPU.	The proposed firewall solution must support logical and physical separation of management plane and data plane on firewall device with capability. Proposed Firewall should be open architecture to protect & scale against dynamic latest security threats with minimum 24 core CPU.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 0	AnnexureN	External NGFW	The proposed NGFW should support provide Client base VPN on the same platform for at 10000 concurrent users. The proposed solution must be able enforce policy based on endpoint profile such as Patch updates, AV status, disk encryption status, data loss prevention for compliance verification and should be able to provide access based on the compliance state. The proposed solution should be able to share the identity information such as IP address, username, device type, OS and software details with other solutions such as NAC for conditional access from day 1.	This Compliance is specific to Core ZTNA , hence requesting DOP to delete this compliance to have good Number of Participants	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 1	AnnexureN	External NGFW	Firewall to have native connector for proposed SSE and enterprise browser.	Firewall to have API/REST APIs for integration with 3rd Party Solutions.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 2	Annexure N	External NGFW	Should support DoS (Denial of Service) Protection to defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood • UDP flood • ICMP flood • IGMP flood	Should support DoS (Denial of Service) Protection to defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood • UDP flood • ICMP flood	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 3	AnnexureN	External NGFW	The Firewall OEM should be SOC2 certified. OEM should certify with SOC2 for customer data privacy protection. The data uploaded for unknown threat emulation and analysis, along with all associated services like sandboxing, must reside within India's judiciary boundaries.	The Firewall OEM should be SOC2 certified. OEM should certify with SOC2 for customer data privacy protection.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 4	AnnexureN	External NGFW		Kindly confirm if performance paramteres mentioned here needs to be achived with single firewall applinace or stacking of solution is permitted ?	As per RFP

Response to the Pre-Bid Queries

16 5	AnnexureN	Server Load Balancer	The solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the solution and integration with automation and CI/CD tools including Ansible, Jenkins, and Terraform.	The solution must support Programmability to support Automation, integration. It should enable provisioning and configuration of the solution and integration with automation and CI/CD tools including Ansible/Jenkins/Terraform.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

16 6	AnnexureN	Server Load Balancer	"The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 2 Million 2) Network interfaces: 8x10G SFP+ and additional 16 x 10G SFP+ for future use 3) SSL Throughput: 20 Gbps with 40K SSL TPS/CPS with RSA 2k keys and 30K SSL TPS/CPS with ECC 4) Storage: 500 GB SSD scalable 1 TB 5) Memory: 32 GB from day 1 scalable to 128 GB"	"The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 1.2 Million 2) Network interfaces: 8x10G SFP+ and additional 4 x 40G QSFP for future use. 3) L7 Throughput: 75 Gbps with 60 K SSL CPS 1:1 with RSA 2k keys and 40K SSL CPS 1:1 with ECDSA. 4) Storage: 480 GB SSD 5) Memory: 128 from day-1.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 7	AnnexureN	Server Load Balancer	The appliance should support virtualisation, and should have atleast 8 virtual instances from day 1 scalable to support upto 20 virtual instance for future use.	The appliance should support virtualisation, and should have atleast 25 virtual instances from day 1 scalable to support upto 50 virtual instance for future use.	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 8	AnnexureN	Server Load Balancer	The proposed solution must have the capability to provide SSL offloading using both RSA and ECC based keys	The proposed solution must have the capability to provide SSL offloading using both RSA and ECC/ECDSA based keys	The revised clause to be read as: “ECC” in the RFP includes ECDSA. The bidder’s wording “RSA and ECC/ECDSA” is acceptable and does not change the requirement. The solution must support SSL offloading for both RSA and ECC (including ECDSA) keys. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 9	AnnexureN	Server Load Balancer	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management. The proposed LB should be capable to trigger a script based on an event	The proposed solution must offer out of band programming for control plane along with data plane scripting for functions like content inspection and traffic management.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

17 0	AnnexureN	Server Load Balancer	The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching, caching & compression, hardware based SSL offload and server side compression.	The Proposed solution should have application delivery features such as Layer-7 load balancing, Layer-7 content switching/routing, caching & compression, hardware based SSL offload and server side compression.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

17 1	AnnexureN	Server Load Balancer	The Proposed solution should be able to monitor the applications using intelligent application monitors which can be either using system defined executable scripts. It should also provide mechanism to bind multiple health checks, support for application specific VIP health check and next gateway health checks	The Proposed solution should be able to monitor the applications using intelligent application monitors. It should also provide mechanism to bind multiple health checks, support for application specific VIP health check and next gateway health checks	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

17 2	AnnexureN	Sandboxing	The proposed solution should be able to support at least 3 unique OS images on single appliance and should run at least 60 parallel sandboxes for analysis and support 40,000 samples/day, Customized sandbox solution should support multiple customizable OS images (Windows desktop/server versions and Linux distributions) and must have the capability to analyze large files and must be able to support more than 50MB file size.	The proposed solution should be able to support at least 3 unique OS images on single appliance and should run at least 60 parallel sandboxes for analysis with scalability to extend to 100 parallel VM's for future usage and support 150,000 samples/day, Customized sandbox solution should support multiple customizable OS images (Windows desktop/server versions and Linux distributions) and must have the capability to analyze large files and must be able to support at least more than 5GB file size.	The revised clause to be read as: "The proposed solution should be able to support at least 3 unique OS images on single appliance and should run at least 60 parallel sandboxes for analysis and support at least 40,000 samples/day, Customized sandbox solution should have capability to analyse file size minimum 5GB. The bidder should propose and size the solution accordingly. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

17 3	AnnexureN	Sandboxing	The proposed solution should be able to support at least 3 unique OS images on single appliance and should run at least 60 parallel sandboxes for analysis and support 40,000 samples/day, Customized sandbox solution should support multiple customizable OS images (Windows desktop/server versions and Linux distributions) and must have the capability to analyze large files and must be able to support more than 50MB file size.	Solution should support pre-configured VM engines and also have a capability to add custom VM. Malware analysis saves administrators set up time and configuration issues. The solution should analyse advanced targeted attacks without adding network and security management overhead. solution and have capability to allow manual submission of suspicious files for analysis	Refer #172

Response to the Pre-Bid Queries

[illegible]

Response to the Pre-Bid Queries

17 5	AnnexureN	Sandboxing		Solution should have integrated regular security threat intelligence content subscription as part of the solution. The security content should be integrated with the solution without any requirement to manually manage and update the feeds. Solution must be completely On-Premise.	As per RFP

Response to the Pre-Bid Queries

17 6	AnnexureN	Sandboxing		Solution should detect zero-day, multi-flow and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment and stop infection and compromise phases of the cyber-attack kill chain by identifying never-before-seen exploits and malware.Solution must be completely On-Premise.	As per RFP

Response to the Pre-Bid Queries

17 7	AnnexureN	Attack Surface Management	Solution should rescan daily or faster	The solution should have the ability to scan for new assets/issues on adhoc basis	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

17 8	AnnexureN	Attack Surface Management	Solution should report all relevant context of each asset type, including the registration information	" Solution should report all relevant context of each aset type, including technologies used and vulnerabilty of the same"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

17 9	AnnexureN	Attack Surface Management	Solution should treat dynamic assets in a simple manner, so that results can be deduplicated when a single identifier is seen hosted many times across large CDNs	" Solution to allow to add the application associated internal IP to reduce the false positives if the application is hosted behind a CDN"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

180	AnnexureN	Attack Surface Management	Solution should distinguish between directly attributable assets and co-located services	"Solution should distinguish between on premise and Cloud assets"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 1	AnnexureN	Attack Surface Management	Solution should label assets with an ownership confidence score	Solution should provide the context if the issue/vulnerability is been exploited in the wild	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 2	AnnexureN	Attack Surface Management	Solution should highlight stale IP registration records for update and to reflect accurate ownership	We request to remove this point as this does not add any value for detecting /remediating threats	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 3	AnnexureN	Attack Surface Management	Risk score should be based on accepted industry metrics, and allow for customization	Risk score should be based on accepted industry metrics	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 4	AnnexureN	Attack Surface Management	Solution should be capable of actually fixing things	A Service provider can only scan and report the issues on the assets; remediation has to be done by the SOC team; we request to remove this point	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 5	AnnexureN	Attack Surface Management	Solution should have the ability to automate common actions. This includes pulling in known asset owners, sending automated emails, or automatically creating tickets for investigation.	Solution should have the ability to integrate with on prem tools and send emails, or create tickets for investigation directly from the portal	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 6	AnnexureN	Attack Surface Management	Solution should have the ability to automatically remediate exposures. This should include full resolution of the incident by reaching back via API and blocking the service at the port level.	Solution must have the ability to block the ports on the firewall from the portal using integration with the firewall	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 7	AnnexureN	Attack Surface Management	Allow customizability to the remediation path	We request to remove this point as this is to be done by the SOC team	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 8	AnnexureN	Attack Surface Management	Solution should have the ability to allow users to customize the weight of incidents in their overall risk score based on the organizations needs	We request to remove this point as this defeats the purpose of having a independent service provider who provides the risk ratings of the organization	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

18 9	AnnexureN	Attack Surface Management	Ability to create or remove risk scoring rules	We request to remove this point as this defeats the purpose of having a independent service provider who provides the risk ratings of the organization	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

190	AnnexureN	Attack Surface Management	Ability to override the default system score and enter a score	We request to remove this point as this defeats the purpose of having a independent service provider who provides the risk ratings of the organization	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 1	AnnexureN	Attack Surface Management	The best practice method of risk scoring is a combination of CVSS and EPSS data	We request to remove this point as this defeats the purpose of having a independent service provider who provides the risk ratings of the organization	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 2	AnnexureN	Attack Surface Management	Create dashboards based on the needs of your organization and what visibility you are looking to have	Create dashbaords according to the various tags created BU/SBU/susbsidary wise"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 3	AnnexureN	Attack Surface Management	Create reports based on the needs of your organization and schedule regular reporting on a particular cadence for quicker reporting cycles	The solution should provide weekly report scans of new assets and vulnerabilities and daily scans of issues on discovered assets	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 4	AnnexureN	Attack Surface Management	Perform AND/OR searches across assets to drill down easily	The solution should provide the ability to search for the assets by using either ASN, IP block,IP address,Domain or sub domain	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 5	AnnexureN	Attack Surface Management	Provide compliance dashboards that map identified Issues to compliance frameworks to help our teams understand their overall compliance with regulatory and organizational policies. These dashboards need to provide executive visibility, prioritize high-risk cybersecurity areas, and measure the progress of our organization's maturity.	The solution should provide executive dashboard which provide the overall threat pertaining to the organization"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 6	AnnexureN	Attack Surface Management	Solution should offer a way of managing assets and identifying risk through policies	Solution should allow identification of assets BU wise/subsidiary wise/tag wise	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 7	AnnexureN	Attack Surface Management	Enables you to define the number of hours after which the user login session will expire.	The solution must logout a user from the portal after been active for some time"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 8	AnnexureN	Attack Surface Management	Enables you to define approved domains and approved IP ranges through which access the platform	The solution should allow restricted users to access individual modules on the platform	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

19 9	AnnexureN	Attack Surface Management	Enables you to deactivate an inactive user & set a deactivation time period	Solution needs to allow to deactivate the users and also provide audit logs of all the users"	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

200	AnnexureN	Attack Surface Management		The threat intelligence should, preferably, be able to provide insight into how attackers and campaigns are organized and what targets are being attacked and, in addition, guidance on how to protect the organization from the attacks.	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

20 1	AnnexureN	Attack Surface Management		The facility should be available to search for threat indicators on the portal. For example, to search for an IP address/hash/domain/CVE identified internally with the organization to check if it is malicious and if it is related to any particular threat group	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

20 2	AnnexureN	Attack Surface Management		Platform should provide ratings of 3rd party vendors according to their risk exposure in open surface and darkweb which will help the organization evaluate supplier risk or assess the security of M&A targets.	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

203	AnnexureN	WAF	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time	The WAF Solution should have mechanism to block bad actor from repeated violation of security policies configured/brute force attack.	The revised clause to be read as: The WAF Solution should have mechanism to block bad actor from repeated violation of security policies configured/brute force attack. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 4	AnnexureN	WAF	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or IP address d. Should be able to generate unique identifier to track attack event	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or IP address d. Should be able to generate unique identifier/ Event ID to track attack event	The revised clause to be read as: The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or IP address d. Should be able to generate unique identifier/ Event ID to track attack event Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 5	AnnexureN	WAF	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic	WAF solution should have GraphQL content profile/protection rules and policy on GraphQL traffic	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 6	AnnexureN	WAF	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware, KVM etc.). (Public Available Reference Link should be shared) Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System It should NOT use/allow 3rd party or open source software to be deployed as network functions on the same hardware.	This is not a core WAF functionality and favouring a specific OEM, Request DOP to Delete this compliance	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 7	Annexure N	WAF	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.	Proposed WAF device shall have native capability to protect against DOS attacks, without relying on any 3rd party device.	Clause is omitted. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 8	AnnexureN	WAF	Bidder to proposed separate Centralized Dashboard and should Provide at least following information: - Application dashboard - Per application analytics - SSL statistics (handshake & cypher breakdown, rejected handshake) - SSL CPS - System dashboard (Device CPU, Memory, Port Status etc) - Network Dashboard (CPS, Throughput, Concurrency, Real Server Availability, HA Status etc) - L4 events - Per transaction type events (delay, user agent, response, headers) - SSL Events (type of handshake, cypher and TLS version) - Attack Dashboard - OWASP Top 10 Based Attack details - Geo Based Attack Details	Bidder to proposed separate Centralized Dashboard and should Provide at least following information: - Application dashboard - Per application analytics - SSL statistics (handshake & cypher breakdown, rejected handshake) - SSL CPS - System dashboard (Device CPU, Memory, Port Status etc) - Network Dashboard (CPS, Throughput, Concurrency, Real Server Availability, HA Status etc) - L4 events - Per transaction type events (delay, user agent, response, headers) - SSL Events (type of handshake, cypher and TLS version) - Attack Dashboard - OWASP Top 10 Based Attack details - Geo Based Attack Details	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

20 9	AnnexureN	WAF	The proposed solution should Support Elastic Licensing Model and support below flexibility : 1. A single throughput/capacity license to be shared across physical and Virtual ADCs, on premise and in the cloud, regardless of location or type 2. A complete automation of ADC services deployment and maintenance, allowing the administrator not only to seamlessly spin up new ADC instances, but also use wizards and scripts to distribute the corresponding ADC service configuration – all at the same push of a button. 3. Reclaim capacity from decommissioned instances and reallocate it to new deployments, ensuring optimal license utilization	Its is recommended to ask for throughput of WAF from day 1,Request DOP to Delete this compliance	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

21 0	AnnexureN	WAF	The proposed device should supports SSL offload for the following protocols: - HTTPS - Generic SSL - SIP - SMTP (STARTTLS) - IMAP (STARTTLS) - POP3 (STARTTLS) - LDAP (STARTTLS) - FTPS	WAF looks after the offloading of HTTPS rest others should be handled by ADC or SSLO,Request DOP to Delete this compliance	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

21 1	Annexure N	WAF	The proposed device should use standard VRRP (RFC – 2338) for High Availability.	The proposed device should use standard VRRP (RFC – 2338) or any proprietary protocol for High Availability.	The revised clause to be read as: The proposed device should use standard VRRP or equivalent protocol for High Availability. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

21 2	AnnexureN	WAF		The proposed WAF should be a dedicated WAF, not part of any ADC	Yes, this is the requirement

Response to the Pre-Bid Queries

21 3	AnnexureN	WAF		The OEM/Bidder should propose a dedicated hardware Web application Firewall The proposed WAF solution should be enabled with all the modules and features from day one without any additional license dependency.	Yes, this is the requirement

Response to the Pre-Bid Queries

21 4	AnnexureN	WAF		The solution must be able to support multi-node operations and deployment.	As per RFP

Response to the Pre-Bid Queries

21 5	AnnexureN	WAF		The Proposed WAF must support two or more of the following deployment modes to monitor web application traffic over the network: - Via a SPAN/TAP port sniffing mode - Layer-2 transparent inline bridge mode - Reverse Proxy mode - Transparent Layer-2 Reverse Proxy mode - L3 reverse proxy mode	As per RFP

Response to the Pre-Bid Queries

21 6	AnnexureN	WAF		If the user or client browser is infected with malware/trojan, the solution must be able to block the user request and should also be able to protect against Man In the Browser attack (MITB).	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

21 7	AnnexureN	WAF		The proposed solution must support at least 50 Gbps of WAF throughput with minimum 128 GB RAM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

21 8	AnnexureN	WAF		he proposed solution must comply following minimum SSL performance throughputs: With RSA (2k keys) :- 500 K TPS With ECC (P256) :- 350 K TPS Here CPS means Connections per second and TPS means Transactions per second.	As per RFP

Response to the Pre-Bid Queries

21 9	AnnexureN	WAF		The solution must support Layer 7 concurrent connection of minimum 2 Million.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

22 0	AnnexureN	WAF		The proposed WAF should support minimum following network interfaces: • 8 x 1Gig RJ45 • 10 x 10Gig SFP+ • 2 x 40Gig SFP+ Device should support link aggregation/ bundling.	Bidder to propose solution, aligned with RFP functional and non-functional requirements. It should support non-blocking architecture and traffic flow of north-south within DCs.

Response to the Pre-Bid Queries

22 1	AnnexureN	Link Load Balancer	The proposed appliance must provide 30 GBPS of throughput from day 1 scalable upto 60 GBPS	The proposed appliance must provide 100 GBPS of Layer 4 throughput from day-1.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 2	AnnexureN	Link Load Balancer	"Appliance should be loaded with following interfaces on day one and should support virtualisation: - 10 Gbps Fiber port - 8 Nos. - 1G Copper port - 8 - Dedicated 10/100/1000 Mbps out-of-band management port - 2 No. and USB port- 1 No. each - RJ45/DB9 console port - 1 No."	"Appliance should be loaded with following interfaces on day one and should support virtualisation: - 10 Gbps Fiber port - 8 Nos. 40G Fiber Port-4 Nos. - Dedicated 10/100/1000 Mbps out-of-band management port - 2 No. and USB port- 1 No. each - RJ45/DB9 console port - 1 No."	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 3	AnnexureN	Link Load Balancer	Proposed solution should be dedicated appliance, The software solution must support Programmability to support Automation, native integration and orchestration. It should enable declarative provisioning and configuration of the software solution across cloud environments and integration with automation and CI/CD tools such as Ansible, Jenkins, Terraform or equivalent.	Proposed solution should be dedicated appliance, The software solution must support Programmability to support Automation, integration. It should enable provisioning and configuration of the software solution across cloud environments and integration with automation and CI/CD tools such as Ansible, Jenkins/Terraform or equivalent.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 4	AnnexureN	Link Load Balancer	Should support Geolocation and Proximity based load balancing	Should support DNS and Geographic Proximity based load balancing	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 5	AnnexureN	Link Load Balancer	"Should support the following or equivalent Global Load balancing algorithms. •Round robin • Global availability • LDNS persistence • Application availability • Geography/Proximity Route • Virtual server capacity • Least connections • Packets per second / Bandwidth • Round trip time / Network • Hops "	"Should support the following or equivalent Global Load balancing algorithms. •Round robin • Global availability • LDNS persistence • Application availability • Geography/Proximity Route • Virtual server capacity • Least connections • Packets per second / Bandwidth • Round trip time / Network"	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 6	AnnexureN	Link Load Balancer	"The proposed device should have Hypervisor based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the hardware should be a specialized purpose-built hypervisor. Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System It should NOT use/allow 3rd party or open source software to be deployed as network functions on the same hardware. The proposed device should support 5 Virtual Instance from Day 1 scalable to 10 for future use."	"The proposed device should have Virtualization feature to create logical Virtual Instance/Virtual systems/Virtual domain Each Virtual Instance contains a complete and separated environment of the Following: a) Independent network b) Configuration c) Management It should NOT use/allow 3rd party or open source software to be deployed as network functions on the same hardware. The proposed device should support 10 Virtual Instance from Day 1 scalable to 25 for future use."	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 7	AnnexureN	Link Load Balancer	"The proposed solution should Support Elastic Licensing Model and support below flexibility : 1. A single throughput/capacity license to be shared across physical and Virtual ADCs, on premise and in the cloud, regardless of location or type 2. A complete automation of ADC services deployment and maintenance, allowing the administrator not only to seamlessly spin up new ADC instances, but also use wizards and scripts to distribute the corresponding ADC service configuration – all at the same push of a button. 3. Reclaim capacity from decommissioned instances and reallocate it to new deployments, ensuring optimal license utilization"	The proposed ADC solution should provide access to the asked full licensed throughput capacity of the platform from Day 1 without requiring any additional licenses.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 8	AnnexureN	Link Load Balancer	"The proposed Link Load Balancer must support: 1. Static NAT 2. Dynamic NAT 3. No-NAT "	"The proposed Link Load Balancer must support: 1. Static NAT 2. Dynamic NAT/Port Forwarding 3. Source NAT 3. No-NAT "	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

22 9	AnnexureN	Link Load Balancer	"The proposed Appliance should supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • NNTP Server Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks"	"The proposed Appliance should support the following health check types: ICMP Health Check TCP Echo Health Check TCP Health Check HTTP Health Check HTTPS Health Check DNS Health Check RADIUS Health Check SMTP Health Check POP3 Health Check IMAP4 Health Check RADIUS Accounting Health Check FTP Health Check TCP Half-Open Connection Health Check TCP SSL Health Check SNMP Health Check SSH Health Check L2 Detection Health Check UDP Health Check SIP Health Check SIP TCP Health Check SNMP Custom Health Check RTSP Health Check MySQL Health Check Diameter Health Check Script Health Check Oracle Health Check LDAP Health Check MSSQL Health Check LDAPS Health Check"	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

23 0				Proposed appliance should have dual hot-swappable PSU and redundant fans.	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

23 1				The solution should offer native Anti-Virus solution, IP reputation, Geo IP Protection and the database should be updated automatically. It should NOT introduce additional software or hardware deployment. nor 3rd-party integration requirements for achieve the functionalities	As per RFP

Response to the Pre-Bid Queries

23 2	Volume II	8. Manpower Requirements	The system integrator shall provide a team of resources during the contract period at DoP-specified locations, as mentioned in this section, to perform the services mentioned in the above sections of this RFP:	Requesting DOP to relax this point to operate the O&M from the SI locations to have better Resource Management	O&M and enhancement team to work from DoP Chennai premises. Key Resources from Delhi NCR/Chennai. Rest as per solution requirements at DC/DR locations.

Response to the Pre-Bid Queries

23 3	Volume II	5.2.4 Detailed Scope of Work , Page#85	36. The SI is required to guarantee a Recovery Time Objective (RTO) of 30 minutes and a Recovery Point Objective (RPO) of ZERO minutes for all hosted solutions in DR and NDC.	RTO and RPO SLA's are bit stringent , Hence Requesting DOP to modify the SLA's as below , RTO - 2 Hrs for Identified Application Components from DC to DR RPO - 15 mins to the Identified Database/FS from DC to NDC	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

23 4	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-2	Storage solution should provide the native capability to replicate data of existing storage between DC, DR and NDC without using any additional Hardware and software.	Clarification Request : This is a restrictive clause. Request DOP to remove this clause for wider participation. Justification: Incase a Native replication with existing storage is required then only an existing storage OEM can qualify which eliminates all other OEM participation. Hence request DOP to remove this clause	Refer #85

Response to the Pre-Bid Queries

23 5	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-3	SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage without using external/3rd party hardware or Software.	Clarification Request : SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage with/without using external/3rd party hardware or Software. Justification: This is a restrictive clause. Request DOP to modify this clause wider participation. Hence request to modify this clause	Refer #86

Response to the Pre-Bid Queries

23 6	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-8	Storage solution should support all Leading enterprise servers and Operating Systems: - CISC-based Servers running Windows, Linux, HP Enterprise Servers running HP/UX, IBM Enterprise Servers running AIX, SUN Enterprise Servers running Solaris, IBM Linux on the POWER platform. It should also support VMWare APIs - VAAI, VASA and RESTful API.	Modification Request :Storage solution should support all Leading enterprise servers and Operating Systems: - CISC-based Servers running Windows, Linux, HP Enterprise Servers running HP/UX, IBM Enterprise Servers running AIX, SUN Enterprise Servers running Solaris. It should also support VMWare APIs - VAAI, VASA and RESTful API. Justification: Since most of the application are going to be on x86 CISC based platform as asked in the RFP which is going to be virtualised with industry standard hypervisor and container platform/operating system, Sun Ent server running solaris, IBM linux on power platform is a niche OS which is not widely deployed, hence it should be modified.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

23 7	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-9	The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture with cache across configured controllers.	Clarification: We understand active active multi controller means all luns should be accesible to all the controllers in case of controller failure. please confirm if our understanding is correct.	Refer #89

Response to the Pre-Bid Queries

23 8	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-12	The proposed storage should have No Single Point of Failure (NSPOF) and, automatic failover architecture. All components must be redundant & hot swappable.	Clarification: We understand that DOP is asking for storage array with No Single Point failure shall include all components in controllers power supplies , IO cards , boot drives etc. please confirm if our understanding is correct.	As per RFP

Response to the Pre-Bid Queries

23 9	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-13	The Storage system must provide cache protection in case of power failure through de-staging to nonvolatile media or a 72-hour battery backup.	Modification Request :The Storage system must provide protection of data written in the cache/Memory in the event of complete power failure through de- staging of cache to non- volatile media or battery backup for at least 72 hours. Justification: Every OEM has different architecture with respect to system cache hence request you to modify this clause.	As per RFP

Response to the Pre-Bid Queries

24 0	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-17	Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes.	Modification Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes or as per OEM guidelines to deliver the performanc e & capacity . Justification: To deliver the performance and capacity, OEM applies their own best practice to configure the storage with the best possible configuration of drives. Hence request to modify this clause.	Refer #91

Response to the Pre-Bid Queries

24 1	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-32	The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 256GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall dynamically support read and write i/o	Modification Request : The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 2 controllers with cache size 256GB at NDC (scalable up to 1TB), protected by vault /battery/destaging. Justification: As DOP has asked for 4 controllers at DC and DR, two controllers are sufficient for NDR site. cache shall be protectected as per OEM best practice architecture. Request DOP to modify this clause.	Refer #93

Response to the Pre-Bid Queries

24 2	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-44	Must support compression supported for replicated traffic (FC/Ethernet) or as per OEM recommendation, redundant FCIP if required.	Modification: This clause provided undue advantage to an OEM offerings hence, request you to delete this cluse for wider participation. In case FCIP routers are required , its shall be asked from all the OEM's. Justification: In a critical banking environment, FCIP routers are must from best practice point of view. Hence request DOP to please make FCIP as a mandatory ask from all the OEM.	As per RFP

Response to the Pre-Bid Queries

24 3	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-54	Must support advanced management: end-to-end mapping, monitoring, capacity planning, alerts, reports.	Modification: Must support advanced management: monitoring, , alerts, reports. Justification : This applicable(end-to-end mapping, capacity planning,) to a public cloud offering hence remove this clause.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

24 4	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-67	Must support consistency groups for multiple volumes across arrays with DB- consistent copies.	Modification: Must support consistency groups for multiple volumes across arrays with Block level/DB consistent copies. Justification: DB consistant copies are a feature of Data base only hence request to modify this clause.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

24 5	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-71	Must support high-availability 3-way / 4-way ZDL solutions for Oracle, Windows, UNIX, and databases.	Modification: Must support high-availability 3-way solutions for Oracle, Windows, UNIX, and databases. Justification: request to modify this clause.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

24 6	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-72	Must optimise WAN replication traffic with compression; redundant FCIP routers if needed.	Modification: This clause provided undue advantage to an OEM offerings hence, request you to delete this clause for wider participation. In case FCIP routers are required , its shall be asked from all the OEM's. Justification: In a critical banking environment, FCIP routers are must from best practice point of view. Hence request DOP to please make FCIP as a mandatory ask from all the OEM.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

24 7	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-77	Must support cyber recovery orchestration with ransomware protection.	Modification: Must support cyber recovery orchestration with inbuilt inline ransomware detection & protection. Justification: Kindly modify this clause with addition of detection feature also.	As per RFP

Response to the Pre-Bid Queries

24 8	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-78	Must support immutable DB- consistent backup copies with WORM/Equivalent, RBAC, SCN-based restore, etc.	Modification: Must support immutable block level/DBconsistent backup copies with WORM/Equivalent, RBAC, SCN-based restore, etc. Justification:DB consistant copies are a feature of Data base only hence request to modify this clause.:	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

24 9	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-85	Storage management must support customised reports, topology monitoring, chargeback, and trending.	Modification: Storage management must support customised reports, topology monitoringand trending. Justification: we believe DOP is not going to use this Infra for cloud setup. Request to remove the charge back from the specification.	The revised clause to be read as: Storage management must support customised reports, topology monitoring, and trending. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

25 0	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-86	Must integrate with existing backup infrastructure.	Justification: This a restrictive clause.please remove this point as this will give undue advantage to existing OEM. Kindly share backup software compliance for wider participation.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

25 1	Volume of the RFP (II)	Annexure L Page No- 260- Backup Solution Clause No 1	Enterprise backup platform supporting three-site architecture with central console and role-based access.	Clarification: we understand this si a backup software solution requirement Enterprise backup platform supporting three-site architecture with central console and role- based access.	As per RFP

Response to the Pre-Bid Queries

25 2	Volume of the RFP (II)	Annexure L Page No- 260- Backup Solution Clause No 18	Multi-site, dedupe-enabled appliances with replication; Hot-swap disks/power; Dual controllers.	Modification: Multi-site, dedupe-enabled appliances with replication; Hot-swap disks/power, Dual controller/as per OEM architecture. Justification: This is a restrive clause The proposed backup appliance provides equivalent or superior availability, data integrity, and recoverability. Redundancy and high availability are achieved through a combination of fault-tolerant hardware components. request to modify this clause for wider participation.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

25 3	Volume of the RFP (II)	Annexure L Page No- 260 San Switch Clause No		Clarification: From a technology vs cost point of view we suggest to consider SAN switch based architecture which can support upto 96 port per switch and will deliver more deployment feasibility options in current sized landscape. We request DOP to modify this request.	The revised clause to be read as: SAN switch shall be configured with 96 ports, each supporting minimum 32 Gbps FC port, with backward compatibility to 16G and forward compatibility preferred. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

25 4	Volume of the RFP (II)	Annexure L Page No- 260 Tape Library Clause No 4	Min 250 slots, scalable upward; adequate media & cleaning cartridges	Modification: Min 240 slots, scalable upward; adequate media & cleaning cartridges. Justification: please change this clause for wider participation	The revised clause to be read as: Min 240 slots, scalable upward; adequate media & cleaning cartridges. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

25 5	Volume of the RFP (II)	Annexure L Page No- 260 Tape Library Clause No 8	High-availability robotic subsystem; dual accessor preferred	Justification: please remove this point as this is giving an undue advantage to a specific OEM	Refer #84

Response to the Pre-Bid Queries

25 6	Volume of the RFP (II)	Annexure L Page No- 260 x86 Server Clause No 1	Form Factor-Rack 1U form factor	Modification Request : Pls help to ammend asked clause as" 1U/2U /4U Form factor " Justifictaion : This will enable Flexiblity to sizie solution as per Application OEM sizing Requirement Based on CPU/Local Drives & GPU Requirement	The revised clause to be read as: "Form Factor-Rack 1U/2U form factor" Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

25 7	Volume of the RFP (II)	Annexure L Page No- 260 x86 Server Clause No 6	Storage Controller Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60	Modification Request : Pls help to ammend asked clause as Integrated/PCIe 4.0/5.0 12Gb/s/24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60 Justification : Industry Standard SAS Controller works on 12Gb/s with PCI 4.0 technology . Pls update asked clause to make its as Industry standard technology	Refer #100

Response to the Pre-Bid Queries

25 8	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 2	2.Router should have a physical separation between control and data planes processor. Router should support inline hardware accelerated encryption for high-throughput Ipsec	As per the clause 16 in specification of core Router external appliance is allowed for firewall Functionality , Request to kindly allow to have IPSEC functionality offloaded to external device . This will remove ambiguity in design and will also insure high scale along with maximum participation while insuring maximum return on investment with next generation architecture	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

25 9	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 3	3. Load balancing feature to be present in routers and must work mainly for internet terminated links. Internet and MPLS both will be terminated in router and the same must work seamlessly in different routing planes without affecting security and maintaining IT security compliance.	we understand that Load balancing / Load Sharing on the internet side can be achieved by BGP learned routes or through Policy based Routing , Kindly confirm	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

26 0	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 9	9. The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should be able to create GRE tunnel.	L2TP is a legacy unencrypted protocol , IPSEC is already asked in the tender which is more secure and support by all leading OEM , Request to relax the clause and allow IPSEC to be used in place of L2TP .Also GRE encapsulates the packet ,no encryption is used in GRE , Request to kindly change the clause by removing GRE encryption and on on demand GRE for solution clarity or allow IPSEC / GDOI while the same can be offloaded to external firewall as requested . Requested clause :- The router must support IKEv1, L2TP/IPSEC , IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption/IPSEC	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

26 1	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 10	10.The router should support 19 Gbps of IPSEC Bandwidth	Request to kindly confirm for offloading the IPSEC to external firewall for leading OEM to participate . The same is also requested in query 1 of core Router	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

26 2	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 11	11.Implementation Agency should ensure necessary encryption 8.5 Gbps throughput (IMIX, EMIX) supported by proposed device at site from day 1: (IPSEC case of SD-WAN)	Request to kindly remove (IPSEC Case of SDWAN) as the same is creating ambiguity . IPSEC will be used on WAN side for traffic encryption as per the Govt Guide lines and frame work for Financial organization . Request change for leading OEM to participate .	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

26 3	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 12	12.Router should be scalable to support up to 4000 tunnels (non-SDWAN) / 8000 SD_WAN tunnel (SD- WAN)	Different OEM have different architecture for providing the traffic encryption using IPSEC .SDWAN for all OEM is proprietary and can not integrate with any other OEM , Request to kindly remove SDWAN or clarify that either of 4K (no-SDWAN) / 8K should be supported .	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

26 4	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 17	17.Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.	Traffic optimization was required on low latency link such as E1 or low speed TDM link which are not used in modern days network , The solution provided will have ethernet connectivity ranging for 1Gps to 100Gbps interface. Also Traffic optimization works on P2P links i.e both side should have functionality . The same is not possible in large and heterogenous network . Request to kindly remove the clause for leading OEM to participate .	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

26 5	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 21	21. Router should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

26 6	Volume II ,	Annexure L , Core-Router , Manageability -Clause 25	25. Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

26 7	Volume II ,	Annexure L , Core-Router , Manageability -Clause 29	29. Router should be IPv6 Certified/IPv6 logo ready	All reputed OEM support IPV6 functionality from day 1 , we are providing latest hardware / solution which supports all IPV6 features from day1 . Request to amend the clause for leading OEM to participate . Requested Clause :- Router should be IPv6 Certified/IPv6 logo ready / IPV6 Ready	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

26 8	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 8	8. Minimum WAN throughput: 20 Gbps (scalable to 40 Gbps).	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the WAN throughput asked is 40Gbps which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Minimum WAN throughput: 320 Gbps (scalable to 340 Gbps).	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

26 9	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 10	10.Forwarding performance: > 30 Mpps.	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the MPPS asked is >30MPPS which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Forwarding performance: > 476Mpps.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

27 0	Volume II ,	Annexure L , WAN Router , Performance Requirement -Claus23	23.Stateful firewall capabilities.	Request to kindly change the clause for leading OEM to Participate . Requested clause:- .Stateful firewall capabilities/ ACL/ Firewall filter	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

27 1	Volume II ,	Annexure L , WAN Router , High Availability -Clause 30,31	30.Non-stop Routing (NSR), Non-stop Forwarding (NSF). 31. Stateful switchover (SSO)	For asked functionality to work redundant CPU / Routing engine is required . Kindly clarify if redundant Routing engine is required from day 1 or only support is asked . Kindly clarify for solution clarity .	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

27 2	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 9	9.The switch should support 30k multicast routes	30K Multicast is on very high side and not required on spine as they act as transit for traffic , request to reduce the route scale for maximum participation for leading OEM to participate . Requested clause :- .The switch should support 8k multicast routes	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

27 3	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 25	25.Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP)	MSDP is used on WAN side and is not widely deployed in Spine devices in data center, instead PIM SSM and PIM SM are used request to relax the clause for leading OEM to participate . Requested clause :- Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) / MLD (Multicast Listener Discovery)	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

27 4	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 37- 39	• Flow path trace (ingress to egress switch) • Per Flow Hop by Hop packet drop with reason of drop • Per Flow latency (per switch and end to end)	Diffrenet OEM have different architecture to learn about Network / Fabric health and suggest the anamoly or congestion / usage state . Request to allow standard based Flowmonitoring usinf SFLOW for leading OEM to participate . Requested Clause :- • Flow path trace (ingress to egress switch) or should support SFLOW / FLOW Monitoring • Per Flow Hop by Hop packet drop with reason of drop or should SFLOW / FLOW Monitoring • Per Flow latency (per switch and end to end) or should SFLOW / FLOW Monitoring	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

27 5	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	17.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

27 6	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	23.The Switch should support intelligent buffer management with a minimum buffer of 36 MB.	Request to kindly change the packet buffer to 32Mb for leading OEM to participate Requested clause :- 23.The Switch should support intelligent buffer management with a minimum buffer of 32 MB.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

27 7	Volume II ,	Annexure L , LEAF SWITCH ,Network Virtualization Features -Clause 26	26.Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualize networking from the single pane of glass	Leaf switch connect to any virtualization platform using VLAN . Switch do not connect to any virtualization Manager . The fabric manager / SDN controller defines the EVPN VXLAN fabric on spine and leaf devices , which can further connect to Orchestrator for single pane of glass management. The clause is restricting leading OEM request to change . Requested clause :- Switch must provide the capability to be integrated with different Hypervisor viz. Vmware, Microsoft Hyper-V , Kubernetes, Redhat Openshift using standard based VLAN	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

27 8	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 29	29.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Refer #275

Response to the Pre-Bid Queries

27 9	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	47.Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro- segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification. The solution must also provide micro segmentation capability on application end host at remote location sites in offline mode (once policy is applied from the DC to workloads on remote sites, in case the sites are dis-connected, the enforcement policy is retained). Mentioned feature/capability should be achieved using same OEM products for a seamless integration, without using any external/3rd party solution.	The micro segmentation in data center in virtualized environment is managed by Virtual machine manager and for Switching environment using Fabric manager . They both integrate using Orchestration layer for single plane of management and integration . The functionality asked is achieved through different architecture from different OEM. The clause in current format is restricting leading OEM's .Request to change the clause for leading OEM to participate . Also request to remove virtualization microsegment into the virtual environment security requirement . This will ensure that level playing field is given to all OEM in data center infra domain. Requested clause :- .Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation basis on connected VLAN / Ports .	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

28 0	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	49.Switch platform should support encryption of traffic i.e. MAC Sec Encryption (802.1AE) in hardware	Spine switch is not asked with MACSEC , this will create confusion in design . Request either remove MACSEC for leaf switch or add the same in SPINE switch for solution clarity .	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

28 1	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Clarification Page No- 260 X86-Based Hypervisor & Virtualization	Clarification :RFP Annexure L Have specification section Named as " X86-Based Hypervisor & Virtualization " , Pls clarify which specification to be followed .	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

28 2	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Solution shall support migration of physical Windows and Linux workloads to virtual environments.	Clarification :We understand Migration of physical Windows and Linux workloads to virtual environments will be Planned & offline activity which may need data Migration manually or using 3rd party tools based on Migration approach . Pls confirm	Yes, migration of physical Windows and Linux workloads to virtual environments will be carried out as a planned activity. MSPs may use native tools and/or third-party tools and manual methods as per their proposed migration approach, ensuring minimal disruption and adherence to the project timelines and SLAs.

Response to the Pre-Bid Queries

28 3	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Single-click upgrade or update capability for all compute, hypervisor, and SDS components.	Clarification : We understand SDS - Software Defined Storage is not in scope of this RFP architecture requirement , Pls Remove ask of SDS Solution Requirement Justification : SAN Storage is asked , Hence SDS is not in scope for architecture Requirement	Bidder to fulfill the requirement of the RFP through the best design possible. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

28 4	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Licenses to deploy a purpose- built, bare-metal hypervisor with in-built SDS support.	Clarification : We understand SDS - Software Defined Storage is not in scope of this RFP architecture requirement , Pls Remove ask of SDS Solution Requirement Justification : SAN Storage is asked , Hence SDS is not in scope for architecture Requirement	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

28 5	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Zero downtime host patching with automated workload migration.	Change Request : Request you to Change asked Clause as "Zero downtime or Planned host patching with automated workload migration. Justification : IN pRoduction environment - Updates/Upgrades required Plananed workload Host Migration .	As per RFP

Response to the Pre-Bid Queries

28 6	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Continuous availability using live shadow VMs for fault tolerance.	Change Request : Request you to Change asked Clause as "Continuous availability using live shadow VMs for fault tolerance/ Highavailability Feature with Live Migration" Justification : fault tolerance can be implemented with High availability Live Migration Feature"	The revised clause to be read as: "Continuous availability using live shadow VMs for fault tolerance/ Highavailability Feature with Live Migration." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

28 7	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support remote port mirroring and 802.1q VLAN configurations.	Please remove asked clause, asked remote port mirroring and 802.1q VLAN configurations is not supported in Virtualization environment	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

28 8	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide VM-level encryption for data at rest and in motion (AES-256).	Change Request : Request you to Change asked Clause as"Provide VM-level encryption for data at rest and in motion (AES-256) using Security Infrastructure . Justification : Encryption for data in motion (AES-256) will be Feature of Firewall / Security Infrastructure	The revised clause may be read as: Provide VM-level or equivalent encryption for data at rest, and ensure AES-256-equivalent encryption for data in motion through the proposed security infrastructure. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

28 9	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide visibility of east-west and north-south network traffic between VMs.	Change Request : Request you to Change asked Clause as"Provide visibility of east- west and north-south network traffic between VMs using 3rd Party Tools & Automation solution Justification : This is 3rd Party solution Feature , which can be Intregrated with Virtualization Platform	The functional requirement to provide visibility of east-west and north-south traffic between VMs is retained. SI may fulfil this requirement using native capabilities of the virtualization platform and/or integrated third-party tool solution.

Response to the Pre-Bid Queries

29 0	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable SDN-based virtualised networking and distributed firewalling.	Change Request : Request you to Change asked Clause as"Enable SDN-based virtualised networking and distributed firewalling using 3rd Part Tools & Automation solution Justification : This is 3rd Party solution Feature , which can be Intregrated with Virtualization Platform	The intent is that the overall solution provides SDN-based virtual networking and distributed firewalling as part of the SDDC and zero-trust design. These capabilities may be provided natively by the virtualisation platform or through an integrated SDN/security solution proposed by the SI.

Response to the Pre-Bid Queries

29 1	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support distributed routing and security system policy migration with VMs.	Change Request : Request you to Change asked Clause as"Support distributed routing and security system policy migration with VMs Nativly or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

29 2	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support network analytics, flow assessment, and zero-trust policy enforcement.	Change Request : Request you to Change asked Clause as"SSupport network analytics, flow assessment, and zero-trust policy enforcemen or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

29 3	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable multi-site network and micro-segmentation across workloads.	Change Request : Request you to Change asked Clause as"Enable multi-site network and micro-segmentation across workloads. or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	These capabilities may be provided natively by the virtualisation platform or through an integrated SDN/security solution proposed by the SI.

Response to the Pre-Bid Queries

29 4	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide service chaining for north-south/east-west traffic inspection.	Change Request : Request you to Change asked Clause as"Provide service chaining for north-south/east-west traffic inspection. or with network & Security devices integration . - Justification: This is Network switch & Security Devices Integration Feature	These capabilities may be provided natively by the virtualisation platform or through an integrated SDN/security solution proposed by the SI.

Response to the Pre-Bid Queries

29 5	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support secure VPN connectivity between data centres and clouds.	Change Request : Request you to Change asked Clause as"PSupport secure VPN connectivity between data centres and clouds. or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

29 6	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support IPv4 and IPv6, extendable overlay and VLAN subnet capabilities.	Change Request : Request you to Change asked Clause as"Support IPv4 and IPv6, extendable overlay and VLAN subnet capabilities or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

29 7	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Offer an automated micro- segmentation policy recommendation engine.	Change Request : Request you to Change asked Clause as"Offer an automated micro-segmentation policy recommendation engine. or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	These capabilities may be provided natively by the virtualisation platform or through an integrated SDN/security solution proposed by the SI.

Response to the Pre-Bid Queries

29 8	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support virtual edge devices for routing, NAT, and security system functions.	Change Request : Request you to Change asked Clause as"Support virtual edge devices for routing, NAT, and security system functions or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

29 9	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable per-workload stateful firewalling and ALGs with central management.	Change Request : Request you to Change asked Clause as"Enable per-workload stateful firewalling and ALGs with central management or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

30 0	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support AES-256 encryption for data at rest and in transit with KMIP 1.1 compliance.	Change Request : Request you to Change asked Clause as"Support AES-256 encryption for data at rest and in transit with KMIP 1.1 compliance nativly or via external KMIP solution intregation - Justification: Option of external KMIP solution intregation will be allowed	The requirement is to support AES-256-equivalent encryption and KMIP-compliant key management, not necessarily a built-in KMS. KMIP-compliant external KMS in HA mode is acceptable. The revised clause to be read as: "Support AES-256-equivalent encryption for data at rest and in transit with KMIP 1.1-compliant key management, either natively or via integration with an external KMIP-compliant KMS in high-availability mode." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

30 1	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should edit or add network adapters, including multiple NIC models, Masquerade, and MAC address customization.	Removal Request : Please remove ask of Masquerade, and MAC address customization. Justification : This is not nactive Feature of Hypervisor , Pls remove this ask of Masquerade, and MAC address customization.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

30 2	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should include a compute virtualization layer on bare metal hardware with no dependence on a general-purpose OS, featuring proactive HA, DRS, replication, fault tolerance with continuous availability, and hot add of CPU, memory, and devices for Windows and Linux VMs.	Change Request : Request you to Change asked Clause as "The solution should include a compute virtualization layer on bare metal hardware with no dependence on a general-purpose OS, featuring proactive HA, DRS, replication, with continuous availability, and hot add of CPU, memory, and devices for Windows and Linux VMs. Justification: Please Remove ask of fault tolerance feature , as this specific to single OEM	The revised clause to be read as : "The solution should include a compute virtualization layer on bare metal hardware with no dependence on a general-purpose OS, featuring proactive HA/fault tolerance or equivalent technology, DRS, replication, with continuous availability, and hot add of CPU, memory, and devices for Windows and Linux VMs." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

30 3	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption.	Change Request : Please Change asked Clause as "The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption & using of San Stoarge base Relication Feature with or with out downtime . Justifictaion : asked solution need to be implemmeted with Storage Based Replication Feature with Downtime .	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

30 4	Volume of the RFP (II)	Annexure L Page No- 260 Automation	The software should support system tracking to audit and verify that machines comply. It should help to discover how a machine has changed over time or compare machines in running cluster to see how they are different.	Clarification: we Understand this is Inventory Tracking & Discovery Feature ask, Pls Confirm	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

30 5	Volume of the RFP (II)	Annexure L Page No- 260 Container Management Platforms	The container platform should be compatible and certified across MEITY empanelled cloud platforms/ Hyperscalers with Enterprise support. It must also provide a single cloud native platform support if and when need be.	Request to change to : The container platform should be - compatible with certified across MEITY empanelled cloud platforms/ Hyperscalers with Enterprise support. It must also provide a single cloud native platform support if and when need be. An equivalent offering may also be quoted	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

30 6	Volume of the RFP (II)	Annexure L Page No- 260 Container Management Platforms	The Container Platform should offer container scanning capability.	Clarification's help to explain the ask here , we Understand this is Security Infrastructure Feature to scan the Containers from security POV	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

30 7	Annexure L	Software LB	The licensing model shall allow flexible resizing (scale up/down) of virtual LB instances.	The licensing model shall allow scalability of virtual LB instances.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

30 8	Annexure L	Software LB	OEM to provide integrated WAF capabilities to protect applications from OWASP Top 10.	OEM to provide integrated WAF capabilities to protect applications from OWASP Top 10 with OWASP Top 10 Dashboard for hostistic view with inbuilt protection from BOT through CAPTCHA challenge and inbuilt BOT signatures, FTP, SMTP, HTTP, HTTPS and application layer DoS and DDoS attacks	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

30 9	Annexure L	Software LB	WAF should support custom security rules, positive security model, and REST-based policy automation.	WAF should support custom security rules, positive security model, and REST-based policy automation and must integrate with multiple third party vulnerability scanning tools to provide virtual patching	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

310	Annexure L	Server LB	WAF should support custom security rules, positive security model, and REST-based policy automation.	WAF should support custom security rules, positive security model, and REST-based policy automation and must integrate with multiple third party vulnerability scanning tools to provide virtual patching	Refer #309

Response to the Pre-Bid Queries

31 1	Annexure N	DDOS	Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation Throughput scalable to 20Gbps.	Restricted clause: Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Firewall,with 70 Gbps of Mitigation/Appliance Throughput	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 2	Annexure N	DDOS	The proposed appliance must provide: 1. Minimum Clean Traffic Throughput- 5 Gbps Scalable to 10 Gbps 2. Minimum SSL TPS/CPS of 40 K with RSA 2K keys via HW based Acceleration	The proposed appliance must provide: 2. Minimum SSL TPS/CPS of 80 K with RSA 2K keys via HW based Acceleration	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 3	Annexure N	DDOS	The proposed DDOS solution must be able to inspect all the SSL traffic and should also have provision to only inspect first packet for Lower Latency.	Restricted clause: The proposed DDOS solution must be able to inspect all the SSL traffic	As per RFP

Response to the Pre-Bid Queries

31 4	Annexure N	DDOS	Inspection and prevention are to be done in same hardware. OEM must be Make in INDIA Class -1 compliant as per Government MII Guidelines & subsequent amendments.	Restricted clause: Inspection and prevention are to be done in same hardware.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 5	Annexure N	DDOS	The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create signatures within 20 Secs for zero-day DDoS attacks and DNS DDOS attacks.	Restricted clause: The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create signatures for zero-day DDoS attacks and DNS DDOS attacks.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 6	Annexure N	DDOS	The Propose Appliance should Support multiple Protection option for Encrypted Attack Mitigation: a) Keyless SSL Protection b) First Request SSL Protection c) Selective Full SSL Protection d) Full SSL Protection	Restricted clause: Please delete this clause as it is specific to a single OEM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 7	Annexure N	DDOS	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection 7. Quantile DoS	Restricted clause: Please delete this clause as it is specific to a single OEM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 8	Annexure N	DDOS	The Proposed Solution should have User Defined Feed which should offers large scale IP or subnet blocking from an external 3rd party data feed using text file via manually update or integration with API. This should support upload of atleast 2M million IP addresses or subnets.	Restricted clause: Please delete this clause as it is specific to a single OEM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

31 9	Annexure N	DDOS	The Proposed Solution should have TLS Fingerprint Reputation Feed to block high-risk malicious fingerprints providing a additional proactive layer of protection.	Restricted clause: Please delete this clause as it is specific to a single OEM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

32 0	Annexure N	DDOS	The Solution should be at least EAL2.	Restricted clause: The Solution should be at least EAL2 or NDPP certified under common criteria program	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

32 1	Annexure N	DDOS	Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Adaptive Rate-Limit – deny real sources (resolvers) that generate too many repeating queries	Restricted clause: Please delete this clause as it is specific to a single OEM.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

32 2	Annexure N	DDOS		The DDOS must provide BOT mitigation functionality (including CAPTCHA) without having to go on internet for some cloud based service and must have inbuilt dedicated BOT signatures with different BOT categories like Trusted BOT, Untrusted BOT, Malicious Bot, Suspicious Browser, Unknown etc .	As per RFP

Response to the Pre-Bid Queries

32 3	Annexure N	DDOS		Solution must have anti-bot protection, Brute force protection with session tracking, Data Guard protection for Information leakage protection and advanced detection methods like- TPS (Transaction per Second) and JavaScript, CAPTCHA Challenge and device fingerprinting.	As per RFP

Response to the Pre-Bid Queries

32 4	Annexure N	DDOS		DDOS Operating System should be tested and certified for EAL 2 / NDPP (Network Device Protection Profile)/NDcPP (Network Device collaborative Protection Profile) or above under Common Criteria Program for security related functions	As per RFP

Response to the Pre-Bid Queries

32 5	Annexure N	Link Load Balancer	The proposed appliance must provide 10 GBPS of throughput from day 1 scalable upto 40 GBPS	The proposed appliance must provide 60 GBPS of throughput from day 1	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

32 6	Annexure N	Link Load Balancer	Appliance should be loaded with following interfaces on day one and should support virtualisation: - 10 Gbps Fiber port - 8 Nos. - 1G Copper port - 8 - Dedicated 10/100/1000 Mbps out-of-band management port - 2 No. and USB port- 1 No. each - RJ45/DB9 console port - 1 No.	Appliance should be loaded with following interfaces on day one and should support virtualisation: - 10 Gbps Fiber port - 8 Nos. -40 Gbps Fiber ports: 2 - Dedicated 10/100/1000 Mbps out-of-band management port -1 ~~2~~ No. and USB port- 1 No. each - RJ45/DB9 console port - 1 No.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

32 7	Annexure N	Link Load Balancer	The offered solution should provide full Authoritative DNS capability to understand records like A, AAAA	The offered solution should provide full Authoritative DNS capability to understand records like A, AAAA, CNAME, DNAME, HINFO, MX, NAPTR, NS, PTR, SOA, SRV, TXT. The solution should have an GUI integrated zone file management tool that simplifies DNS zone file management and reduce the risk of misconfiguration.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

32 8	Annexure N	Link Load Balancer	The proposed solution should Support Elastic Licensing Model and support below flexibility : 1. A single throughput/capacity license to be shared across physical and Virtual ADCs, on premise and in the cloud, regardless of location or type 2. A complete automation of ADC services deployment and maintenance, allowing the administrator not only to seamlessly spin up new ADC instances, but also use wizards and scripts to distribute the corresponding ADC service configuration – all at the same push of a button. 3. Reclaim capacity from decommissioned instances and reallocate it to new deployments, ensuring optimal license utilization	The solution should provide DNS SEC validation by acting as a recursive name server to verifies all of the signatures from the answer back to the closest trust anchor (a public key it knows and trusts). Should be able to do convert DNS requests to DNSSec on the fly	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

32 9	Annexure N	Link Load Balancer	The proposed device should use standard VRRP (RFC – 2338) for High Availability.	The proposed device should use standard VRRP (RFC – 2338) or equivalent for High Availability.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

33 0	Annexure N	Link Load Balancer	The proposed Device should have the Proximity based LLB which monitors 24/7 Full-path transaction completion through Application-aware full-path Health Monitoring module and automatically measures the real-time status of two-way routes between the network and the remote user or servers on the internet based on multiple parameters including latency, packet loss, Cost and load time of the link.	The proposed Device should have the Proximity based LLB which monitors 24/7 Full-path transaction completion through Application-aware full-path Health Monitoring module and automatically measures the real-time status of two-way routes between the network and the remote user or servers on the internet based on parameters like latency/packet loss/Cost or load time of the link.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

33 1	Annexure N	SLB	The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 2 Million 2) Network interfaces: 8x10G SFP+ and additional 16 x 10G SFP+ for future use 3) SSL Throughput: 20 Gbps with 40K SSL TPS/CPS with RSA 2k keys and 30K SSL TPS/CPS with ECC 4) Storage: 500 GB SSD scalable 1 TB 5) Memory: 32 GB from day 1 scalable to 128 GB	The appliance must support below minimum performance numbers: 1) L7 Request Per Second: 2 Million 2) Network interfaces: 8x10G SFP+ and additional ~~46~~ 8 x 10G SFP+ for future use 3) SSL Throughput: 30 Gbps with 60K SSL TPS/CPS with RSA 2k keys and 30K SSL TPS/CPS with ECC 4) Storage: 1 TB 5) Memory: 128 GB	Refer #166

Response to the Pre-Bid Queries

33 2	Annexure N	SLB		The proposed solution must support SSL VPN and Single Sign On functionality on same hardware solution running on same OS version from same OEM in future. The Solution must support the following checks and has ability to define different security checks for different user groups: * Able to perform Antivirus/Malware software checks, including checks for Enabled State, Engine & Database version, Last Scan, and Last Update of the antivirus software. * The proposed VPN Solution shall have functionality to restrict copy & paste on RDP session and same should be configurable. * Able to perform Operating System, Windows Registry, File or Process checks. * Able to check if mobile devices have been jailbroken	As per RFP

Response to the Pre-Bid Queries

33 3	Annexure N	WAF	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #207

Response to the Pre-Bid Queries

33 4	Annexure N	WAF	The proposed solution should Support Elastic Licensing Model and support below flexibility : 1. A single throughput/capacity license to be shared across physical and Virtual ADCs, on premise and in the cloud, regardless of location or type 2. A complete automation of ADC services deployment and maintenance, allowing the administrator not only to seamlessly spin up new ADC instances, but also use wizards and scripts to distribute the corresponding ADC service configuration – all at the same push of a button. 3. Reclaim capacity from decommissioned instances and reallocate it to new deployments, ensuring optimal license utilization	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #209

Response to the Pre-Bid Queries

33 5	Annexure N	WAF	The proposed device should use standard VRRP (RFC – 2338) for High Availability.	The proposed device should use standard VRRP (RFC – 2338) or equivalent for High Availability.	Refer #211

Response to the Pre-Bid Queries

33 6	Annexure N	WAF		WAF must provide inbuilt capability of API security including support for uploading swagger file and protect leakage of user credentials accessing the web applications using HTML field Obfuscation to protect against malware-based attacks and the solution should have capability to protect Credential Attacks that can steal credentials from the user's browser to avoid cyber exploits. It should be able to authenticate users based on browser type and version, operating system type and version. Necessary logs to be generated for audit and compliance.	As per RFP

Response to the Pre-Bid Queries

33 7	Annexure N	WAF		System should support inbuilt ability to encrypt the user credentials in real time at the browser level (data at rest) before the traffic hits the network so as to protect the credentials especially password, Aadhar number or any other sensitive parameter to protect from cyber actors, key loggers and credential stealing malware residing in the end user's browsers. Necessary logs to be generated for audit and compliance.	As per RFP

Response to the Pre-Bid Queries

33 8	Volume II	Section 5.1.4 ii System Support pt (I) page 33	Auditors/ RBI/CERT- In/statutory/regulatory authorities	Please confirm if DOP will be liasing with these external agencies and bear their cost	As per RFP

Response to the Pre-Bid Queries

33 9	Volume II	Section 5.1.4 ix Other Activities pt (k) page 37	The SI will be required to provide training to the DOP staff after each change in functionalities	Please provide details of 'DOP staff' mentioned here like count, location etc	Refer RFP Volume 2 Section 5.4

Response to the Pre-Bid Queries

34 0	Volume II	Section 5.1.4 ix Other Activities pt (m) page 37	Reconciliation	Please clarify if reconciliation of ATM transactions is also included in the scope of SI	Not in scope. Bidder to ensure integration.

Response to the Pre-Bid Queries

34 1	Volume II	Section 5.1.5.1 C. Ongoing Support Services pt (1) page 44	Supporting the DR and IT BCP frameworks prepared by DoP for key applications and systems.	Please clarify if SI is expected to support frameworks prepared by DOP (only for POSB solution) as is or there is enhancement/change expected as Change Request (CR)	As per RFP

Response to the Pre-Bid Queries

34 2	Annexure N	IDAM		Kindly confirm on all the employees/contractors/third parties who access the applications for IDAM scope. (except for customers). The IDAM solution must cover all users across the enterprise, including Finacle CBS and all supporting applications. Restricting scope creates identity silos and prevents effective cross-application Segregation of Duties (SoD) enforcement. Unified user coverage ensures consistent identity definitions, role models, and lifecycle controls, enabling enterprise-wide audit traceability, regulatory compliance, and least-privilege enforcement while maintaining identity uniformity across core banking and non-core systems.	As per RFP

Response to the Pre-Bid Queries

34 3	Volume II	5.1.3 Upgrade of Finacle CBS and Alert Solution	Additional clause to clauses 2, where it is asked "The upgraded system will also include comprehensive bank-centric alert features, including fraud detection alerts for staff, operational downtime notifications, escalation mechanisms, prioritized alert management, and compliance-driven reporting aligned with regulatory requirements. The solution must seamlessly integrate with the DoP's Finacle CBS, communication platforms to deliver scalable, secure, and user-friendly alerting capabilities."	The Following clause should be included in the IDAM Specifications. "The IDAM solution must provide out-of-the-box, productized integration with Finacle Core Banking Solution (CBS) version 10.2.x or higher, without reliance on custom development or system-integrator-built connectors. The integration shall support core identity and access use cases including role-based access control, segregation of duties, and audit logging for Finacle users. The bidder must demonstrate successful production deployments of this integration with Finacle 10.2.x in Indian BFSI institutions, and provide verifiable customer references within India upon request."	As per RFP

Response to the Pre-Bid Queries

34 4	Annexure N	IDAM	The solution should provide customers with a comprehensive solution for role-based governance, delivering capabilities to discover, design and manage roles, with the ability to discover roles using a top-down, bottom-up or a hybrid approach.	The Following clause should be replaced with the following comprehensive statement in IDAM Specifications. "The solution must provide comprehensive role engineering and governance through a unified, GUI-driven role modeling framework that supports top-down business roles and bottom-up technical roles, with graphical hierarchy visualization and nested role mapping. It must enforce policy-based, service-on-demand role assignment with real-time conflict and SoD checks, and include an advanced role mining and optimization engine that continuously analyzes access patterns to recommend, simulate, and validate roles—reducing entitlement sprawl and ensuring least-privilege governance. The solution must provide a fully out-of-the-box (OOB) role engineering and governance engine, not reliant on system-integrator customization or bespoke configuration."	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

34 5	Annexure N	IDAM	Sizing related Queries	How many applications are to be integrated under IDAM Scope ?	As per RFP

Response to the Pre-Bid Queries

34 6	Annexure N	MFA and SSO	Additional clause recommended for a high performance authentication platform	The Following clause should be included in the MFA and SSO Specifications. "The MFA authentication server must be provided as a dedicated, purpose-built hardware appliance from the OEM, specifically engineered for two-factor authentication (2FA) workloads. The appliance shall be OEM-supplied, hardened, and pre-configured to run the MFA authentication services, ensuring predictable performance and high availability. The OEM hardware appliance shall be fully supported, patched, and warranted by the OEM throughout its lifecycle."	As per RFP

Response to the Pre-Bid Queries

34 7	Annexure N	MFA and SSO	Additional clause recommended for a high performance authentication platform	The Following clause should be included in the MFA and SSO Specifications. "The MFA solution must provide its own OEM-manufactured hardware authenticators that are purpose-built for strong authentication and certified against recognized ISO standards for tamper evidence and physical security. The hardware authenticators shall demonstrate resistance to physical tampering, cloning, and unauthorized modification, with documented ISO-compliant certification. Third-party or non-certified authenticators shall not be acceptable. The OEM must take full responsibility for the security design, certification, lifecycle support, and continued compliance of the hardware authenticators used in regulated environments."	Refer #346

Response to the Pre-Bid Queries

34 8	Annexure N	MFA and SSO	Additional clause recommended for a high performance authentication platform	The Following clause should be included in the MFA and SSO Specifications. "The MFA OEM-manufactured hardware authenticator should support contactless as well as USB-A/USB-C, enabling authentication via tap on mobile devices or card readers, alongside FIDO2, PIV smart-card and HOTP token functions"	Refer #347

Response to the Pre-Bid Queries

34 9	Annexure N	MFA and SSO	Solution should allow captured recording to be filtered by type of actions without changing the code of the application	This clause should be removed from the MFA & SSO requirements	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

35 0	Annexure N	MFA and SSO	Solution should allow captured recordings to be searchable by keyword or date without changing the code of the application	This clause should be removed from the MFA & SSO requirements	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

35 1	Annexure N	MFA and SSO	Solution should be able to block specific users from downloading files from specific websites without changing the code of the application	This clause should be removed from the MFA & SSO requirements	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

35 2	Annexure N	MFA and SSO	Solution should be able to block specific users from copying text to the clipboard for specific websites without changing the code of the application	This clause should be removed from the MFA & SSO requirements	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

35 3	Annexure N	MFA and SSO	Sizing related Queries	How many users are under scope for both software and hardware authenticators and how many applications to be integrated under SSO ?	Requirement has been defined in the RFP. Bidder to propose the solution as per the solution architecture.

Response to the Pre-Bid Queries

35 4	Volume II	Section 5.1.5.2 a. Domain Services Table 9, page 47	Scope mentioned under Database Management and Middle ware Management is exactly same	Please clarify	As per RFP

Response to the Pre-Bid Queries

35 5	Volume II	Section 5.1.5.2 page 47	No details are provided for "Additional Services" section mentioned on Page 47 below Table 8		As per RFP

Response to the Pre-Bid Queries

35 6	Volume II	Section 5.1.5.2 b. Cross Functional Services Table 10, page 48	Incident and Ticket	Please clarify, which tool(s) are being used for Incident and Ticket Tracking, will these tools continue to be available through out the contract period to SI for use	SI shall integrate with HDMS solution developed by DoP. Tickets from the HDMS solution shall be transferred to the SI.

Response to the Pre-Bid Queries

35 7	Volume II	Section 5.1.5.2 Table 10, page 49	Software License Management - Manage compliance with all Software licenses by monitoring and auditing all Software use, regardless of fiscal responsibility for the Software.	Please Modify to: Software License Management - Manage compliance with all Software licenses by monitoring and auditing all Software used by POSB solution (in scope for SI under this RFP), regardless of fiscal responsibility for the Software.	As per RFP

Response to the Pre-Bid Queries

35 8	Volume II	Section 5.1.5.2 Table 10, page 49	Vendor Performance Management - Monitor and analyse the performance of each vendor (appointed by DOP) associated with and responsible for a part of the overall Technology Solution deployed by DOP.	Please Modify to: Vendor Performance Management - Monitor and analyse the performance of each vendor (appointed by DOP) associated with and responsible for a part of the POSB Solution (in scope for SI under this RFP) deployed for DOP.	This is specific to POSB IT Systems.

Response to the Pre-Bid Queries

35 9	Volume II	Section 5.2.1.2.7 pt (5) page 65	The SI shall ensure that the UAT environment is refreshed periodically with sanitised and updated data to reflect realistic business scenarios.	Please clarify if SI can take data from production and refresh in UAT as such or any kind of masking to be done before putting this data in UAT env	All data shall be appropriately masked or anonymised in line with RBI Guidelines, applicable statutory regulations, and compliance with DoP's security and data protection policies.

Response to the Pre-Bid Queries

36 0	Volume II	Section 5.2.1.2.8 pt (2) DR Drills page 67	The SI shall ensure that DR drills are conducted biannually (every six months) for all in-scope applications, databases, middleware, and infrastructure components,	Dependency of any external agency/third party has to be ensured by DOP. In case of non-readiness of other parties (not in control of SI) teh SI will not be held responsible for not happening of these DR drills. Please confirm.	Coordination with external agencies or third parties, where applicable, will be managed jointly with DoP. Non-readiness of parties outside the control of the SI shall be considered during scheduling and execution of the drills.

Response to the Pre-Bid Queries

36 1	General	Application Support	Support of all applications	Support of all existing applications should continue at least till 6 months beyond the start of contract	DoP shall facilitate continuation of support arrangements, wherever required, for a limited transition period to enable knowledge transfer (KT) and orderly handover to the selected bidder.

Response to the Pre-Bid Queries

36 2	Volume II	Section 4 – Current State Overview; Annexure A – Existing Infrastructure	The RFP provides existing infrastructure details for POSB systems while also referencing multiple systems such as PLI, Core Banking, Mobile Banking, Internet Banking, CTS, AML, RBA, etc. However, the infrastructure breakup across these systems is not clearly segregated.	Kindly confirm whether the infrastructure details provided in Annexure A are exclusive to POSB systems only or inclusive of PLI and other allied systems. If inclusive, request application/system-wise segregation of infrastructure.	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

36 3	Volume II	Section 4; Annexure A	The total number of servers inferred from various sections and applications does not clearly reconcile with the server inventory listed in Annexure A.	Kindly confirm the authoritative total server count to be considered for bid purposes, along with environment-wise breakup (Production / DR / Test / UAT / Staging).	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

36 4	Volume II	Annexure A – Existing Infrastructure	Detailed RAM and CPU configuration is not consistently available for all servers listed across DC and DR environments.	Kindly provide server-wise RAM and CPU configuration, or alternatively an average RAM per server category, to enable accurate capacity planning and solution sizing.	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

36 5	Volume II	Section 5.1.4 – Operations and Maintenance of Existing Applications	The SI is responsible for 24x7 operations and SLA compliance; however, the monitoring scope for non-production environments is not explicitly defined.	Kindly clarify whether enterprise monitoring requirements apply only to Production and DR, or whether non-production environments (UAT/Test/Training/Sandbox) are also in scope for monitoring and sizing.	As per RFP

Response to the Pre-Bid Queries

36 6	Volume II	Section 5.1.4; Section 6 – SLA	The RFP mandates application and infrastructure monitoring but does not explicitly define the depth of monitoring expected.	Kindly clarify whether DoP expects infrastructure-only monitoring or full-stack monitoring covering applications, databases, integrations, and end-to-end transaction flows to meet SLA requirements.	SI shall be responsible for monitoring the entire POSB IT systems.

Response to the Pre-Bid Queries

36 7	Volume II	Section 5.1.4 (vi) – Application Monitoring Support	Log management is mandated across all layers, but log volume, retention period, and critical log sources are not specified.	Kindly specify the expected log retention period, approximate daily log volume, and whether logs from applications, databases, middleware, OS, and security systems are all in scope.	Approximate log volume per day is around 20GB for Middleware and Web Logs. On database, standard user audit is enabled with 30 days retention. There is no auditing enabled for Operating systems and error logs are cleared regularly. Application logs are maintained only for one day and the size is around 60GB.

Response to the Pre-Bid Queries

36 8	Volume II	Section 6.10 – SLAs for conducting DR Drills	DR drills and SLA compliance are specified; however, monitoring expectations during DR drills are not clearly detailed.	Kindly clarify whether real-time monitoring and reporting during DR drills is expected to be equivalent to Production monitoring, and whether DR infrastructure is to be monitored continuously or only during drills.	DR infrastructure is to be monitored continuously.

Response to the Pre-Bid Queries

36 9	Volume II	Section 2.2 – Background of the Project; Annexure O – Key Statistics	The RFP highlights scale and growth in users, accounts, and transactions but does not specify infrastructure growth assumptions over the contract period.	Kindly provide indicative year-on-year growth assumptions for servers, users, and transaction volumes to be considered for scalable solution sizing.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

37 0	General	Volumetrics of Transactions	Volumetrics and year-on-year growth projections of transactions through different channels	Volumetrics and year-on-year growth projections of transactions through different channels till end of contract, needs to be provided for proper sizing	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

37 1	Annexure N	MFA & SSO	Solution should be able to provide an option to enforce capturing of each step taken during a web session for selected users, without changing the code of the application, for audit purposes at least 50 license only.	This clause is not relevant for MFA and SSO; hence, it should be omitted.	Clause is omitted. Bidders may refer to Corrigendum Annexure N for updated details of the requirement.

Response to the Pre-Bid Queries

37 2	Annexure N	MFA & SSO	Solution should allow captured recording to be filtered by type of actions without changing the code of the application	This clause is not relevant for MFA and SSO; hence, it should be omitted.	Refer #349

Response to the Pre-Bid Queries

37 3	Annexure N	MFA & SSO	Solution should allow captured recordings to be searchable by keyword or date without changing the code of the application	This clause is not relevant for MFA and SSO; hence, it should be omitted.	Refer #350

Response to the Pre-Bid Queries

37 4	Annexure N	MFA & SSO	Solution should be able to block specific users from downloading files from specific websites without changing the code of the application	This clause is not relevant for MFA and SSO; hence, it should be omitted.	Refer #351

Response to the Pre-Bid Queries

37 5	Annexure N	MFA & SSO	Solution should be able to block specific users from copying text to the clipboard for specific websites without changing the code of the application	This clause is not relevant for MFA and SSO; hence, it should be omitted.	Refer #352

Response to the Pre-Bid Queries

37 6	Volume II	Page no. 51 Clause: 5.2.1.1 Facility Requirements Sub Clause: 5.2.1.1.1 General Requirements	The proposed DCF shall have a minimum Tier-III standard certificate by an agency such as Uptime Institute or a TIA 942 design certificate.	Rrequest DOP to kindly consider and include the Rated classification as well.	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

37 7	Volume II	Annexure I Section B: Physical Security Requirement Point no. 4	The proposed facility shall have 24x7 surveillance (CCTV with built-in intelligence and auto triggering of alert/response for unusual activities).	Requesting DOP to relax the the requirement of video analytics–based auto alerting.	The revised clause to be read as: The facility shall have 24×7 CCTV surveillance with continuous monitoring of DoP specific caging areas and defined procedures for detection, alerting, and response to unusual activities. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

37 8	Volume II	Annexure I Section B: Physical Security Requirement Point no. 4 (subpoint 4)	Surveillance should be integrated with IBMS as well as the NOC central monitoring.	Requesting DOP to relax this compliance to permit integration with IBMS only.	The revised clause to be read as: Surveillance should be integrated with IBMS. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

37 9	Volume II	Annexure I Section B: Physical Security Requirement Point no. 7	The hosting space entrance & exit should be accessible using the biometric access system with minimum two-factor authentication (fingerprint sensor + access card control system) in addition to the physical lock (Palm sure scanner, iris scanner, face scanner may be considered).	Requesting DOP to relax requirement of palm vein and iris scanners.	The revised clause to be read as: The hosting space entrance & exit should be accessible using the biometric access system with minimum two-factor authentication (fingerprint sensor/ Biometric + access card control system). in addition to the physical locking mechanism. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 0	Volume II	Annexure I Section B: Physical Security Requirement Point no. 9	The DCF Provider shall provide a dual door/trap door solution at the main entry of the Server Room to avoid tailgating. Apart from this, the main entrance to the DC area should have a half-height Turnstile/Tripod/Flap barrier, along with access card access.	While a dual door / trap door solution is not deployed, the facility implements alternative access control measures designed to prevent tailgating and unauthorized entry. These include full-height turnstiles and access-controlled lifts with card-based authentication and monitoring. Relaxation is requested to accept the existing configuration.	As per RFP

Response to the Pre-Bid Queries

38 1	Volume II	Annexure I Section C: Power Point no. 2	The proposed co-location facility for Data Centre hosting shall have the incoming utility power supply from two different sub-stations (redundancy planning) as the primary source, and automatic switchover to Data Centre Continuous Rated Diesel Generators set as a secondary source. In case of power failure, automatic switchover to the DG set as a secondary source provision should be available. The Diesel Generators shall have sufficient fuel to cater to the infrastructure for a minimum of 72 hours in the event of a major outage. The fuel lines providing fuel to the Diesel Generators shall be in redundancy along with the supply pumps as well.	Relaxation is requested to modify the diesel fuel storage requirement from 72 hours to a minimum of 24 hours, in alignment with industry-accepted standards and best practices.	The revised clause to be read as: The proposed co-location facility for Data Centre hosting shall have the incoming utility power supply from two different sub-stations (redundancy planning) as the primary source, and automatic switchover to Data Centre Continuous Rated Diesel Generators set as a secondary source. In case of power failure, automatic switchover to the DG set as a secondary source provision should be available. The Diesel Generators shall have sufficient fuel to cater to the infrastructure for a minimum of 24 hours in the event of a major outage. The fuel lines providing fuel to the Diesel Generators shall be in redundancy along with the supply pumps as well. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 2	Volume II	Annexure I Section C: Power Point no. 3	Backup generators (Redundant) should be capable of providing power backup for 72 hours. Backup generators should be capable of providing power continuously for at least 72 hours, and even during the refilling period of fuel tanks. The capacity of each set of diesel generators should be sufficient to take care of the entire power load of the Data Centre. The DCF Provider should ensure an uninterrupted supply of diesel to the DG with an adequate storage facility. The Diesel Generators shall be of Data Centre Continuous (DCC) rating type.	Relaxation is requested to modify the diesel fuel storage requirement from 72 hours to a minimum of 24 hours, in alignment with industry-accepted standards and best practices.	The revised clause to be read as: Backup generators (Redundant) should be capable of providing power backup for 24 hours. Backup generators should be capable of providing power continuously for at least 24 hours, and even during the refilling period of fuel tanks. The capacity of each set of diesel generators should be sufficient to take care of the entire power load of the Data Centre. The DCF Provider should ensure an uninterrupted supply of diesel to the DG with an adequate storage facility. The Diesel Generators shall be of Data Centre Continuous (DCC) rating type. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 3	Volume II	Annexure I Section C: Power Point no. 7	Two separate power paths from the UPS are to be provided to the Server room area and the network communication area. The UPS should be configured in parallel active mode, and each should not be loaded more than % of its capacity.	Dept of Post is requested to kindly share the understanding of UPS configured in parallel active mode as we have UPS with N+N Redundancy	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

38 4	Volume II	Annexure I Section C: Power Point no. 9	The UPS systems should be fault-tolerant with 2 separate paths for the power supply to each rack. Adequate battery backup should be available for maintaining the uptime requirement of the IT Infrastructure.	In the previous point , the UPS redundancy has been specified as N+1 and fault-tolerant. However, as per TIA-942 Rated-3 / Uptime Tier III requirements, the UPS system is required to be concurrently maintainable and not fault-tolerant. Fault-tolerant design is a requirement for Tier IV (Rated-4) facilities. We seek clarification here.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

38 5	Volume II	Annexure I Section F: Server Room Area Point no. 2	The server room area should have a raised floor height of 2ft.	The Server Room area is designed with a raised floor height of minimum 2 feet. Modern Data Centre designs increasingly adopt raised floor heights exceeding 2 feet to effectively support medium- and high-density deployments, improved airflow management, enhanced cable routing, and scalability requirements. In view of evolving industry practices, we request the clause be revised from “raised floor height of 2 feet” to “raised floor height of minimum 2 feet.”	The revised clause to be read as: The server room area shall have a raised floor height of minimum 2 ft . Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 6	Volume II	Annexure I Section F: Server Room Area Point no. 4	DC Power (UPS output/ power input).	Dept of Post is requested to clarify that do we need DC power in Data Centre.	The revised clause to be read as: AC power through UPS output as per RFP specifications. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 7	Volume II	Annexure I Section F: Server Room Area Point no. 26	Perimeter Wall and Doors should have at least 1 1-hour fire Rating.	The previous clauses are requesting the same as 2 hours. Please clarify.	The revised clause to be read as: "The Data Centre facility shall have fire-rated construction for DC halls and all critical areas (including UPS, electrical and battery rooms) with minimum 2-hour fire resistance rating for walls and doors, in compliance with applicable NBC/TIA- 942 or equivalent standards." Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

38 8	Volume II		The DCF Provider shall furnish a complete water leak detection system, including (but not limited to) electronic alarm modules, water sensing cable, graphic display map, auxiliary equipment, etc. The system shall be capable of automatically detecting the presence of water or any other liquid at any point covering the entire DC and should be able to generate an alarm and locate, with a digital display, the point of contact.	We install the Water leak detection system in the PAHU Galleries area prone to water leakage , So we request to please modify the same.	As per RFP

Response to the Pre-Bid Queries

38 9	Volume II	Annexure I Section H: Building Management System Point no. 14	Shall provide on monthly basis and/or upon request from DoP, the details of people accessing all the facilities provided to DoP such as server room area, communication area by sharing entries made in the security register that contains the name, company and contact details of persons entered, purpose of entry, etc. along with reports, access logs, CCTV video clips etc.	We only share the entire of the customer specified area that is caging and not for the communication room as ours is a shared facility so request Dept of Post to modify the clause accordingly.	The revised clause to be read as: The Service Provider shall provide, on a monthly basis and/or upon request from DoP, details of personnel accessing all facilities provided to DoP, including the server room area, caging area, and any other area designated for DoP. Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

39 0	Volume II	Section 5.2.4.3 Pt (17) page 90	The SI is required to guarantee the retention of data backup until the occurrence of the last transaction in the system.	Please clearly specify the exact backup retention period of transactions, separately in HOT and Cold backup	As per RFP

Response to the Pre-Bid Queries

39 1	Volume II	Section 5.2.4 Point 22 Page 83	The SI is required to follow the below matrix for installing the application instances in DC, DR and NDR environments within the infrastructure.	The matrix indicates Preprod setup to be of 100% capacity as production both in DC and DR. Please clarify a. Does it also require 100% storage capacity to be provisioned? . Does the matrix apply to all the applications in the landscape?	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

39 2	Volume II	Section 6.7.3 Point 2 Page 149	Syncing of Training, UAT, Pre Pre-Prod environments after any change in the Production Environment.	Typically, the pre-prod environment is maintained identical to the production version. The training environment is driven by the training requirements and can be maintained at the same level as production. However, the UAT environment being used for UAT activities will always have code for recent changes being validated. Please clarify if the environments are to be maintained at the same versions or should be allowed to vary depending on the requirements.	The Training environment shall be maintained functionally equivalent to the Production environment. The UAT environment shall align with the Pre-Production setup and host upcoming changes/releases for validation. All changes shall be tested and validated in UAT prior to deployment to Production

Response to the Pre-Bid Queries

39 3	Annexure N	Application Performance monitoring	Solution should support automatic javascript injection for real user monitoring, by simple installation of Agent on the following web server technologies and should not require any manual changes in web pages or any configuration files : IBM HTTP Server, Java Servlet based web applications, ASP.Net core, Microsoft IIS, NGINX, Node.JS, Oracle HTTP SERVER, APACHE HTTP SERVER	This Clause is highly OEM-specific and typically not supported natively by most observability platforms, including Elastic. Elastic's RUM solution requires a one-time manual insertion of the JavaScript agent into web pages or templates, which is a standard and widely accepted approach. We recommend that the RFP language remain open to solutions that support streamlined and well-documented RUM agent deployment, rather than mandating fully automated injection across all web server technologies, to ensure flexibility and compatibility with best-in-class observability platforms.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

39 4	Annexure N	Application Performance monitoring	Solution should automatically discover all the deployed applications on a server or a virtual machine, and automatically enable the code level monitoring for all applications without any changes to the code or configuration files. It should not require manual placement of jar files, or any other libraries or files to enable monitoring.	This Clause is highly OEM-specific and typically not supported natively by most observability platforms, including Elastic. Elastic provides streamlined onboarding and automation tools—such as the Elastic APM agent attacher for Kubernetes and automated deployment scripts—to simplify agent installation and minimize manual steps. However, enabling deep code-level monitoring generally requires an initial agent deployment or minimal configuration, which is standard across leading observability solutions. We recommend that the RFP language remain open to solutions that support automated discovery and simplified agent deployment, rather than mandating fully native, zero-configuration code-level instrumentation, to ensure	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

39 5	Annexure N	Application Performance monitoring	Solution should support automated detection of new applications or microservices and enabled monitoring be default. In a monitored environment, if any new microservice or application service is deployed, solution should discover it automatically, enabled deep monitoring with code and query level insight and discover the dependence and relationships without any manual action or configuration change of any kind.	This Clause is typically an OEM-specific capability, often requiring proprietary hooks or platform-specific integrations. Elastic provides robust automated discovery and default monitoring for new services at the infrastructure and log level, and offers tools to streamline application-level instrumentation—especially in orchestrated environments like Kubernetes. However, enabling comprehensive code-level and query-level monitoring for all new services generally requires an initial agent deployment or minimal configuration. We recommend that the RFP language remain open to solutions that support automated discovery and streamlined onboarding, rather than mandating fully native, zero-configuration deep instrumentation, to ensure flexibility and access to best-in-class observability platforms.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

39 6	Annexure N	Application Performance monitoring	Solution should support comprehensive monitoring of cloud services. It should support monitoring of all cloud managed services, baseline the metrics automatically and alert when cloud services behave abnormally. Additionally it should establish automatic cause and effect relationship between application service and cloud service for accurate root cause analysis.	We request clarification regarding the requirement for comprehensive monitoring of all cloud-managed services, including the automatic baselining of metrics, anomaly alerting, and the establishment of automatic cause-and-effect relationships between application and cloud services for root cause analysis. While Elastic offers extensive integrations for monitoring a wide range of cloud services and provides advanced machine learning features for automatic baselining and anomaly detection, it is important to note that fully automated root cause analysis—where the platform independently determines and presents definitive cause-and-effect relationships—is generally a specialized capability found in certain OEM or AIOps solutions. Elastic excels at correlating application and cloud service metrics, visualizing dependencies, and surfacing likely contributing factors, but we request that the RFP remain open to solutions that provide strong correlation and integration capabilities, rather than mandating native, fully automated root cause analysis. This approach ensures flexibility and allows organizations to leverage best-in-class	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

				observability and analytics tools.	

Response to the Pre-Bid Queries

39 7	Annexure N	Application Performance monitoring	Solution should capture process crashes (JVM Crash, .NET crash or any other process). The provided crash details include the signal that killed the process (for example, Segmentation fault or Abort), the execution stack frame that crashed, and more. The crash type—such as a native core dump, Java core dump, or abnormal program exit due to an exception should be available.	The requirement for the solution to natively capture and analyze process crashes (such as JVM or .NET process terminations), including details like the signal that killed the process, execution stack frames, and crash type (e.g., native core dump, Java core dump, or abnormal program exit), such deep crash diagnostics and core dump analysis are typically provided by specialized OEM tools or platform-specific profilers, rather than by general-purpose observability platforms. Elastic's observability suite can ingest and analyze crash-related logs and events from external sources, enabling centralized alerting, correlation, and visualization of crash incidents. We request that the RFP language remain open to solutions that support integration with leading crash analysis tools, rather than mandating native core dump or stack frame analysis, to ensure flexibility and leverage best-in-class capabilities for both observability and crash diagnostics.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

39 8	Volume II	Section 5.2.4.7 Testing Page 93	Verify data migration pre and post using reputable testing tools facilitated by an external testing agency. The SI is required to address various testing aspects through an external testing agency	Please clarify that if only the tools facilitated by an external testing agency are to be used OR testing also needs to be conducted/results to be verified by external testing agency	Testing results to be verified by external testing agency (CERT-In and STQC empaneled).

Response to the Pre-Bid Queries

39 9	Volume II	Section 5.2.5 Application Development & Integration of new functionalities Page 93	The testing shall be performed in accordance with the approved test plans and test cases	Please clarify if all the test plans and test cases will be approved by DOP	Test plans and test cases shall be submitted to DoP for review/approval prior to execution. Post execution, detailed test reports and results shall also be shared with DoP.

Response to the Pre-Bid Queries

400	Volume II	Section 5.2.5.4 Data Archival & Retrieval Solution	implementation of a Data Archival and Retrieval Solution for POSB	Please elaborate the needs of Retrieval solution in details	As per RFP

Response to the Pre-Bid Queries

40 1	Annexure N	Application Performance monitoring	Solution should support mobile app monitoring and crash analytics for mobile applications developed for iOS and Android frameworks (e.g. ReactNative, Flutter, Cordova or equivalent). It should offer analytics like Device types impacted by crash, OS version and app versions where crashes are observed, stacktrace of crash, and users impacted by crash.	We request for clarification on the requirement for native mobile app monitoring and crash analytics for iOS and Android frameworks (including React Native, Flutter, Cordova, or equivalent). In the observability industry, comprehensive crash analytics—such as automatic capture of device types, OS versions, app versions, stack traces, and user impact—are typically provided by specialized OEM solutions like Firebase Crashlytics, Sentry, or Bugsnag, rather than by general-purpose observability platforms. Elastic's observability suite offers robust backend and API monitoring, and can ingest and analyze crash data from third-party mobile analytics tools, enabling unified visualization and reporting. We recommend that the RFP language remain open to solutions that support integration with leading mobile crash analytics platforms, rather than mandating native SDK support, to ensure flexibility and access to best-in-class capabilities for both mobile and backend monitoring.	As per RFP

Response to the Pre-Bid Queries

40 2	Annexure N	Application Performance monitoring	CPU Overhead of the monitoring agent should be less than 3%. To maintain this, solution should not toggle sampling rate and should be able to offer highest data capture rates. Solution should not revert to high sampling for maintaining overhead	Regarding the requirement that the monitoring agent's CPU overhead must remain below 3% at all times, without toggling sampling rates and while maintaining the highest data capture rates. In the observability industry, it is common for leading solutions to provide configurable sampling options, allowing customers to balance data fidelity with resource consumption based on their unique workloads and environments. Agents are engineered for low overhead and can be configured for full data capture (100% sampling) while typically maintaining CPU usage well below 3%. However, it is important to note that the ability to guarantee fixed, ultra-low overhead at the highest data capture rates—without any adaptive sampling or data throttling—is highly OEM-specific and may not reflect standard industry practice. We recommend that the RFP language allow for solutions that offer transparent, configurable sampling and resource controls, ensuring both performance and flexibility, rather than mandating a fixed approach that could limit the range of best-in-class observability offerings.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

40 3	Annexure N	Application Performance monitoring	Solution should offer a common agent both for applications and Server Infrastructure monitoring (including VM/Containers/Kubernetes/EC 2 etc). This would help the operations team to minimize administrative overhead of managing multiple agents, and also ensure that infrastructure and application services dependencies are automatically discovered and mapped.	Please Clarify the requirement for a "common agent" that supports both application and server infrastructure monitoring (including VMs, containers, Kubernetes, EC2, etc.) within a single binary. In the observability industry, it is standard practice for leading platforms—including Elastic—to provide specialized agents: Elastic Agent for infrastructure and cloud resource monitoring, and language-specific APM agents for deep application instrumentation. This approach ensures optimal performance, security, and flexibility for diverse technology stacks. Elastic's tightly integrated agents work seamlessly together to provide unified visibility, automatic discovery, and dependency mapping across both infrastructure and application layers, while minimizing administrative overhead. We request that the RFP language remain open to solutions that deliver unified observability through integrated agents, rather than mandating a single OEM agent, to ensure the best fit for modern, heterogeneous environments and to leverage the strengths of best-in-class monitoring technologies.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

40 4	Annexure N	Application Performance monitoring	Solution should capture and replay the user interactions like a movie. This would help the teams to understand and reproduce UI related usability issues and frustration points present in the application interface and help them teams to improve overall usability. The video capture should be anonymized to protect user privacy	We would like to seek clarification regarding the requirement for the solution to "capture and replay user interactions like a movie," enabling teams to visually reproduce UI-related usability issues and frustration points. While this feature is highly valuable for usability analysis, it is important to note that such session replay capabilities—where user interactions are recorded and replayed as a video—are typically provided by specialized OEM solutions (e.g., FullStory, Glassbox) rather than core analytics or observability platforms. Elastic's observability suite offers comprehensive real-time analytics, user journey tracking, and anomaly detection across web and mobile applications, and can be seamlessly integrated with leading session replay tools to deliver a unified experience. We request that the RFP language remains open to solutions that provide native or integrated support for session replay, rather than mandating this as a core specific OEM feature, to ensure the broadest and most flexible range of offerings and to leverage best-of-breed capabilities in both observability and session replay domains.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

40 5	Volume II	Scope of Work- Page 226	36 X MS SQL Databases	How many MS SQL Servers will be part of the data & database activity monitoring scope? What are the versions and counts? What is the total volume? Please provide detailed architecture for Production DBs	As per RFP

Response to the Pre-Bid Queries

40 6	Volume II	Scope of Work- Page 232	32 X Oracle Servers Oracle DB Enterprise Edition X 377 Oracle RAC X 288	How many Oracle Servers will be part of the data & database activity monitoring scope? What are the versions and counts? What is the total volume? Please provide detailed architecture for Production DBs	As per RFP

Response to the Pre-Bid Queries

40 7	Volume II	Scope of Work- Page 226	125837 X CAL/Devices	How many users are there in the Active Directory?	As per RFP

Response to the Pre-Bid Queries

40 8	Volume II	Scope of Work- Page 216	DS 8870- 630TB DS 8910- 335TB	How much of this storage is in form of CISF/NFS share which be part of data classification scope? Are there any NAS fillers in scope? If yes what are the make, modell, count and storage?	Refer Existing Inventory details in RFP/Corrigendum.

Response to the Pre-Bid Queries

40 9	Volume II	Scope of Work- Page 261	Aadhar Data Vault- - Mysql 8.0.36	How many MySQL Servers will be part of the data & database activity monitoring scope? What are the versions and counts? What is the total volume? Please provide detailed architecture for Production DBs	Refer Existing Inventory details in RFP/Corrigendum.

Response to the Pre-Bid Queries

41 0	Volume II	Scope of Work- Page 266	Mobile Banking-PostgreSQL	How many My SQL Servers will be part of the data & database activity monitoring scope? What are the versions and counts? What is the total volume? Please provide detailed architecture for Production DBs	Refer Existing Inventory details in RFP/Corrigendum.

Response to the Pre-Bid Queries

41 1	Volume II	Scope of Work- Page 234 and 235	278 + 80 at DC 278 + 80 at DR	How many database servers will be part of the data & database activity monitoring scope? What are the versions and counts? What is the total volume?	Refer Existing Inventory details in RFP/Corrigendum.

Response to the Pre-Bid Queries

41 2	Volume II	Scope of Work- Page 216	Application and Associated Databases	Please provide current used size of all DBs mentioned in the list e.g. CBS, MIS, FAS, EB, MB, etc	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

41 3	Volume II	Scope of Work- Page 232	Supported version of Databases	Does all DBs are on Supported Version? Please provide exact version of all Production DBs	Yes supported, CBS/EB/MB/FAS/MIS- Oracle 19.24.0.0 and SASAMLand RBA- 12.2.0.10

Response to the Pre-Bid Queries

41 4	Volume II	Scope of Work- Page 216	Application and Associated Databases	Please provide detail on Transactions Per Second (TPS) for each applications listed	As per RFP

Response to the Pre-Bid Queries

41 5	Volume II	Scope of Work- Page 28	Tools and Reporting setup	Please provide detail on Monitoring tool used for Databases, Queries, etc.	Native DB tools.

Response to the Pre-Bid Queries

41 6	Volume II	Provision and Maintenance of Training Env pt (b) page 124	The SI shall be responsible for provisioning required applications, databases, and operating systems at all training locations.	Is it about the desktops/laptops to be used at training locations. If yes, then please provide details of locations, number of desktops (make, model etc) at each location	DoP shall provision for its Trainees.

Response to the Pre-Bid Queries

41 7		AnnexureN / DDOS / 1	Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation Throughput scalable to 20Gbps.	Change request:Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation/Flood Prevention Throughput scalable to 20Gbps.	Refer #311

Response to the Pre-Bid Queries

41 8		AnnexureN / DDOS / 24	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active mode	Change Request:The Proposed Solution should be able to work in High Availability (HA) architecture and should be deployable in an Active-Standby or Active-Active design	All security appliances to be deployed in High Availability mode with redundancy.

Response to the Pre-Bid Queries

41 9		AnnexureN / DDOS / 29	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection 7. Quantile DoS	Change Request: The appliance should have below Security Protection Profiles: 1. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection	Refer #317

Response to the Pre-Bid Queries

42 0		AnnexureN / DDOS / 38	Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Adaptive Rate-Limit – deny real sources (resolvers) that generate too many repeating queries	Change Request:Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Rate-Limit – Allows to configure the rate limits . should also support learning and suggestion of thresholds while implementing	Refer #321

Response to the Pre-Bid Queries

42 1	II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	15. CTS - An online image-based cheque clearing system where cheque images and Magnetic Ink Character Recognition (MICR) data are captured at the collecting branch and transmitted electronically, eliminating the actual cheque movement.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 2	II	Page 41: 5.1.4.5 Operations and Maintenance Support for the Centralised Cheque Clearing System (CTS)	DoP has an ongoing contract with M/s Oritso Pvt. Ltd. for Monitoring and Maintenance Support for the Centralised Cheque Clearing System (CTS), valid until June 2026. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 3	II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	eKYC/ADV - Applications integrated with UIDAI to enable Aadhaar-based authentication and KYC services, with secure storage of Aadhaar data in compliance with UIDAI guidelines.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 4	II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	DoP has an existing contract with M/s Integra Micro Solutions for the Maintenance of Aadhaar-compliant eKYC and Data Vault, valid until November 2029. Both functionalities have been implemented and are currently being maintained by Integra's resources. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines, or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format. This includes support for Aadhaar Data Vault (ADV), an eKYC Solution, and a Hardware Security Module (HSM), in compliance with the guidelines issued by UIDAI and relevant regulatory bodies.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 5	II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	3. The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-2 Level 3 or higher standards.	As FIPS 140-2 validation certificates will be moved to the Historical List in September 2026, they will no longer be considered active for regulated compliance or new procurements. Request: Replace the existing clause with the following updated compliance requirement: "The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-3 Level 3 or higher standards."	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 6	II	Page 17: 4. Current State Overview Table 4: Functional Blocks of POSB	9. Card Management System - Card Management System is a solution that manages the complete ATM/Debit Card Issuance cycle for DoP customers.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

42 7	II	Page 16: 4. Current State Overview	13. ATM Switch - ATM Switch is required to handle all ATM transactions of the customers	Please include a dedicated HSM technical specification as part of this requirement.	ATM switch is not in scope. Bidder has to ensure integration.

Response to the Pre-Bid Queries

42 8		Database Activity Monitoring	The solutions should provide customisable policies using algorithms as well as algorithmic validators wherever possible to discover and classify sensitive records in MySQL.	Our understanding is that DOP have 2 core 36 on-prem MS SQL databases, and there are no other databases. Considering the expansion, please confirm if the number of databases can go up to 100?	As per RFP

Response to the Pre-Bid Queries

42 9	II	Volume II Page 96	The SI is required to provide a collaborative SOC team for mitigating potential security threats. The SI is required to provide below product stack to run SOC: 1. Data & Database Activity Monitoring 2. Multi Factor Authentication (MFA) & Single Sign On (SSO) 3. Identity and Access Management (IDAM) 4. Domain Name System (DNS) 5. Secured Internet Access 6. Security Information and Event Management (SIEM) 7. User and Entity Behaviour analysis (UEBA), 8. Security Orchestration, Automation and Response (SOAR), 9. Threat Intel Management (TI) 10. Network Traffic Analysis (NTA) 11. Application Performance Monitoring 12. Next-Gen Firewall 13. Data Loss Protection (DLP) 14. Distributed Denial of Service (DDoS) 15. Host based Intrusion Prevention System (HIPS) 16. Network Intrusion Prevention System (NIPS) 17. Privileged Identity Management (PIM) 18. Privileged Access Management (PAM) 19. Sandbox 20. Link Load Balancer (LLB) 21. Server Load Balancer (SLB) 22. Web Application Firewall	Annexure N specifically outlines requirements for a 'Secure Browser,' yet this component is missing from the main Scope of Work (SOW) and Bill of Material (BoM). To ensure alignment and avoid ambiguity, we request that the DOP incorporate the 'Secure Browser' into the primary SOW and BoM as a mandatory line item.	Bidders may refer to the Corrigendum for updated details of the requirements.

Response to the Pre-Bid Queries

			(WAF) 23. Attack Surface Management (ASM) 24. Decoy-based Threat Detection		

Response to the Pre-Bid Queries

43 0	II	Page 96, Volume II Technical Specifications BOQ_937457.xls	Clarification :	We observe that none of the mandatory security components described in the Technical Scope are captured in the commercial BOQ. The is request is to include these items in BOQ , providing specific sizing and quantity details for the DC, DR, and NDR locations for each component.	In the commercial BoQ Bidder is required to add the components meeting the requirements in the RFP and Corrigendum.

Response to the Pre-Bid Queries

43 1	II	Page 89 5.2.4.3 Integration, Clause No. 11	The SI is required to deploy engineers from the OEM for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	Propose to modify as follows, The SI is required to deploy manpower from the OEM or OEM certified engineer for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	Bidders may refer to the Corrigendum for updated details of the requirements. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.

Response to the Pre-Bid Queries

43 2	II	Page 96, Volume II AnnexureN "Secure Internet Access" SN. 5	Clarification : Kindly confirm number of user / number of license for Secure Internet Access	Kindly confirm number of user / number of license for Secure Internet Access	SIA solution license to be sized for minimum 500 users from day 1 scalable upto 1000 users

Response to the Pre-Bid Queries

43 3	II	Page 96, Volume II AnnexureN "SIEM" SN. 1	Solution must provide capabilities of SIEM, SOAR, NTA, TIP, Threat hunting, AI/ML Analytics and UEBA OOTB within a single unified frontend and datalake solution.	Clarification : We understand that the proposed solution is required to provide a single, unified management dashboard for the operation of all specified modules, including SIEM, SOAR, NTA, TIP, Threat Hunting, AI/ML Analytics, and UEBA.	The revised clause to be read as: "Solution must provide capabilities of SIEM, SOAR, TIP, Threat hunting, AI/ML Analytics and UEBA OOTB within a single unified frontend and datalake solution" Bidders may refer to Corrigendum Annexure I for updated details of the requirements.

Response to the Pre-Bid Queries

43 4	II	Page 96, Volume II AnnexureN "SIEM" Network Traffic Analysis (NTA) SN. 3	The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the NPCL's environment. Integration to be ensured by the bidder.	Request that the specification be updated to correct a typo Change Request : The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the POSB's environment. Integration to be ensured by the bidder.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

43 5	II	Page 96, Volume II AnnexureN "SIEM"	Clarification	he SIEM sizing requirement (in GB/day) is missing. Kindly confirm the exact daily data volume to allow for an accurate proposal.	Bidder to propose

Response to the Pre-Bid Queries

43 6	II	Page 96, Volume II AnnexureN "External NGFW"	Clarification : Kindly confirm quantity of firewall in DC, DR and NDR	Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for firewalls at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	All the core & critical component should be in redundant & HA mode. For ex: Core router, internet router, replication router, core (spine) switch, NGFW, DDOS, SLB, etc. Bidder has to size the proposed solution to meet RFP functional and non-functional requirements. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

43 7	II	Page 96, Volume II AnnexureN "NIPS"	Clarification : Kindly confirm quantity of NIPS in DC, DR and NDR	Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for NIPS at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

43 8	II	Page 96, Volume II AnnexureN "Attack Surface Mgmt"	Clarification : Kindly confirm number IP to be scanned	Clarification : We note that the specific volume for Attack Surface Management is not defined in the scope. Kindly confirm the total number of public IP addresses that require scanning	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

43 9	II	Page 96, Volume II AnnexureN "Decoy-based Threat Detection" SN. 16	All Windows high interaction activity should be logged, not just code execution attempts. High-interaction should not involve transfer of malicious code to a separate analysis VM, but should provide full interactive access to the attacker.	Mandating "full interactive access" without sandboxing (transfer to analysis VM) runs the risk of giving attackers a pivot point.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

44 0	II	Page 96, Volume II AnnexureN "Secure Browser" SN. 5	Clarification : The proposed solution must be licensed to support all specified features from Day 1 for a total of 5000 users.	Clarification : Please clarify the Day 1 licensing requirement for the Secure Browser. Is the initial scope fixed at 5,000 users, or is there a phased deployment schedule?	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

44 1	II	Page 96, Annexure N, Tab "PAM", Clause No. 26	The proposed solution must support the below listed workflows. Justification for Access (user must submit a reason/comment before accessing) Access Approval (single and/or multi-tiered). Just-in-Time Administration Secret Erase Workflow	Restrictive (OEM Baised) : The requirement for a 'Secret Erase Workflow' appears to utilize terminology specific to a single OEM. Standard PAM solutions typically handle this via 'Secret Deletion,' 'Account Deprovisioning,' or 'One-Time Password (OTP)' workflows.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

44 2	II	Page 96, Annexure N, Tab "PAM", Clause No. 52	The proposed solution must support a configuration where RDP & SSH sessions are brokered through PAM's own "jumpbox"/proxy component without Microsoft Remote Desktop Service Infra	Request to remove OEM specific reference	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

44 3	II	Page 96, Annexure N, Tab "PAM", Clause No. 101	Solution must support real-time reputation checking	As per our understanding, the requirement is around risk analysis of the application and recommending actions to be evaluated. Please confirm	Refer #39

Response to the Pre-Bid Queries

44 4	II	Page 96, Annexure N, Tab "PIM", Clause No. X	General query	Please let us know the count of Privilege Administrators to be considered for PAM requirements	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

44 5	II	Page 96, Annexure N, Tab "PIM", Clause No. X	General query	Please let us know the concurrency of privilege sessions for recommending optimal hardware sizing	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

44 6	II	Page 96, Annexure N, Tab "PAM", Clause No. X	General query	Please let us know the count of endpoints to be considered for PIM requirements	Bidder to propose

Response to the Pre-Bid Queries

44 7	II	Page 96, Annexure N, Tab "MFA & SSO", Clause No. X	General query	Please let us know the count of workforce used to be considered for MFA & SSO requirements.	Minimum requirement is mentioned in the RFP, Bidder is free to propose the solution as per their propose solution stack in line with RFP requirement.

Response to the Pre-Bid Queries

44 8	II	Page 96, Annexure N, Tab "MFA & SSO", Clause No. 9 and 14	The proposed solution should support multifactor authentication for Windows, Mac, Linux Operating systems	As per our understanding, the count of endpoints to be considered here are same as the count of endpoints to be considered for endpoint protection in the "PAM" tab requirements. Please confirm.	Minimum requirement is mentioned in the RFP, Bidder is free to propose the solution as per their propose solution stack in line with RFP requirement.

Response to the Pre-Bid Queries

44 9	II	Page 96, Annexure N, Tab "PAM", Clause No. X	General query	Please share the number of users and applications this solution will be utilized for?	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

45 0	Volume II	Section 5.2.4.7 Testing Page 93	Verify data migration pre and post using reputable testing tools facilitated by an external testing agency. The SI is required to address various testing aspects through an external testing agency	Please clarify that if only the tools facilitated by an external testing agency are to be used OR testing also needs to be conducted/results to be verified by external testing agency	Refer #398

Response to the Pre-Bid Queries

45 1	Volume II	Section 5.2.5 Application Development & Integration of new functionalities Page 93	The testing shall be performed in accordance with the approved test plans and test cases	Please clarify if all the test plans and test cases will be approved by DOP	Refer #399

Response to the Pre-Bid Queries

45 2	Volume II - Scope of Work	Page 24	Figure II: Existing Contract(s) Timeline (Apr 2026 onwards)	Request here in increasing the upgrade timelines	Refer #361

Response to the Pre-Bid Queries

45 3	Volume II - Scope of Work	Page 241	Annexure D – Mobile Banking	Is DoP using Finacle mBanking and to what extent. Also please confirm the integration with Finacle MBanking.	DoP is currently using mBanking and a revamped mobile banking application is under development through Winjit.

Response to the Pre-Bid Queries

45 4	-	General	-	In accordance with Edgeverve's (OEM) guidelines, DoP is requested to execute the License Agreement directly with Edgeverve (OEM).	As per RFP

Response to the Pre-Bid Queries

45 5	BOQ_93745 7	2.9 Finacle licence cost		If DoP confirms that it will enter into a direct contract with Edgeverve for the licensing, then our understanding is that the Finacle license cost sheet will be excluded from the overall Total Contract Value (TCV)	As per RFP

Response to the Pre-Bid Queries

45 6	-	General	-	With regard to the existing contract with Oems, we would like to seek confirmation on whether the DOP intends to remit the ATS payments directly to Oems for the duration of the existing contract's validity	As per RFP

Response to the Pre-Bid Queries

45 7	Volume II - Scope of Work	Page 261	Annexure M – Tech Stack	Is CSIS configured in DOP?	As per RFP

Response to the Pre-Bid Queries

45 8	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall provide a unified view of all UPI transactions initiated across various platforms.	Does DOP support UPI merchant transactions?	UPI solution is not implemented. It is under development through a separate engagement. Bidder has to size and provision the Hardware for both Mobile Banking and UPI including the HSM.

Response to the Pre-Bid Queries

45 9	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall support digital self-onboarding processes for new customers (e.g., Savings Accounts) and existing customers for new products/schemes (e.g., FD/RD) through an OTP-based eKYC/vKYC mechanism within the Internet Banking platform.	Are loan/CCA/ODA accounts present?	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

46 0	Volume II - Scope of Work	Page 261	Annexure M – Tech Stack	Please share current finacle architecture diagram in DOP.	To be shared with selected Bidder

Response to the Pre-Bid Queries

46 1	Volume II - Scope of Work	Page 209	Annexure A – Existing Infrastructure	What is the current size of the Finacle DB	CBS prod is 138.24 TB as on 31st January 2026

Response to the Pre-Bid Queries

46 2	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall provide a unified view of all UPI transactions initiated across various platforms.	1) What is the current UPI solution used by DOP or it has a link with IPPB for processing UPI transactions 2) Kindly elaborate on the processes ?	UPI solution is not implemented. It is under development through a separate engagement. IPPB shall be the sponsor bank.

Response to the Pre-Bid Queries

46 3	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: system shall provide comprehensive functionalities for fund transfers, including intra-bank (POSB to POSB) and interbank (NEFT, RTGS, IMPS)	1) What is the process for handling cross border inward remittances ? 2) What are the channels for processing this ?	Only integration is in scope of the Bidder.

Response to the Pre-Bid Queries

46 4	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: Seamless Integration between Internet & Mobile Banking Platform.	1) Assuming current mobile app is Winjit , what is the process followed to connect with online Banking 2) How we are envisaging cross channel experience	Refer #453

Response to the Pre-Bid Queries

46 5	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall support digital self-onboarding processes for new customers (e.g., Savings Accounts) and existing customers for new products/schemes (e.g., FD/RD) through an OTP-based eKYC/vKYC mechanism within the Internet Banking platform.	Kindly provide more details on the existing Origination system/intermediary onboarding system(if any) in the Bank to be able to complete the flow between Channels, Origination and Core banking solution.	As per RFP

Response to the Pre-Bid Queries

46 6	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system should provide functionalities for Integration with DMAT Accounts (up to 4 Demat account providers)	1) What is the process for access and integration of internet (online) with DMAT account 2) What are the related use cases	As per RFP

Response to the Pre-Bid Queries

46 7	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system should provide functionalities for NACH mandate/ e-mandate management.	1) What are the scenarios for NACH mandate considering loan EMI from DOP is not there ? Is this for insurance, utility bill or any other mandate	As per RFP

Response to the Pre-Bid Queries

46 8	Volume II	Annexure O – Key Statistics	Online transactions per day 10,00,000	Please mention whether these are business transaction volume or individual credits/debits (part-trans) In Finacle terms, please clarify whether this volume is referenced from HTD table or HTH table.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

46 9	Volume II	Annexure O – Key Statistics	Offline transactions per day (peak) 1,50,00,000	Please provide breakup of these transactions as system generated (interest/fees/charges/etc.) or customer generated (transfer/deposit/withdrawal/etc.)	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

47 0	Volume II	5.2.5.10 Middleware	Performance and Scalability Metrics: • The solution must handle a sustained throughput of at least 20,000 transactions per second (TPS) with the capacity to scale up to 50,000 TPS to accommodate future growth over the contract period.	Please clarify whether Hardware capacity estimations are to be provided for 20,000 TPS, 50,000 TPS or 300 TPS	Refer #6

Response to the Pre-Bid Queries

47 1	Volume II	Annexure O – Key Statistics	8. Online transactions per second (TPS) 300	Please provide year wise business volume projections as per adjacent sheet "Finacle Sizing Questionnaire"	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

47 2	Volume II	Annexure O – Key Statistics	User Metrics:		Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

47 3	Volume II	7. Physical Server Details Annexure M – Tech Stack	3. E-Banking 4. FAS (Finacle Alert Solutions) 5. Finacle CBS	Please provide details of Current Hardware provisions as per adjacent sheet "Current Finacle HW Details"	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

47 4	Volume I	5.20 Form 20: Manufactures'/Producers Authorization Form		The proforma provided is more onerous than we typically agree. We suggest using a template that has been pre-approved other central government entities and PSUs.	As per RFP

Response to the Pre-Bid Queries

47 5	Volume 1	5.22 Form A 22: Proforma for Individual Non-Disclosure Agreement		The NDA format provided is designed for individual employees. Please provide revised NDA format that applies to subcontractor entities. Moreover, please note that it may be operationally difficult to enter into individual NDAs with employees. Hence, we request that at least with respect to a subcontractor entity, the NDA be restricted to an organizational level as the organization will be responsible for all acts and omissions of its employees.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

47 6	Volume 3	1.20.1 (ii): Insurance Cover	The above insurance policies shall be of appropriate values so as to cover risks of SI under this Agreement.	We suggest specifying limits on insurance claim for all types of insurance policies to be maintained as per the MSA, in the following manner: USD 1 Million per occurrence and USD 2 Million on annual aggregate of the claims.	As per RFP

Response to the Pre-Bid Queries

47 7	Volume II - Scope of Work	Page 14	Upgrade of Finacle Core Banking solution from version 10.2.13 to 10.2.25 and Finacle Alerts Solution, incorporating the most recent service packs to ensure optimised system performance and capabilities.	We recommend DoP to change 10.2.25 to 10.2.25 or higher version available during the solutioning.	The upgrade of the Finacle Core Banking Solution shall be limited to 10.2.25 as per the RFP. Any discussions or initiatives pertaining to upgrades beyond version 10.2.25 are excluded from the scope of this RFP and shall be undertaken directly between DoP and the OEM, as deemed necessary.

Response to the Pre-Bid Queries

47 8	BOQ_93745 7	For Example in "Tab : 2.4 New Development" and similarly to other tabs		The level of breakup required as per the format may not be possible for a few items.	As per RFP

Response to the Pre-Bid Queries

47 9	Volume I	A1 -Bidder's Credential Strength - Banking- Core Banking Solution, Page 38	The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and allied products within the last five (5) years from the date of bid submission, with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally.	Please clarify programs undertaken by the departments under Ministry of Finance (MoF) as Acceptable credentials which can be submitted against this ask for the BFSI sector	As per RFP

Response to the Pre-Bid Queries

48 0	Volume I	A1 -Bidder's Credential Strength - Banking- Core Banking Solution, Page 38	The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and allied products within the last five (5) years from the date of bid submission, with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally.	The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and /or allied products within the last five (5) years from the date of bid submission, with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally.	As per RFP

Response to the Pre-Bid Queries

48 1	Volume I	B2- Bidder's Credential Strength - Infra-DC DR Migration Page; 39	The Bidder must have experience of executing at least one completed project of DC/DR migration on private cloud / co-location for any organization in India during the last 5 years as on date of bid submission.	Request to modify the clause as "The Bidder must have experience of executing at least one completed project of DC/DR migration or DC DR Build on private cloud / co-location for any organization in India during the last 5 years as on date of bid submission.	As per RFP

Response to the Pre-Bid Queries

48 2	Volume I	B2- Bidder's Credential Strength - Infra-DC DR Migration Page; 39	The Bidder must have experience of executing at least one completed project of DC/DR migration on private cloud / co-location for any organization in India during the last 5 years as on date of bid submission.	Request to modify the clause as "The Bidder must have experience of executing at least one completed project of DC/DR migration on private cloud / co-location for any organization in India or Globally during the last 5 years as on date of bid submission.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

48 3	Volume I	Key Resources- Banking Expert, Page 41	Experienced in executing 2 or more large projects of similar nature in the Banking domain	Experienced in executing 2 or more large projects of similar nature in the Banking/Financial domain	As per RFP

Response to the Pre-Bid Queries

48 4	Volume I	Key Resources- Solution Delivery Lead, Page 41	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products	As per RFP

Response to the Pre-Bid Queries

48 5	Volume I	Key Resources- Project Manager, Page 42	Experienced in 2 or more projects related to the implementation / operations, and maintenance of Core Banking services	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products	As per RFP

Response to the Pre-Bid Queries

48 6	Volume I	Key Resources-Enterprise Architect, Page 42	Experienced in 2 or more projects related to the implementation / operations, and maintenance of Core Banking services	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

48 7	Volume I	Key Resources-Application Architect, Page 43	Experienced in 2 or more projects related to the implementation / operations, and maintenance of Core Banking services	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

48 8	Volume I	Key Resources-Infra Architect, Page 43	Experienced in 2 or more projects related to the implementation / operations, and maintenance of Core Banking services	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

48 9	Volume I	Key Resources-Network Lead, Page 43	Experienced in 2 or more projects related to the implementation / operations, and maintenance in BFSI domain	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

49 0	Volume I	Key Resources-Security Architect, Page 44	Experienced in 2 or more projects related to the implementation / operations, and maintenance in BFSI domain	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

49 1	Volume I	Key Resources-Data Architect, Page 44	Experienced in 2 or more projects related to the implementation / operations, and maintenance in BFSI domain	Experienced in 2 or more projects related to the implementation / operations and maintenance of Core Banking services/ Allied Products / large Scale government of Public sector initiatives	As per RFP

Response to the Pre-Bid Queries

49 2	Volume I	2.23 Sub-contractors- Page 43	Subcontracting is allowed only for Manpower and Data Centre facility services and the details for the same needs to be disclosed by the Bidder in their technical proposal. The overall value of all the subcontracted work/services shall not exceed more than 20% of the total value of contract.	Please confirm that Professional Services for installation/Implementation/Configuration of Hardware and Software will not be considered as sub contracting	Professional Services for installation/Implementation/Configuration of Hardware and Software will not be considered as sub contracting.

Response to the Pre-Bid Queries

49 3	Annexure N	DDOS	Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation Throughput scalable to 20Gbps.	Change request:Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation/Flood Prevention Throughput scalable to 20Gbps.	Refer #311

Response to the Pre-Bid Queries

49 4	Annexure N	DDOS	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active mode	Change Request:The Proposed Solution should be able to work in High Availability (HA) architecture and should be deployable in an Active-Standby or Active-Active design	Refer #418

Response to the Pre-Bid Queries

49 5	Annexure N	DDOS	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection 7. Quantile DoS	Change Request: The appliance should have below Security Protection Profiles: 1. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection	Refer #317

Response to the Pre-Bid Queries

49 6	Annexure N	DDOS	Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Adaptive Rate-Limit – deny real sources (resolvers) that generate too many repeating queries	Change Request:Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Rate-Limit – Allows to configure the rate limits . should also support learning and suggestion of thresholds while implementing	Refer #321

Response to the Pre-Bid Queries

49 7	Volume II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	15. CTS - An online image-based cheque clearing system where cheque images and Magnetic Ink Character Recognition (MICR) data are captured at the collecting branch and transmitted electronically, eliminating the actual cheque movement.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

49 8	Volume II	Page 41: 5.1.4.5 Operations and Maintenance Support for the Centralised Cheque Clearing System (CTS)	DoP has an ongoing contract with M/s Oritso Pvt. Ltd. for Monitoring and Maintenance Support for the Centralised Cheque Clearing System (CTS), valid until June 2026. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

49 9	Volume II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	eKYC/ADV - Applications integrated with UIDAI to enable Aadhaar-based authentication and KYC services, with secure storage of Aadhaar data in compliance with UIDAI guidelines.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

50 0	Volume II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	DoP has an existing contract with M/s Integra Micro Solutions for the Maintenance of Aadhaar-compliant eKYC and Data Vault, valid until November 2029. Both functionalities have been implemented and are currently being maintained by Integra's resources. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines, or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format. This includes support for Aadhaar Data Vault (ADV), an eKYC Solution, and a Hardware Security Module (HSM), in compliance with the guidelines issued by UIDAI and relevant regulatory bodies.	Please include a dedicated HSM technical specification as part of this requirement.	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

50 1	Volume II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	3. The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-2 Level 3 or higher standards.	As FIPS 140-2 validation certificates will be moved to the Historical List in September 2026, they will no longer be considered active for regulated compliance or new procurements. Request: Replace the existing clause with the following updated compliance requirement: "The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-3 Level 3 or higher standards."	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

50 2	Volume II	Page 17: 4. Current State Overview Table 4: Functional Blocks of POSB	9. Card Management System - Card Management System is a solution that manages the complete ATM/Debit Card Issuance cycle for DoP customers.	Please include a dedicated HSM technical specification as part of this requirement.	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

50 3	Volume II	Page 16: 4. Current State Overview	13. ATM Switch - ATM Switch is required to handle all ATM transactions of the customers	Please include a dedicated HSM technical specification as part of this requirement.	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

50 4	Volume I	Form A 22: Proforma for Individual Non-Disclosure Agreement		Submitting NDA along bid is not practice, This can be submitted before we commence the Project execution after the bid is awarded	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

50 5	Annexure N	Data & Database Monitoring	The solutions should provide customisable policies using algorithms as well as algorithmic validators wherever possible to discover and classify sensitive records in MySQL.	Our understanding is that DOP have 2 core 36 on-prem MS SQL databases, and there are no other databases. Considering the expansion, please confirm if the number of databases can go up to 100?	As per RFP

Response to the Pre-Bid Queries

50 6	Volume II	Page #96	The SI is required to provide a collaborative SOC team for mitigating potential security threats. The SI is required to provide below product stack to run SOC: 1. Data & Database Activity Monitoring 2. Multi Factor Authentication (MFA) & Single Sign On (SSO) 3. Identity and Access Management (IDAM) 4. Domain Name System (DNS) 5. Secured Internet Access 6. Security Information and Event Management (SIEM) 7. User and Entity Behaviour analysis (UEBA), 8. Security Orchestration, Automation and Response (SOAR), 9. Threat Intel Management (TI) 10. Network Traffic Analysis (NTA) 11. Application Performance Monitoring 12. Next-Gen Firewall 13. Data Loss Protection (DLP) 14. Distributed Denial of Service (DDoS) 15. Host based Intrusion Prevention System (HIPS) 16. Network Intrusion Prevention System (NIPS) 17. Privileged Identity Management (PIM) 18. Privileged Access Management (PAM) 19. Sandbox 20. Link Load Balancer (LLB) 21. Server Load Balancer (SLB) 22. Web Application Firewall	Annexure N specifically outlines requirements for a 'Secure Browser,' yet this component is missing from the main Scope of Work (SOW) and Bill of Material (BoM). To ensure alignment and avoid ambiguity, we request that the DOP incorporate the 'Secure Browser' into the primary SOW and BoM as a mandatory line item.	Refer #429

Response to the Pre-Bid Queries

			(WAF) 23. Attack Surface Management (ASM) 24. Decoy-based Threat Detection		

Response to the Pre-Bid Queries

50 7	Volume II	Page 96, Volume II Technical Specifications BOQ_937457.xls		We observe that none of the mandatory security components described in the Technical Scope are captured in the commercial BOQ. The is request is to include these items in BOQ , providing specific sizing and quantity details for the DC, DR, and NDR locations for each component.	Refer #430

Response to the Pre-Bid Queries

50 8	Volume II	Page 89 5.2.4.3 Integration, Clause No. 11	The SI is required to deploy engineers from the OEM for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	Propose to modify as follows, The SI is required to deploy manpower from the OEM or OEM certified engineer for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	Refer #431

Response to the Pre-Bid Queries

50 9	Annexure N	Page 96, Volume II AnnexureN " Secure Internet Access " SN. 5	Clarification : Kindly confirm number of user / number of license for Secure Internet Access	Kindly confirm number of user / number of license for Secure Internet Access	Refer #432

Response to the Pre-Bid Queries

51 0	Annexure N	Page 96, Volume II AnnexureN " SIEM " SN. 1	Solution must provide capabilities of SIEM, SOAR, NTA, TIP, Threat hunting, AI/ML Analytics and UEBA OOTB within a single unified frontend and datalake solution.	Clarification : We understand that the proposed solution is required to provide a single, unified management dashboard for the operation of all specified modules, including SIEM, SOAR, NTA, TIP, Threat Hunting, AI/ML Analytics, and UEBA.	Refer #433

Response to the Pre-Bid Queries

51 1	Annexure N	Page 96, Volume II AnnexureN " SIEM " Network Traffic Analysis (NTA) SN. 3	The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the NPCL's environment. Integration to be ensured by the bidder.	Request that the specification be updated to correct a typo Change Request : The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the POSB's environment. Integration to be ensured by the bidder.	Refer #434

Response to the Pre-Bid Queries

51 2	Annexure N	Page 96, Volume II AnnexureN " SIEM "		The SIEM sizing requirement (in GB/day) is missing. Kindly confirm the exact daily data volume to allow for an accurate proposal.	As per RFP

Response to the Pre-Bid Queries

51 3	Annexure N	Page 96, Volume II AnnexureN "External NGFW"		Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for firewalls at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	As per RFP

Response to the Pre-Bid Queries

51 4	Annexure N	Page 96, Volume II AnnexureN " NIPS "		Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for NIPS at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

51 5	Annexure N	Page 96, Volume II AnnexureN " Attack Surface Mgmt "		Clarification : We note that the specific volume for Attack Surface Management is not defined in the scope. Kindly confirm the total number of public IP addresses that require scanning	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

51 6	Annexure N	Page 96, Volume II AnnexureN " Decoy-based Threat Detection " SN. 16	All Windows high interaction activity should be logged, not just code execution attempts. High-interaction should not involve transfer of malicious code to a separate analysis VM, but should provide full interactive access to the attacker.	Mandating "full interactive access" without sandboxing (transfer to analysis VM) runs the risk of giving attackers a pivot point.	Refer #439

Response to the Pre-Bid Queries

51 7	Annexure N	Page 96, Volume II AnnexureN " Secure Browser " SN. 5		Clarification : Please clarify the Day 1 licensing requirement for the Secure Browser. Is the initial scope fixed at 5,000 users, or is there a phased deployment schedule?	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

51 8	Annexure N	Page 96, Annexure N, Tab " PAM ", Clause No. 26	The proposed solution must support the below listed workflows. Justification for Access (user must submit a reason/comment before accessing) Access Approval (single and/or multi-tiered). Just-in-Time Administration Secret Erase Workflow	Restrictive (OEM Baised) : The requirement for a 'Secret Erase Workflow' appears to utilize terminology specific to a single OEM. Standard PAM solutions typically handle this via 'Secret Deletion,' 'Account Deprovisioning,' or 'One-Time Password (OTP)' workflows.	Refer #441

Response to the Pre-Bid Queries

51 9	Annexure N	Page 96, Annexure N, Tab " PAM ", Clause No. 52	The proposed solution must support a configuration where RDP & SSH sessions are brokered through PAM's own "jumpbox"/proxy component without Microsoft Remote Desktop Service Infra	Request to remove OEM specific reference	Refer #442

Response to the Pre-Bid Queries

520	Annexure N	PAM	Solution must support real-time reputation checking	As per our understanding, the requirement is around risk analysis of the application and recommending actions to be evaluated.Please confirm	Refer #39

Response to the Pre-Bid Queries

52 1	Annexure N	PIM		Please let us know the count of Privilege Administrators to be considered for PAM requirements	Refer #444

Response to the Pre-Bid Queries

52 2	Annexure N	PIM		Please let us know the concurrency of privilege sessions for recommending optimal hardware sizing	Refer #445

Response to the Pre-Bid Queries

52 3	Annexure N	PIM		Please let us know the count of endpoints to be considered for PIM requirements	Refer #446

Response to the Pre-Bid Queries

52 4	Annexure N	PAM		Please let us know the count of workforce used to be considered for MFA & SSO requirements.	Refer #447

Response to the Pre-Bid Queries

52 5	Annexure N	Page 96, Annexure N, Tab " MFA & SSO ", Clause No. 9 and 14	The proposed solution should support multifactor authentication for Windows, Mac, Linux Operating systems	As per our understanding, the count of endpoints to be considered here are same as the count of endpoints to be considered for endpoint protection in the "PAM" tab requirements. Please confirm.	Refer #448

Response to the Pre-Bid Queries

52 6	Annexure N	PAM		Please share the number of users and applications this solution will be utilized for?	Refer #449

Response to the Pre-Bid Queries

52 7	Volume 1		Timeline(Months) defination	The timelines for the milestone deliverables and the associated acceptance criteria should follow a sequence of T + 2 months= (T2), T2 + 6 months= (T3), and so forth, taking into account the dependencies linked to the timelines of the preceding milestone deliverables.	As per RFP

Response to the Pre-Bid Queries

52 8	Volume II	5.1.5.1 General A. Core Responsibilities	Ensure uninterrupted availability and reliability of IT services in compliance with applicable regulatory and security standards, including RBI, CERT-In, and PMLA.	PLs provide which RBI and ISO standards needs to be additionally provided for existing system for bidder to plan. There is no mention of which particular standards that need to be followed as a priority for compliance standards.	Bidders are expected to ensure adherence to relevant RBI, CERT-In, DPDP Act, and any other applicable regulatory and statutory compliances.

Response to the Pre-Bid Queries

52 9	Volume II	5. Detailed Scope of Work	Track 2: Operations and Maintenance of IT Infra at new DC, NDC and DR	RFP asks for Zero RPO - but when the operations transfer to DR then how will Zero RPO be maintained without a NDR site. We request Zero RPO to be removed when moving to DR site.	Zero RPO shall be applicable after go-live of new DC, DR and NDC.

Response to the Pre-Bid Queries

53 0	Volume II	3.2 Broad Scope of Work Sub Point : 3. Application Development and Enhancements Page 14	Establishment of separate environments for development, user acceptance testing (UAT), and sandbox/pre-production. Each environment should simulate a near-production network, security, and data flows.	There needs to be percentages defined for each environment for app Non production (in relation to production)else there will be no way to assess and compare one Bidder's Sizing to another objectively. Typicall in any Banking set up - percentages are defined for each enviornment like (for example:) 10% of Prodcution for Development (example) 30% for UAT (example only) 100% for Pre Prod (example only) 100% for Load Testing (with say 60% utilisation) - example only 100% for DR	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

53 1	Volume 1	Training and Capability Building:		What are the types of trainings expected and how many days of such training are required to be conducted?	Training shall cover all new developments and implementations undertaken as part of the scope of work under this RFP, including any configurations, integrations, and customizations carried out during the project duration. Depending upon the functionality, minimum 1 to 4 days of training to be provisioned by the SI. The training plan to be submitted accordingly. Trainings can be conducted in-person/virtually based on criticality of functionality as mutually agreed between DoP and the SI.

Response to the Pre-Bid Queries

53 2	Volume 1	Training and Capability Building:		Please specify the duration of each classroom training session for which the content has to be prepared. (assuming in form of PPTs)	Depending upon the functionality, minimum 1 to 4 days of training to be provisioned by the SI. The training plan to be submitted accordingly.

Response to the Pre-Bid Queries

53 3	Volume 1	Training and Capability Building:		To train master trainers, what will be the estimated batch size?	Approx 50 for physical/in- person session. Approx 100 for virtual session.

Response to the Pre-Bid Queries

53 4	Volume 1	Training and Capability Building:		What are the modules and topics to be considered for the training?	Training shall cover all new developments and implementations undertaken as part of the scope of work under this RFP, including any configurations, integrations, and customizations carried out during the project duration.

Response to the Pre-Bid Queries

53 5	Volume 1	Training and Capability Building:		At which location, trainings are required to be conducted? Who will provide infrastructure like furniture, Internet, LAN Cables, Projector, desktops/workstations, projectors etc. for these trainings?	Trainings can be conducted in-person/virtually based on criticality of functionality as mutually agreed between DoP and the SI. In-person sessions shall be conducted in Postal Training Centres and Chennai. DoP shall provision infrastructure for trainees.

Response to the Pre-Bid Queries

53 6	Volume 1	Training and Capability Building:		Is it expected to make arrangement for Lunch and refreshments of the users/ trainees attending any type of trainings?	DoP shall provision for its trainees.

Response to the Pre-Bid Queries

53 7	Volume 1	Training and Capability Building:		Do we need to budget for travelling, fooding and lodging for trainers only or for trainees as well?	DoP shall provision for its trainees.

Response to the Pre-Bid Queries

53 8	Volume 1	Training and Capability Building:		Is it expected to provide hard copy of any other training materials (except user manual) post training?	As per RFP

Response to the Pre-Bid Queries

53 9	Volume 1	Training and Capability Building- content development		Do we need to create content in English language only? Or any other language has to be factored in?	English and Hindi.

Response to the Pre-Bid Queries

54 0	Volume 1	Training and Capability Building- LMS		Do we need to budget for Learning Management System?	DoP has its own LMS. Bidder to create the required content.

Response to the Pre-Bid Queries

54 1	Volume 1	Training and Capability Building- LMS		If Yes, for how many users and the duration?	As per RFP

Response to the Pre-Bid Queries

54 2	Volume 1	Training and Capability Building- LMS		LMS tool to be proposed needs to be hosted on cloud or will this be on premise implementation?	DoP has its own LMS. Bidder to create the required content.

Response to the Pre-Bid Queries

54 3	Volume 1	Training and Capability Building- LMS		If No, where we need to take publish training calendar, enroll users, take feedback, take assessment, upload training content etc.?	DoP has its own LMS. Bidder to create the required content and provision for feedback collection.

Response to the Pre-Bid Queries

54 4	Vol III – 1.14.5	Limitation of Liability	Liability capped at 1× TCV; exclusions for indemnity, confidentiality, data/security breach, IPR, gross negligence, willful misconduct, fraud.	Revise cap to the fees paid in the preceding 12 months for the affected SOW; narrow exclusions to willful misconduct and fraud or adopt single aggregate cap at X% TCV inclusive of all applicable LDs/penalties.	As per RFP

Response to the Pre-Bid Queries

54 5	Vol III – 1.14.1 & 1.14.2	General & IPR Indemnity	Broad indemnities covering DPDP Act breaches, confidentiality, data breaches, and full IPR indemnity with procure/replace/modify obligations.	Limit indemnity to third-party IPR claims and SI-attributable confidentiality/data protection breaches; exclude customer-provided data and make indemnity subject to liability cap.	As per RFP

Response to the Pre-Bid Queries

54 6	Vol III – 1.14.4	Risk Purchase	DoP may procure at SI's risk/cost; recovery up to 1.5× of non-delivered value; appears to override caps.	Limit recovery to actual documented differential costs; make subject to overall liability cap; delete 1.5× multiplier.	As per RFP

Response to the Pre-Bid Queries

54 7	Vol III – 1.13.4	Termination for Convenience	DoP may terminate for convenience with 60 days' notice; no termination fee specified.	Introduce early termination/wind-down charges (unrecovered mobilization, 3 months O&M fees, third-party pass-throughs).	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

54 8	Vol I – EMD; Vol III – 1.4.2(a)	EMD & Performance Bank Guarantee	EMD INR 29 Cr; PBG 5% of overall project cost (incl. GST) valid 60 days beyond all obligations.	Reduce PBG to 3%; exclude GST from base; align validity to active performance period with rolling renewals.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

54 9	Vol III – 1.5.5; Vol II – Sec. 6/11	LDs & SLA Penalties Aggregation	LDs capped at 10% TCV; separate SLA penalties deducted; termination if LD cap breached.	Confirm single aggregate cap where all LDs/SLA penalties/credits across term do not exceed 10% TCV and count toward overall liability cap.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

55 0	Vol III – 1.17	Audit & Access	Broad audit rights over SI and subcontractors (routine/ad-hoc/forensic) with rectification at SI cost.	Add 15 business days' notice (except emergencies), business-hours access, scope limited to project records/systems; SI bears audit costs only if material non-compliance proven.	The scope of Audit shall be as per RFP.

Response to the Pre-Bid Queries

55 1	Vol III – 1.18 & 1.21	Ownership/IPR & Escrow	Bespoke IP owned by DoP; source code escrow in India with release triggers; third-party licenses in DoP's name.	Limit escrow to SI-developed bespoke code only; exclude SI pre-existing tools/accelerators and COTS; confirm DoP gets perpetual royalty-free license to Deliverables.	As per RFP

Response to the Pre-Bid Queries

55 2	Vol II – CBS/FAS Upgrade (OEM Audit)	Mandatory OEM Audit & Fixes	OEM audit mandatory after CBS/FAS upgrade; SI must rectify all deviations at no extra cost.	Limit 'at no cost' to SI-attributable defects; treat OEM-mandated scope changes via Change Control (T&M).	As per RFP

Response to the Pre-Bid Queries

55 3	Vol II – Licensing	Licenses in DoP Name; Extra at No Cost	All licenses in DoP's name; any additional licenses required but not quoted to be provided at no extra cost.	Limit 'no extra cost' to BoQ-committed items; any new/changed needs handled via Change Control.	As per RFP

Response to the Pre-Bid Queries

55 4	Vol II – Sec. 6; Vol III – 1.5.5	SLA Baselines & DR Targets	99.95% availability; RPO=0, RTO=30 min; penalties across availability/incident/training/DR drills, etc.	Align SLA baselines to deployed architecture; add 90-day stabilization waiver; set DR targets realistically (e.g., RPO ≤ 15 min where supported); aggregate penalties within overall cap.	Existing vendors will manage SLA responsibilities for months 1-3. From month 4 onwards, the selected bidder assumes SLA responsibilities. SLA measurements shall be done during months 4-6 without penalties to facilitate smooth transition. After the transition period, SLAs and corresponding penalties shall be applicable to the selected SI.

Response to the Pre-Bid Queries

55 5	Vol I – 2.10 & Form A.13	NIL Deviations	Mandatory NIL deviations certificate; material deviations lead to rejection.	Permit a non-scoring 'Contract Exceptions' annexure limited to legal/commercial terms for post-award finalization.	As per RFP

Response to the Pre-Bid Queries

55 6	Vol III – 1.12.2(c)	Payment Timeline & Withholding	Payments within 60 working days post-acceptance; DoP may withhold disputed amounts.	Reduce to 30 calendar days; add interest on overdue undisputed amounts at SBI MCLR; release of undisputed portion within 7 days.	As per RFP

Response to the Pre-Bid Queries

55 7	Vol III – 1.12.3	Taxes & Change in Law	SI bears taxes; TDS by DoP; change-in-law adjustment available; SI indemnifies for tax deficiencies.	Confirm GST is payable extra; include reciprocity for DoP-caused tax issues; clarify pass-through for change-in-law.	Change-in-law adjustment is already provided in the RFP. Accordingly, the position shall remain As per RFP

Response to the Pre-Bid Queries

55 8	Vol I – Sub-contracting; Vol II – Sec. 7	Sub-contracting Limits	Only L1/L2 manpower and DCF services allowed; no L3/SME/Key roles via subs; overall cap ~20%.	Permit specialist/OEM L3 subcontracting with SI accountability; raise cap to 40% for niche areas with prior approval.	As per RFP

Response to the Pre-Bid Queries

55 9	Vol III – 1.5.3	Change of Control	On CoC with reduced net-worth, DoP may demand replacement PBG; failure may lead to termination.	Add materiality qualifier and 60-day cure process before termination; restrict to demonstrable adverse impact.	As per RFP

Response to the Pre-Bid Queries

56 0	Vol III – 1.12.1(j)	Time-bar on Claims	Claims time-barred after 3 years from due date (unless under correspondence).	Add that SLA penalties/LDs must be notified within 60 days of the relevant month/milestone or deemed waived.	As per RFP

Response to the Pre-Bid Queries

56 1	Vol II – Training SLAs	Training Penalties & Feedback Thresholds	Penalties tied to training completion and user feedback ≥ 80%; remedial training at SI cost; cap 5% of training cost.	Remove subjective feedback KPI; limit to deliverable-based acceptance; if retained, cap at 1% and exclude from aggregate penalty stack.	As per RFP

Response to the Pre-Bid Queries

56 2	Vol I – 2.24; 2.12	Make in India & Bordering Countries	Class-I local supplier required; GFR 144(xi) undertakings extend to subcontractors.	Confirm read-only remote OEM L3 support permitted subject to DPDP & GFR compliance.	As per RFP

Response to the Pre-Bid Queries

56 3	Vol III – 1.5.4	Final Testing & Certification	Broad set of testing/certification criteria with DoP prerogative to amend.	Freeze acceptance criteria at design sign-off; any new tests to be handled via Change Control.	As per RFP

Response to the Pre-Bid Queries

56 4	Vol III – 1.1.4	Ambiguities within Agreement	Specific clause prevails over general; Agreement prevails over schedules; Agreement prevails over RFP & Proposal.	Confirm that mutually agreed proposal clarifications (pre-bid responses) prevail where RFP is silent/ambiguous.	As per RFP

Response to the Pre-Bid Queries

56 5	Vol III – 1.1.5	Priority of Documents	Order: Corrigenda > Agreement > Vol I/II > SI Technical/Financial Response > Schedules > others.	Elevate mutually agreed clarifications and finalized proposal (including BoQ) above generic RFP provisions for conflicts.	As per RFP

Response to the Pre-Bid Queries

56 6	Vol III – 1.11.3	Security & Safety (Regulatory Updates)	Compliance with IT Act, DPDP, CERT-In, ISMS, CCMP and industry standards as updated from time to time.	Process new/changed regulatory requirements through Change Control with mutually agreed effort/cost/schedule.	As per RFP

Response to the Pre-Bid Queries

56 7	Vol III – 1.6.1(o); 1.14; 1.16	DPDP/Data Breach Liability	SI must comply with DPDP and indemnify for data breaches; confidentiality obligations broad.	Limit liability to SI-controlled systems/acts; exclude DoP-originated or third-party-caused breaches; subject to overall cap.	As per RFP

Response to the Pre-Bid Queries

56 8	Vol II – Multiple sections (Compliance Changes)	Regulatory Changes at No Cost	DoP directives/RBI/UIDAI/NPCI/ FIU updates to be implemented without additional cost.	Treat material regulatory changes as Change Requests unless already included in base scope.	As per RFP

Response to the Pre-Bid Queries

56 9	Vol III – 1.12.2(d)	Payment Withholding on Bona Fide Disputes	DoP can withhold disputed portion without clear resolution timeline.	Time-bound dispute resolution (15 days) and release of undisputed portion within 7 days; add interest on amounts later found payable.	As per RFP

Response to the Pre-Bid Queries

57 0	Vol III – 1.12.1(e)	Auto-deduction of Penalties	SLA penalties/LDs deducted from invoices.	Require joint penalty computation sign-off prior to deduction; provide dispute mechanism with reversal timeline.	As per RFP

Response to the Pre-Bid Queries

57 1	Vol III – 1.14.3 (read with 1.14.1/1.14.2)	Third-party/OEM Failures	SI indemnity exposure not expressly carved out for OEM/COTS defects.	Exclude OEM/COTS failures and mandated patches from SI indemnity; align to pass-through warranties only.	As per RFP

Response to the Pre-Bid Queries

57 2	Vol II – 5.1.1/5.1.2/5.1.3	Multi-Vendor Transition Dependencies	Incumbents continue till expiry; SI takes lead from month 4; SLAs continue.	Define shared-responsibility matrix; carve-out penalties where dependencies on incumbents/OEMs cause delay/failure.	Refer #554

Response to the Pre-Bid Queries

57 3	Vol II – Infra Utilization/Up grades	>75% Utilization – 1-month Upgrade	If utilization >75%, SI to propose and upgrade within one month.	Attribute utilization to business changes; upgrades funded via CR unless within SI-controlled optimization scope.	Refer Section 6.11 of RFP Vol 2 for Utilization KPIs

Response to the Pre-Bid Queries

57 4	Vol II – AMC/ATS Management	Legacy Estate Support	SI to manage ATS/AMCs for existing legacy infra and software.	Seek inventory sign-off and OEM support status baseline; no liability for unsupported/EoS assets; gaps to be addressed via CR.	As per RFP

Response to the Pre-Bid Queries

57 5	Vol II – Manpower SLAs	Resource Replacement Penalties	High penalties for key resource replacement/absence; strict approval timelines.	Remove or cap resource penalties; allow reasonable notice/transition periods without penalties.	As per RFP

Response to the Pre-Bid Queries

57 6	Vol II – DR SLAs	RPO = 0; RTO = 30 minutes	Aggressive DR targets applied across platforms.	Align DR targets to actual replication architecture; define service-wise RPO/RTO.	As per RFP

Response to the Pre-Bid Queries

57 7	Vol II – 24x7x365 Support	Onsite Coverage	Round-the-clock onsite teams, including holidays.	Permit hybrid onsite/offsite; phased ramp-up over 90 days; define minimum onsite coverage bands.	As per RFP

Response to the Pre-Bid Queries

57 8	Vol III – Schedule III (Exit)	Exit Support Duration/Cost	SI to support exit/transition up to 6 months post-termination.	Pay exit support at O&M rates; define capped scope & hours for exit assistance.	As per RFP

Response to the Pre-Bid Queries

57 9	Vol III – Schedule III (Exit) & 1.18	Handover of Materials	Transfer of configurations, scripts, SOPs, source code, accesses.	Limit handover to customer-specific deliverables; exclude SI pre-existing IP/accelerators; grant license where necessary.	Refer section 1.18 (Ownership and Intellectual Property Rights) of Volume 3.

Response to the Pre-Bid Queries

58 0	Vol III – 1.20	Insurance	Multiple mandatory insurances (PI, product liability, worker safety); non-compliance → termination.	Align to IT services norm (PI only); or allow equivalent global policies; provide 30-day cure before adverse action.	As per RFP

Response to the Pre-Bid Queries

58 1	Vol III – 1.22.5	Publicity/Trademarks	No publicity/reference without DoP consent.	Permit anonymized reference to sector and scope post go-live, subject to prior written approval not unreasonably withheld.	As per RFP

Response to the Pre-Bid Queries

58 2	Vol III – 1.22.14 (Dispute Resolution)	Arbitration & Continuity of Services	IIAC arbitration; seat New Delhi; SI must continue performance during dispute.	Right to suspend services for non-payment > 60 days of undisputed sums; expedited interim relief for payment disputes.	As per RFP

Response to the Pre-Bid Queries

58 3	Vol III – Schedule I (Governance)	Governance/Escalation Bias	Formal governance under DoP, PMC reviews; DoP discretion on amendments.	Establish joint governance with bilateral SLAs for response, decision timelines, and neutral dispute triggers.	As per RFP

Response to the Pre-Bid Queries

58 4	Vol I – 2.5; 2.25	Code of Integrity & Debarment	Broad grounds for blacklisting (corruption/fraud/obstructive practice).	Add due-process safeguards, clear definitions, cure/representation window before any debarment.	As per RFP

Response to the Pre-Bid Queries

58 5	Vol II – Reporting & MIS	Unbounded Reporting Cadence	Daily/weekly/monthly/quarterly reporting across modules; auto penalties for delay.	Consolidate into unified cadence and template; define materiality thresholds; remove penalties for minor delays without service impact.	As per RFP

Response to the Pre-Bid Queries

58 6	Vol- III , Section 1.14.6. Page No. 32	Step-In-rights	In the event of the SI's failure to perform its obligations or breach of the Agreement, the DoP reserves the right to step in and procure equivalent services or deliverables from alternate sources at the SI's risk and cost. Any additional expenses incurred shall be recoverable from pending dues, the Performance Bank Guarantee, or through legal process. DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding 15 days) for rectification. If the SI fails to remedy the default within the said period, DoP may exercise its step-in rights without further notice. Upon invocation of step-in, the SI shall provide DoP or its designated agency full access to project sites, systems, data, documentation, software, and any other resources reasonably required for continued delivery of services. The SI shall extend all cooperation and technical assistance to ensure smooth transition and continuity of operations. DoP shall have the right to use, for the duration of the step-in period, all project assets, equipment, tools, and licences (including third-party software licences, to the extent	We propose that, rather than implementing a step-in right, the Customer should have increased management oversight over the delivery of services. This can be achieved through the establishment of a steering committee or similar governance mechanisms, where any defaults or delays can be promptly identified, discussed, and addressed. The right to step in should be exercised only in the event of a material breach that is directly attributable to Infosys and remains uncured. In such a case, the step-in rights should be restricted to accessing Infosys systems that are exclusively used for the Customer's services. Additionally, a clearly defined step-out period should be established to ensure a smooth transition back to normal operations. The incremental costs associated with the step-in should be capped, ranging between 10% to 15%.	As per RFP

Response to the Pre-Bid Queries

			transferable or sublicensable) necessary for performance of services. Invocation of step-in rights shall not relieve the SI of its obligations, liabilities, or warranties under this Agreement, nor be construed as a waiver of any rights or remedies available to DoP. During the step-in period, the SI shall continue to be responsible for ensuring data integrity, confidentiality, and compliance with all applicable information security and regulatory requirements until the Department confirms formal transition of such responsibilities. If the Department's step-in rights remain in effect for a continuous period exceeding sixty (60) days, or if in the Department's reasonable opinion, the SI is unable to resume satisfactory performance of the affected Services within such period, the Department shall have the right to terminate the Statement of Work (SOW) for which the step-in was invoked, without any liability or penalty. Upon such termination, the Department may permanently retain control of all project materials, data, systems, and deliverables related to the affected SOW and may engage any		

Response to the Pre-Bid Queries

			third party to continue or complete the Services at the risk and cost of the SI. Such termination of an SOW under this clause shall not prejudice the Department's rights to claim damages, invoke the Performance Bank Guarantee, or recover any losses incurred due to the SI's failure.		

Response to the Pre-Bid Queries

58 7	Vol- III, Section 1.22.9	Compliance with Applicable Law	The SI shall comply with the provision of all laws including the Digital Personal Data Protection Act, 2023, labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the DoP shall be applicable in the performance of this Agreement and the SI shall abide by these laws. The SI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. The SI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations. The SI shall also adhere to all security requirement/regulations of the DoP during the execution of the work.	The obligation is acceptable subject to addition of "to the best of its knowledge" as it limits the service provider's liability to what it reasonably knows at the time of making the representation related to the IT Service Providing industry. This way the service provider acknowledges that there may be unknown or unforeseen legal obligations or changes in law. This qualifier helps ensure that the service provider is not held liable for non-compliance with laws it was unaware of, despite having made reasonable efforts to stay informed and compliant.	As per RFP

Response to the Pre-Bid Queries

58 8	Annexure N	Secure Internet Access	The solution provider should have achieved DoD Impact Level 5 (IL5) and FedRAMP High Authorization to reflect better security standards. The offered solution must be certified with CSA STAR, FedRamp, ISO 27001, ISO 27017, ISO 27018, SOC 2 / 3, FIPS 140-2, certification and Zero Trust Architecture designed by NIST (National Institute of Standards and Technology).	Because both DoD IL5 and FedRAMP High involve high-impact security controls and federal compliance mandates, we request a modification of this clause to ensure full regulatory alignment: "The solution provider should have achieved DoD Impact Level 5 (IL5) or FedRAMP High Authorization to reflect better security standards. The offered solution must be certified with CSA STAR, FedRamp, ISO 27001, ISO 27017, ISO 27018, SOC 2 / 3, FIPS 140-2, certification and Zero Trust Architecture designed by NIST (National Institute of Standards and Technology)."	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

58 9	Annexure N	Secure Internet Access	The solution must have the ability to apply data masking controls to hide PII information on the web browser for sensitive applications accessed via Secured Browser or Remote Browser Isolation.	This requirement is redundant as it is already addressed in Section 24 of the Secure Browser specifications. Consequently, we request its removal from the Secure Internet Access section.	Bidder is free to propose integrated solution in the same box or by third party solution

Response to the Pre-Bid Queries

59 0	Annexure N	Secure Internet Access	The solution must have control to restrict access to camera, microphone, provide read-only access to secure application accessed via Secured Browser or Remote Browser Isolation.	This requirement is redundant as it is already addressed in Section 35 of the Secure Browser specifications. Consequently, we request its removal from the Secure Internet Access section.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

59 1	Annexure N	Secure Internet Access	The solution must have file encryption capabilities to encrypt the files downloaded from the sensitive applications accessed via Secured Browser or Remote Browser Isolation.	This requirement is redundant as it is already addressed in Section 25 of the Secure Browser specifications. Consequently, we request its removal from the Secure Internet Access section.	Refer #3

Response to the Pre-Bid Queries

59 2	Annexure N	Secure Internet Access	The solution must have NGFW, IPS for both web and non-web, Advanced Threat Protection, Advanced Sandbox and DNS Security feature from day 1 to secure internet traffic. The DNS Security solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc. extended for all DNS over HTTPS (DoH).	DOH can be blocked at client level using Inline policies so hence we request you to modify the clause for wider participation "The solution must have NGFW, IPS for both web and non-web, Advanced Threat Protection, Advanced Sandbox and DNS Security feature from day 1 to secure internet traffic. The DNS Security solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc."	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

59 3	Annexure N	Secure Internet Access	Proposed solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc. extended for all DNS over HTTPS (DoH) regardless of DoH resolver used (no bypass)	DOH can be blocked at client level using Inline policies so hence we request you to modify the clause for wider participation "Proposed solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc."	The revised clause to be read as: Proposed solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc. Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

59 4	Annexure N	Secured Browser	The proposed solution must provide access to private applications without any dependency on a connector, virtual appliance, or hardware appliance in the customer's data center.	This clause appears to favor a specific firewall OEM, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

59 5	Annexure N	Secured Browser	The proposed solution must have the ability to establish a secure, encrypted tunnel to the existing perimeter firewall in the customer's data center to enable access to private applications.	This clause appears to favor a specific firewall vendor, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

59 6	Annexure N	Secured Browser	The proposed SSE solution must provide a configuration option within the management console that allows the administrator to select and activate the required Compute/PoP location for processing and inspecting user transaction traffic to applications.	This clause appears to favor a specific OEM, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

59 7	Annexure N	Secured Browser	The Secure Private Browser must have strict Data Masking controls based on content policy. The customer must be able to dynamically mask any confidential information with a pattern such as email address, credit card number, PAN Card etc. Masking must allow partial view such as last 4 digits for certain user groups.	This clause appears to favor a specific OEM, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

59 8	Annexure N	Secured Browser	The Secure Private Browser must have File Protection control to allow users to download a file on endpoint which must be automatically encrypted and only viewable through the secure web browser. Encrypted files must only be allowed to be uploaded to sanctioned applications within the secure private browser only.	This clause appears to favor a specific OEM, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

59 9	Annexure N	Secured Browser	The Secure Private Browser must have keylogger protection to prevent any leakage of any sensitive data and informtaion from the secure private browser to the key logger application that might be present on the same user endpoint.	This clause appears to favor a specific OEM, which may limit competitive bidding. We request its removal to encourage broader participation and ensure a vendor-neutral procurement process	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 0	Annexure N	Secured Browser	The Secure Private Browser must provide keylogger protection to ensure that no sensitive data or information is leaked from the secure private browser to any keylogger application present on the user's endpoint.	This requirement is redundant as it is already addressed in Section 26 of the Secure Browser specifications. We request its remove this.	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 1	Annexure N	Secured Browser	The Secure Private Browser must support centrally configuring browser artifacts such as proxy configuration, trusted ca certificates, mic and camera controls, autofill etc. These configurations must be locked down and must not be modifiable by the end user.	This is favoring a specific OEM so we request you to modify this clause for broader participation as "The Secure Private Browser must support centrally configuring browser artifacts such as proxy configuration, trusted ca certificates. These configurations must be locked down and must not be modifiable by the end user."	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 2	Annexure N	Secured Browser	The proposed solution must have the capability to seamlessly integrate with traditional on-premises directory services using LDAP, RADIUS, and Kerberos protocols.	This is favoring a specific firewall vendor as Radius protocol mostly integrated with Firewall not with SSE security solution, so we request you to modify this clause for broader participation as "The proposed solution must have the capability to seamlessly integrate with traditional on-premises directory services using LDAP, Active Directory or Kerberos protocols."	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 3	Annexure N	Secured Browser	The DNS Security functionality must support enforcing sinkholing for malicious DNS requests to identify the actual source. It must also prevent DNS attacks on DoH (DNS over HTTPS), DoT (DNS over TLS). Additionally it must provide control to block or allow DoH/DoT.	DOH can be blocked at client level using Inline policies so hence we request you to modify the clause for wider participation "The DNS Security functionality must support enforcing sinkholing for malicious DNS requests to identify the actual source. It must also prevent DNS attacks on DoH (DNS over HTTPS), DoT (DNS over TLS) or it must provide control to block or allow DoH/DoT.	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 4	Annexure N	Secured Browser	The solution must have advance Sandbox capabilities to prevent zero-day attacks across different platforms including Windows, Linux, MacOS. The Sandbox must support multiple filetypes from day 1 including but not limited to archives, executables, msoffice files, Script (BAT, JS, VBS, PS1, and HTA) files , JAR Files, Archive (RAR, 7-Zip, ZIP) files, pdfs and other web content like adobe flash, java applet, ELF, DMG and HTML.	We request you to modify this clause for broader participation as "The solution must have advance Sandbox capabilities to prevent zero-day attacks across different platforms including Windows/Linux/MacOS. The Sandbox must support multiple filetypes from day 1 including but not limited to archives, executables, msoffice files, Script (BAT, JS, VBS, PS1, and HTA) files , JAR Files, Archive (RAR, 7-Zip, ZIP) files, pdfs and other web content like adobe flash, java applet, ELF, DMG and HTML.	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

60 5	Annexure N	Secure Internet Access		The Proposed solution should handle any type of TCP or UDP traffic, including non-web protocols and provides deep inspection for data and malware, even for files transferred over non-web protocols like FTP, SFTP, FTPS, Telnet.	As per RFP

Response to the Pre-Bid Queries

60 6	Annexure N	Secure Internet Access		The propsoed solution must be able to provide Shadow discovery of Gen AI apps running in customer environment and also must be able to restrict and differentiate the Corporate and public Instance. It must be able to restrict the sensitive data upload to Gen AI apps on the public instance.	As per RFP

Response to the Pre-Bid Queries

60 7	Annexure L	Software LB	Solution shall support integration with VMware vCenter for automated LB instance deployment and discovery.	We request removal of the words “automated deployment and discovery” from the VMware vCenter integration clause, as these are not mandatory for Software Load Balancer operation. Basic VMware compatibility should be sufficient to allow wider participation. It is suggested to amend the clause as "Solution shall support integration with VMware vCenter for automated LB instance."	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

60 8	Annexure L	Software LB	OEM to provide integrated WAF capabilities to protect applications from OWASP Top 10.	The listed specifications relate to Web Application Firewall (WAF) features that have been incorporated within the Software Load Balancer requirements. We humbly request the Committee to consider deletion of these WAF-specific conditions to allow broader participation from eligible bidders.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

60 9	Annexure L	Software LB	WAF should support custom security rules, positive security model, and REST-based policy automation.	The listed specifications relate to Web Application Firewall (WAF) features that have been incorporated within the Software Load Balancer requirements. We humbly request the Committee to consider deletion of these WAF-specific conditions to allow broader participation from eligible bidders.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

61 0	Annexure L	Software LB	HSM integration-ready; FIPS 140-2 compliant cryptographic module preferred.	Kindly remove the FIPS 140-2 compliant word for wider participation of OEM because HSM integration is already asked. It is suggested to amend the clause as "HSM integration-ready."	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

61 1	Annexure L	Software LB	Support for TLS 1.3, OWASP Top 10 protections through WAF (native or integrable), and audit logging.	The listed specifications relate to Web Application Firewall (WAF) features that have been incorporated within the Software Load Balancer requirements. We humbly request the Committee to consider deletion of these WAF-specific conditions to allow broader participation from eligible bidders.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

61 2	Annexure N	Link Load Balancer	The proposed Appliance should supports the following health check types: • Link Health Checks, • TCP Health Checks, • UDP Health Checks, • ICMP Health Checks, • HTTP/S Health Checks, • FTP Server Health Checks, • POP3 Server Health Checks, • SMTP Server Health Checks, • NNTP Server Health Checks, • WAP Gateway Health Checks, • LDAP/LDAPS Health Checks, • Windows Terminal Server Health Checks, • ARP Health Checks, • DHCP Health Checks, • Virtual Wire Health Checks, • DSSP Health Checks, • Script-Based Health Checks, • Cluster-based Health Checks	The clause mentions that all health checks are required for the server load balancer. However, as per the requirement of the LLB, only limited health checks are necessary. We request that the clause be modified and the change will ensure wider participation while maintaining the required quality and compliance standards. It is suggested to amend this clause. It is suggested to amend the clause as: "Supports the following health check types: • Link Health Checks, • TCP Health Checks, • ICMP Health Checks"	Refer #229

Response to the Pre-Bid Queries

61 3	Annexure N	WAF	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.	The requirement for “unique messaging mechanism” between WAF and DDoS enforces same-OEM proprietary integration and restricts participation for 2 different OEM. As per standard practice WAF and DDoS should be different OEM. We request deletion or relaxation of this clause to allow wider participation without compromising security.	Refer #207

Response to the Pre-Bid Queries

61 4	Annexure N	DDOS	The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create signatures within 20 Secs for zero-day DDoS attacks and DNS DDOS attacks.	OEM specific clause, restricting us to participate.pls ammend as"The Proposed Solution should protect against Zero Day DDoS Attacks. ZERO DAY ATTACK PROTECTION should be provided using behaviour based /challenge response / http authentication technology."	Refer #315

Response to the Pre-Bid Queries

61 5	Annexure N	DDOS	Cloud Scrubbing OEM should have 15 Tbps of Scrubbing capacity for future Use. The proposed DDoS Solution OEM should be able to offer On-Demand & Always-On services.	OEM specific and not a practical clause. Best possible way of tackling it is using appliance and ISP clean pipe scrubbing with integration of both. Having OEM cloud based scrubbing has routing and compliance challenges .As per compliances banks traffic cant be routed to a third paty cloud service as well which will lead to integrity and security issues. It is request you to ammend the clause as "The solution should support Integration with ISP clean pipe Scrubbing Centres in case of Bandwidth Saturation attacks"	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

61 6	Annexure N	DDOS	The proposed appliance should have atleast 5000+ inbuilt Signatures apart from custom Signatures from Day 1	DDOS requires a lot of research where asking for 5000+ signatures seems to be someone proposing IPS appliance with very limited count of signatures. DDOS generally works on threshold and learning .Request you to ammend the clause as suggested "The proposed device should support learning and threshold."	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

61 7	Annexure L	Core Router	Router should have a physical separation between control and data planes processor. Router should support inline hardware accelerated encryption for high-throughput IPsec	We recommend to modify the clause as below Router should have a physical separation between control and data planes or processor. Router should support inline hardware accelerated encryption or provide high-throughput IPsec	Refer #258

Response to the Pre-Bid Queries

61 8	Annexure L	Core Router	Router should have minimum IP forwarding throughput of 38 Gbps	We recommend to modify the clause as below Router should have minimum IP forwarding throughput of 30Gbps or Higher	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

61 9	Annexure L	Core Router	Router should support minimum 4M IPv4 & IPv6 routes	We recommend to modify the clause as below Router should support minimum 100K or higher IPv4 & IPv6 routes	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

62 0	Annexure L	Core Router	No. of Firewall session: 2M	We recommend to remove this clause	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

62 1	Annexure L	Core Router	The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should be able to create GRE tunnel.	We recommend to modify the clause as below The router must support IKEv1,, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should be able to create GRE tunnel.	Refer #260

Response to the Pre-Bid Queries

62 2	Annexure L	Core Router	Router should be scalable to support up to 4000 tunnels (non-SDWAN) / 8000 SD_WAN tunnel (SD- WAN)	We recommend to modify the clause as below Router should be scalable to support up to 512 tunnels or higher (non-SDWAN) / 8000 SD_WAN tunnel (SD- WAN)	Refer #263

Response to the Pre-Bid Queries

62 3	Annexure L	Core Router	Router should support VRF level segmentation with min support for 8000 VRF segments	We recommend to modify the clause as below Router should support VRF level segmentation with min support for 128 VRF segments or higher	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

62 4	Annexure L	Core Router	Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling from Day 1	We recommend to modify the clause as below Router should support static Routes, OSPFv2, OSPFv3, BGP4, MBGP/EVPN, BFD, Policy based routing, IPv4 and IPv6 tunnelling from Day 1	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

62 5	Annexure L	Core Router	The Router should support Zone Based Firewall feature or an external appliance for the same functionality can be provided.	We recommend to remove this clause	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

62 6	Annexure L	Core Router	Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.	All modern routers support Traffic optimization does in some form and shape. Need more clarification on this clause	Refer #264

Response to the Pre-Bid Queries

62 7	Annexure L	Core Router	Should support advanced encryption algorithms like AES-256 and AES-GCM	We recommend to modify the clause as below Should support advanced encryption algorithms like AES-256 or AES-GCM	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

62 8	Annexure L	Core Router	The router should be able to support Hierarchical QoS. QoS should be supported both at Physical and sub-interface level	We recommend to modify the clause as below The router should be able to support Hierarchical QoS/Advanced QoS features. QoS should be supported both at Physical and sub-interface level	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

62 9	Annexure L	Core Router	Router shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	Router shall conform to UL 60950 or IEC 60950/62368 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

63 0	Annexure L	WAN Router	Minimum 64 GB RAM; hardware-assisted IPsec/GRE capabilities.	We recommend to modify the clause as below Minimum 16GB RAM or higher hardware-assisted IPsec/GRE capabilities.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

63 1	Annexure L	WAN Router	Route table capacity: 1M IPv4, 500K IPv6, 1M MPLS labels.	We recommend to modify the clause as below Route table capacity: 1M IPv4, 500K IPv6,	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

63 2	Annexure L	WAN Router	Optional support for 4G/5G failover modules.	Requesting DOP to remove Clause	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

63 3	Annexure L	WAN Router	Stateful firewall capabilities.	Requesting DOP to remove Clause	Refer #270

Response to the Pre-Bid Queries

63 4	Annexure L	WAN Router	DoS/DDoS mitigation (RTBH, uRPF, NetFlow-based detection).	We recommend to modify the clause as below DoS/DDoS mitigation (RTBH/ uRPF/ NetFlow-based detection).	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

63 5	Annexure L	WAN Router	Non-stop Routing (NSR) , Non-stop Forwarding (NSF).	Non-stop Routing (NSR) or equivalent , Non-stop Forwarding (NSF).	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

63 6	Annexure L	WAN Router	Stateful Switchover (SSO).	Requesting DOP to remove Clause	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

63 7	Annexure L	WAN Router	Operating temperature: 0°C to 45°C or better.	We recommend to modify the clause as below Operating temperature: 0°C to 40°C or better.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

63 8	Annexure L	Spine Switch	The switch proposed should have minimum 64 MB Packet Buffer	We recommend to modify the clause as below The switch proposed should have minimum 50 MB Packet Buffer	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

63 9	Annexure L	Spine Switch	Switch should support segment routing and VRF route leaking functionality from day 1	We recommend to modify the clause as below Switch should support segment routing / EVPN and VRF route leaking functionality from day 1	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

64 0	Annexure L	Spine Switch	Switch should support minimum 1000 VRF instances with route leaking functionality	We recommend to modify the clause as below Switch should support minimum 128 VRF instances with route leaking functionality	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

64 1	Annexure L	Spine Switch	Min of 34 non-blocking interfaces populated with multimode 40/100G Transceivers from day 1. Switch should have console port for local management & out of band management interface for remote management.	We recommend to modify the clause as below Min of 34 32 non-blocking interfaces populated with multimode 40/100G Transceivers from day 1. Switch should have console port for local management & out of band management interface for remote management.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

64 2	Annexure L	Spine Switch	Device should be based on simple and intelligent shared-memory buffered architecture that simplifies the system buffer management and queuing implementation. Both the SAN switch and the Spine/Leaf switches should be from the same OEM	We recommend to modify the clause as below Device should be based on simple and intelligent shared- memory buffered architecture that simplifies the system buffer management and queuing implementation.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

64 3	Annexure L	Managed Switch	802.1X, DHCP Snooping, Dynamic ARP Inspection, Port Security, IP Source Guard.	We recommend to modify the clause as below 802.1X, DHCP Snooping, Dynamic / ARP Inspection, Port Security, IP Source Guard.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

64 4	Annexure L	Leaf Switch	Switch should support minimum 1000 VRF instances with route leaking functionality	We recommend to modify the clause as below Switch should support minimum 256 VRF instances with route leaking functionality	Refer #640

Response to the Pre-Bid Queries

64 5	Annexure L	Leaf Switch	The switch should support min 800k IPv4 LPM routes	We recommend to modify the clause as below The switch should support min 350K IPv4 LPM routes	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

64 6	Annexure L	Leaf Switch	The switch should have MAC Address table size of 500k	We recommend to modify the clause as below The switch should have MAC Address table size of 350K	Refer #275

Response to the Pre-Bid Queries

64 7	Annexure L	Leaf Switch	The Switch should support intelligent buffer management with a minimum buffer of 36 MB.	We recommend to modify the clause as below The Switch should support intelligent buffer management with a minimum buffer of 32MB.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

64 8	Annexure L	Leaf Switch	Switch must provide the capability to be integrated with different Hypervisor Managers viz. VMware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualise networking from the single pane of glass	We recommend to modify the clause as below Switch must provide the capability to be integrated with different Hypervisor Managers viz. VMware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage / support	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

64 9	Annexure L	Leaf Switch	Switch should support minimum 500k of MAC addresses	We recommend to modify the clause as below The switch should have MAC Address table size of 350K	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

65 0	Annexure L	Leaf Switch	Switch should support segment routing and VRF route leaking functionality from day 1	We recommend to modify the clause as below Switch should support segment routing / EVPN and VRF route leaking functionality from day 1	Refer #639

Response to the Pre-Bid Queries

65 1	Annexure L	Leaf Switch	Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification. The solution must also provide micro segmentation capability on application end host at remote location sites in offline mode (once policy is applied from the DC to workloads on remote sites, in case the sites are dis-connected, the enforcement policy is retained). Mentioned feature/capability should be achieved using same OEM products for a seamless integration, without using any external/3rd party solution.	We recommend to modify the clause as below Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro-segmentation based on VM attributes like hostname/OS/VM Tags/ FQDN,/Microsoft AD/IP based classification. The solution must also provide micro segmentation capability on application end host at remote location sites in offline / online mode (once policy is applied from the DC to workloads on remote sites, in case the sites are dis-connected, the enforcement policy is retained). Mentioned feature/capability should be achieved using same OEM products for a seamless integration, without using any external/3rd party solution.	Refer #279

Response to the Pre-Bid Queries

65 2	Annexure L	Leaf Switch	Switch platform should support encryption of traffic i.e. MAC Sec Encryption (802.1AE) in hardware	Requesting DOP to remove this Clause	Refer #280

Response to the Pre-Bid Queries

65 3	Annexure L	Leaf Switch	Switch should support Dynamic ARP Inspection	We recommend to modify the clause as below Switch should support Dynamic / ARP Inspection	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

65 4	Annexure L	Leaf Switch	prevent degradation of switch performance from storm due to network attacks and vulnerabilities. Both the SAN s with and the Spine/Leaf switches should be from the same OEM	We recommend to modify the clause as below prevent degradation of switch performance from storm due to network attacks and vulnerabilities.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

65 5	Annexure L	Leaf Switch	Switch must have Switched Port Analyzer (SPAN) with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	We recommend to modify the clause as below Switch must have Switched Port Analyzer (SPAN) / Port Mirroring with minimum 4 active session and ERSPAN on physical, Port channel, VLAN interfaces	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

65 6	Annexure L	RISC Server		While the RFP specifies a RISC platform, Finacle is fully proven on modern x86 servers, which deliver equal or better performance, availability, and security for core banking workloads. Infosys Finacle has been benchmarked at very high transaction volumes on industry-standard Intel x86 platforms, demonstrating excellent scalability and performance for large core-banking workloads. Leading banks globally today running Infosys Finacle on x86, meeting stringent regulatory, TPS, and resilience requirements, with validated OS, database, and middleware stacks. Allowing x86 servers instead of RISC will give IPPB better price-performance, easier scalability, and more flexibility in capacity planning as digital transaction volumes grow. Standardized x86 platforms reduce TCO through broader competition, simpler lifecycle management, and a larger pool of skills and ecosystem support. We therefore request that the RFP clause be updated to "RISC or x86 servers meeting Infosys Finacle OEM specifications" so that IPPB can choose the most optimal certified platform	As per RFP

Response to the Pre-Bid Queries

				without any risk to the application.	

Response to the Pre-Bid Queries

65 7	Annexure L	SAN Storage	Storage solution should provide the native capability to replicate data of existing storage between DC, DR and NDC without using any additional Hardware and software.	Please change the clause as " Proposed Storage solution should provide the native capability to replicate data of Proposed storage between DC, DR and NDC without using any additional Hardware and software. "	Refer #85

Response to the Pre-Bid Queries

65 8	Annexure L	SAN Storage	Storage must be scalable to at least double capacity without adding any additional controllers with the same set of drives and RAID.	Please change the clause as "Storage must be scalable to at least double capacity without or With adding additional controllers with the same set of drives and RAID "	Refer #87

Response to the Pre-Bid Queries

65 9	Annexure L	SAN Storage	Storage Capacity must be as per the RFP capacity clauses.	Storage Capacity mentioned in Volume 2: Scope of Work Page 216 is with Data Reduction ?	As per RFP

Response to the Pre-Bid Queries

66 0	Annexure L	SAN Storage	Must integrate with VMware, Nutanix, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible).	Please change the clause as " Must integrate with VMware, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible)."	Refer #97

Response to the Pre-Bid Queries

66 1	Annexure L	SAN Director	The switch must support port aggregation of up to 16 physical ports. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model. The port channel should support trunk/port channel members from different ASICs / modules ports into a single aggregated link to ensure that the bundle can remain active in the event of a port, Application-Specific Integrated Circuit (ASIC), or module failure.	Please change the Clause as "The switch must support port aggregation of up to 8 physical ports. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model. The port channel should support trunk/port channel members from different ASICs / modules ports into a single aggregated link to ensure that the bundle can remain active in the event of a port, Application-Specific Integrated Circuit (ASIC), or module failure or Create multiple ISL trunks, each within a port-group/ASIC boundary and Distribute them across different blades/ASICs and even separate fabrics (Fabric A / Fabric B) for resilience, rather than stretching one trunk across ASICs	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

66 2	Annexure L	SAN Director	It should natively support power-on auto provisioning (POAP) to automate software image upgrades and configuration file installation on newly deployed switches.	Please change the clause as "It should support single touch software image upgrades and configuration file installation on newly deployed switches"	The revised clause to be read as: It should natively support power-on auto provisioning (POAP)/Zero Touch Provisioning (ZTP) to automate software image upgrades and configuration file installation on newly deployed switches. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

66 3	Annexure L	SAN Director	There should be common Operating System family for Data Center Ethernet switching and SAN Switching for simplified Software Management across Data Center.	Please delete this clause for broader participation	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

66 4	Annexure L	SAN Director	Chassis must support Virtual Output Queue (VOQ) to ensure line-rate performance on each port, independent of traffic pattern, by eliminating head-of-line blocking.	Please change the cause as "Chassis must support Virtual Output Queue (VOQ) or non blocking with line-rate forwarding using credit-based flow control and deep buffering to ensure line-rate performance on each port, independent of traffic pattern, by eliminating head-of-line blocking."	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

66 5	Annexure L	SAN Director	SFPs proposed along with switches should be compatible with any generation of SAN switches for investment protection.	Please change the clause as "SFPs proposed along with switches should be compatible with +/- 2 generation of SAN switches for investment protection."	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

66 6	Annexure L	Backup Solution		Proposed purpose-built backup appliance should support enterprise applications and database backups without integration with Backup Software, for better visibility of backups to application and database owners, thus ensuring faster and direct recovery on application/database level. This integration should be available for Oracle, SAP, DB2, MS SQL, etc.	As per RFP

Response to the Pre-Bid Queries

66 7	Annexure L	Backup Solution		The proposed purpose built backup appliance must provide efficient data reduction by using variable block length deduplication at the source as well as target side. Proposed purpose-built backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS, CIFS, FC, OST and NDMP protocols. All the protocols should be available to use concurrently with global deduplication for data ingested across all of them.	As per RFP

Response to the Pre-Bid Queries

66 8	Annexure L	Backup Solution		The offered purpose-built backup appliance must have an inbuilt mechanism to defend the backup data against data integrity issues, it should also have a mechanism that check, validate and repair the backup data residing on the appliance against any corruption without any human intervention.	As per RFP

Response to the Pre-Bid Queries

66 9	Annexure L	Backup Solution		Proposed backup appliance must have data security feature retention lock WORM (Write Once Read Many) and which will ensure that not even system/backup administrator can delete, expire, modify backed up data before expiry of retention period from the backup appliance.	As per RFP

Response to the Pre-Bid Queries

67 0	Annexure L	Backup Solution		OEM & SI must ensure & implement backup solution in such a way that if Backups could be wrongfully expired and eventually deleted by tampered system clocks through a compromised NTP server. In this case, the local system clock would sync up based on the hacked NTP clock. This will minimize the systems clock tampering by an option which allows the security officer to set an allowed limit for the time drift between local clock & NTP server. The proposed purpose-built backup appliance must have security feature which should protect against NTP hacking/compromise in case of Ransomware or Cyber-Attacks.	As per RFP

Response to the Pre-Bid Queries

67 1	Annexure L	Backup Solution		The offered purpose-built backup appliance should be sized appropriately for backup of front-end data of 500 TB (30% DB & 70% VM & File System) as per below mentioned backup policies:	As per RFP

Response to the Pre-Bid Queries

67 2	Annexure L	Backup Solution		a. Daily incremental backup – retained for 4 weeks in the backup appliance.	Refer #885

Response to the Pre-Bid Queries

67 3	Annexure L	Backup Solution		b. Weekly full backup for all data types – retained for 4 Weeks in the backup appliance.	Refer #885

Response to the Pre-Bid Queries

67 4	Annexure L	Backup Solution		c. Monthly full backup – retained for 12 months in the backup Appliance.	Refer #885

Response to the Pre-Bid Queries

67 5	Annexure L	Backup Solution		d. Yearly full backup - retained for 5 years in the backup appliance.	Refer #885

Response to the Pre-Bid Queries

67 6	Annexure L	Backup Solution		The offered purpose-built backup appliance should be quoted	As per RFP

Response to the Pre-Bid Queries

67 7	Annexure L	Backup Solution		with minimum 600 TB usable capacity. The proposed purpose-built backup appliance must be sized for adequate capacity considering 1% daily data change rate for the contract period. Any additional backup storage capacity, software and any other component required as per sizing needs to be provided by the MSI and OEM at the time of bid. Bidder must provide the backup appliance sizing on OEM's letter head with seal & sign from the authorized signatory basis the backup retention policies mentioned along with Rack, Power & cooling requirements to run the complete infrastructure.	As per RFP

Response to the Pre-Bid Queries

67 8	Annexure L	Backup Solution		Proposed purpose-built backup appliance should have the ability to perform different backup, restore, replication jobs simultaneously and must supports communications and data transfers through 32GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with minimum 1 x 1Gbps NIC, 8x 10/25G SFP+ and 8x 32Gbps FC.	As per RFP

Response to the Pre-Bid Queries

67 9	Annexure L	Backup Solution		Proposed purpose-built backup appliance should support at least 75TB/hr of backup ingest throughput.	As per RFP

Response to the Pre-Bid Queries

68 0	Annexure L	Backup Storage	Disk-based backup appliances, SAN/NAS, VTL; Support for multi-site storage targets.	The proposed purpose built backup appliance must provide efficient data reduction by using variable block length deduplication at the source as well as target side. Proposed purpose-built backup appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS, CIFS, FC, OST and NDMP protocols. All the protocols should be available to use concurrently with global deduplication for data ingested across all of them.	Refer #107

Response to the Pre-Bid Queries

68 1	II	Annexure L, X86-Based Hypervisor, Clause No. 19	Support SAN and IP-based storage for shared datastore access.	To provide more options, please rephrase the clause to "Support SAN and IP- based storage for shared datastore / storage class access."	The revised clause to be read as: Support SAN and IP- based storage for shared datastore / storage class access. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

68 2	II	Annexure L, X86-Based Hypervisor, Clause No. 28	Continuous availability using live shadow VMs for fault tolerance.	To provide more options, please rephrase the clause to "Support high availability for virtual machines through automatic recovery on node failure."	Refer #286

Response to the Pre-Bid Queries

68 3	II	Annexure L, Virtualization, Clause No. 18	The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption.	To provide more options, please rephrase the clause to "The solution should support VM migration over long distances with low network latency"	Refer #303

Response to the Pre-Bid Queries

68 4	II	Annexure L, Virtualization, Clause No. 18	The solution should create a cluster out of multiple storage datastores and automate load balancing using storage characteristics.	To provide more options, please rephrase the clause to "The solution should provide policy-based storage provisioning for virtual machine workloads by supporting multiple storage providers"	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

68 5	II	Annexure L	X86-Based Hypervisor	Since in same Annexure L there is already a Virtualization technical spceifications section so the technical spceifications section on Hypervisor should be removed.	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

68 6	II	Annexure J, Middleware, Clause No . 4	Cross-language client SDKs with support for programming languages including but not limited to Java, C, C++, C#, Ruby, Perl, Python, PHP, and VB6.	VB6 is now legacy. Request you to please remove the same. The STOMP protocol provides this connectivity without a propriety adapter. Request to please remove VB6.	Refer #8

Response to the Pre-Bid Queries

68 7	II	Annexure J, Middleware, Clause No . 5	Support for multiple messaging protocols including OpenWire, STOMP, AMQP, MQTT, and JMS.	The OpenWire protocol is considered deprecated in modern enterprise messaging platforms.	Refer #9

Response to the Pre-Bid Queries

68 8	II	Annexure J, Middleware, Clause No . 8	Support for pluggable transport protocols such as In-VM, TCP, SSL, NIO, UDP, multicast, JGroups, and JXTA.	The in-VM protocols is considered legacy architectural patterns for modern, cloud-native deployments. Request to pelase remove this. JXTA is a legacy peer to peer protocol which industry moved away from the past 10-15 years. Modern peer to peer is handled now via JGroups now. Request to please remove the same.	Refer #10

Response to the Pre-Bid Queries

68 9	II	Annexure J, Middleware, Clause No . 10	Appliance-based deployment options should be supported.	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

69 0	II	Annexure J, Middleware, Clause No . 15	Support for message groups, virtual destinations, wildcards, and composite destinations.	VirtualDestinations element is now legacy and the same is acheived through Addresses, Queues, and Routing. Composite Destination can also be acheived using multicast Addresses.	As per RFP

Response to the Pre-Bid Queries

69 1	II	Annexure J, Middleware, Clause No . 22	Compliance and support for BOLA (Broken Object Level Authorization) mitigation and adherence to OWASP Top 10 security testing.	While middleware technologies provide native security capabilities, external security and native-kubernetes networking protocols etc help acheive this requirement. Request to please remove the same as it will not be catered by middleware directly.	As per RFP

Response to the Pre-Bid Queries

69 2	II	Annexure J, Middleware, Clause No . 29	Solution should support deployment flexibility including appliance, container, and Kubernetes environments.	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

69 3	II	Annexure J, Middleware, Clause No . 39	The ESB should offer integrated support for IBM MQ Server on the same hardware as a single unit-of-work transaction.	Request to pelase remove this point as it opints to a specific vendor.	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

69 4	II	Annexure J, Middleware, Clause No . 40	The ESB shall allow integration with multiple programming environments, including Java, .NET (C#, VB, F#, etc.), PHP, ESQL, and C++.	Request to please remove ESQL for larger participation. Apache Camel is the standard defacto open source standard offering more flexibility compared to vendor locked ESQL.	Refer #11

Response to the Pre-Bid Queries

69 5	II	Annexure J, Middleware, Clause No . 65	Platform should contain client development kit available for all the programing languages including VB6	VB6 is now legacy. Request you to please remove the same. The STOMP protocol provides this connectivity without a propriety adapter. Request to please remove VB6.	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

69 6	II	Annexure J, Middleware, Clause No . 66	Platform should support appliance based deployment options	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	As per RFP

Response to the Pre-Bid Queries

69 7	II	Annexure J, Middleware, Clause No . 78	Maven based repository for OSGi modules and plugins	Apache Camel, the defacto open-source standard for ESB now does not mandate the complexity of OSGI at runtime. Camel technologies can now run on Kubernetes as lightweight, immutable containers.	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

69 8	II	5.2.5 Application Development & Integration of new functionalities	The SI shall design, develop and perform UAT testing on their environment and deploy the applications directly on the new DC/DR.	We understand that the connectivity (BSNL/SIFY) from existing DC to the new DCF as per project timelines will be provided by DOP. And respective API connectivities with the existing application will be provided by bidder.	Connectivity from existing DC to the new DCF as per project timelines will be provided by DoP NI. Respective API connectivities with the existing application to be provided by Selected Bidder.

Response to the Pre-Bid Queries

69 9	II	4. Current State Overview	Details of Core Banking Platform and Version	What is the Web application server (WAS) version on existing core banking J2EE server. How many Finacle environments are currently used by DOP POSB	8.5.5.19, PROD/MIS/UAT/SIT/Training

Response to the Pre-Bid Queries

70 0	II	page 182	Monitor CBS and its various integrated modules like NEFT/RTGS/UPI/AEPS, etc.	What is current solution for UPI transactions, will it require any change or need new solution for it ?	Refer #458

Response to the Pre-Bid Queries

70 1	II	page 182	Monitor CBS and its various integrated modules like NEFT/RTGS/UPI/AEPS, etc.	With AEPS as new requirement, does this mean DOP do not do any AEPS transactions today?	AePS is currently not implemented.

Response to the Pre-Bid Queries

70 2	II	page 36	The SI shall ensure that all interfaces are fully automated, with minimal manual intervention, and that accurate reconciliation and accounting are conducted for all transactions processed through these interfaces	With AEPS and IMPS coming in, do SI need to factor a reconciliation solution additionally or can use existing recon by extending it to AEPS and IMPS? How NEFT/RTGS recon is done today?	Bidder to analyze the current solution and propose accordingly.

Response to the Pre-Bid Queries

70 3	II	page 191	Project Delivery Timelines	Timeline for CBS and Alert solution upgrade looks challenging due to technical upgrade that might become a pre-requisite (if WAS version is lower)before 10.2.25 upgrade, can we increase it to 15months?	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

70 4	II	page 110	API Gateway & Management Tool Solution	What is current solution for APIG?	APIG is currently not implemnted.

Response to the Pre-Bid Queries

70 5	II	5.2.5.9	5.2.5.9 EFRM	What is current solution for Enterprise Fraud Risk Management?	EFRM is currently not implemnted.

Response to the Pre-Bid Queries

70 6	II	5.2.5.1	5.2.5.1 cKYC	What is current solution for cKYC?	cKYC is currently not implemnted.

Response to the Pre-Bid Queries

70 7	II	5.2.5.4	5.2.5.4 Data Archival & Retrieval Solution	Whether DOP has any Data Archival & Retrieval Solution?	Data Archival & Retrieval Solution is currently not implemented.

Response to the Pre-Bid Queries

70 8	II	5.2.5	5.2.5.2 FINnet 2.0 5.2.5.3 I4C	How is FINnet2.0 and I4C, reporting managed currently?	FINnet 2.0 and I4C are currently not implemnted.

Response to the Pre-Bid Queries

70 9	II	Annexure O – Key Statistics - Page 268	User Metrics	What is the % breakup of online transactions & peak volume (TPS) in NEFT/RTGS/AEPS/UPI/ATM/POS/OTHER	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

71 0	II	Annexure O – Key Statistics - Page 268	User Metrics	What is the EOD timings in current 10.2.13 Finacle core	7-8 Hours (3 steps at branch level and 3 steps at DC) on an average.

Response to the Pre-Bid Queries

71 1	II	Annexure O – Key Statistics - Page 268	User Metrics	In offline transactions- what is the break up of customer induced and bank induced (system generated)	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

71 2	II	4. Current State Overview	Current State Overview	Can we get existing enterprise application architecture from DOP	Bidders are required to analyze and base their proposals on the information provided in the RFP and subsequent corrigenda.

Response to the Pre-Bid Queries

71 3	II	page 238	Tibco	Tibco is mentioned in the software inventory list. It's license and AMC both expired as of now, does it renewed by DOP? Does SI need to renew it, migrate to new DC and continue to support?	Tibco is not related to POSB IT systems.

Response to the Pre-Bid Queries

71 4	II	page 16	Cheque Book	What does Cheque Book Delivery Channel mean in terms of CBS?	Cheque book requests are initiated by DoP counter staff through CBS (Finacle) and are subsequently processed by the cheque book vendor as per the existing workflow.

Response to the Pre-Bid Queries

71 5	II	page 113	5.2.5.8 Two-Factor Authentication to log in to the Core Banking System (Finacle) via Biometric/OTP	What is current implementation for biometric authentication and 2FA?	This is not implemented currently and shall be part of New Developments.

Response to the Pre-Bid Queries

71 6	II	page 247	AML Solution - GST, Income tax or other revenue authority	How GST is hanadled currently?	As per RFP

Response to the Pre-Bid Queries

71 7	II	page 116	Deliver a comprehensive investigative workbench supporting alert triage, case creation, collaborative investigation, document management, workflow automation, audit trail, and escalation	1) Please confirm , if Department of Post is already using a Document Management System ? 2) Please share the Document Management Application Name & Current Version Number ? 3) Is there a Need of a New Document Management Application to store all critical Banking documents ? 4) Please confirm , the current Document Volume (In GB/TB) currently residing in a Document Management System ? 5) Is there a Need of Migrating Documents from the Current Document Management Application to the New Proposed Document Management System ? 6) Total & Concurrent Number of Users for DMS 7) Whether it should be migrated to new DC and part of AMS?	Document Management for POSB is currently done through Finacle SVS (Photo and Signature), it is part of the bundled Finacle solution. Bidder to provision for DMS.

Response to the Pre-Bid Queries

71 8	II	5.2.5.4 Data Archival & Retrieval Solution	The SI shall be responsible for the design, development, integration, and implementation of a Data Archival and Retrieval Solution for POSB	Which all application data needs to be archived and what will be data size for archieval?	As per DoP Data Archival policy.

Response to the Pre-Bid Queries

71 9	II	4. Current State Overview	Current State Overview	Whether debit Card Management system is in scope of SI AMS and need to be migrated to new DC?	Only integration is required.

Response to the Pre-Bid Queries

72 0	II	4. Current State Overview	Current State Overview	What is current solution for NACH?	DoP is currently live for ACH Credit Inward and ACH Credit Outward under NACH. ACH Debit including mandate management is not implemented and shall be developed and operationalized by the selected SI.

Response to the Pre-Bid Queries

72 1	II	4. Current State Overview	Current State Overview	What is current solution for ATM switch and whether it will be moved to new DC and part of AMS?	Only integration is required.

Response to the Pre-Bid Queries

72 2	II	5.1.2.3 Transition of Applications	Transition of Applications	Which batch processing system is used?	CBS native framework is used.

Response to the Pre-Bid Queries

72 3	II	3.2 Broad Scope of Work	Figure I: Solution Architecture IT 2.0	All the components mentioned in this diagram like ECRM, Dispute Mgmt, HR & other systems are not in scope of RFP, unless it's explicitly mentioned in the scope section. Please confirm?	As per RFP

Response to the Pre-Bid Queries

72 4	III	1.19.1 Standard	Warranty - 6 months post completion of this Agreement	Warranty should be till the contract period and not beyond	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

72 5	II	5.2.4 Detailed Scope of Work	The SI is required to initiate the hardware warranty after the successful installation and obtaining sign-off from the bank. The Annual Maintenance Contract (AMC) for hardware will commence after the completion of the three-year warranty period.	What if Warranty is for less than or more than 3 years. Date of AMC start will be changed in that case.	Bidder to propose.

Response to the Pre-Bid Queries

72 6	II	5.2.4.7 Testing	The SI is required to address various testing aspects through an external testing agency	Which external agency?	CERT-In and STQC-empanelled testing agency.

Response to the Pre-Bid Queries

72 7	II	5.4.2 Capacity Building	Master Trainers - Users who are responsible for training the end users - 2000	Need break up of Master trainers for application to prepare training BoQ	As per RFP

Response to the Pre-Bid Queries

72 8	II	4. Current State Overview	List of applications	What is application name for Agent Portal, whether it will be moved to new DC and in scope of AMS?	The Agent Portal is part of the Finacle e-Banking application (used by MPKBY agents). Operations & Maintenance and any enhancements/developments related to Agent Portal shall be in scope of the selected Bidder.

Response to the Pre-Bid Queries

72 9	II	4. Current State Overview	List of applications	Can you share list of all applications and list of applications that needs to be made available in new DC.	As per RFP

Response to the Pre-Bid Queries

73 0	II	4. Current State Overview	List of applications	Which all applications has RAC database	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

73 1	II	4. Current State Overview	List of applications	Can you share technology and infrastructure details of all applications that needed to made available in new DC?	As per RFP

Response to the Pre-Bid Queries

73 2	II	8.1 Key Resources	DevSecOps SME	Which all tools are currently used for version control and DevOps ? Does it need to be migrated to new DC ? What is the DevSecOps requirement?	Bidder to propose

Response to the Pre-Bid Queries

73 3	II	Annexure O – Key Statistics	User Metrics	What is expected YoY growth for next seven years for each of these parametrs to calculate the TPS ? Do you suggest to consider any specifc % growth across parameters SI should consider?	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

73 4	II	Annexure O – Key Statistics	User Metrics	What is the Average and peak TPS for NEFT, RTGS, AEPS ?	Current transaction volume is around 20000 per day for NEFT/RTGS. AEPS is not used in DOP. Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

73 5	II	5.2.5.11 Video KYC	Video KYC	Please provide details of folllwing NFRs ? Latency Uptime Retention Average Call Duration	Latency: ≤ 200-300 ms Uptime: 99.5%-99.9% Retention: 10+ years Average Call Duration: 4 to 8 minutes

Response to the Pre-Bid Queries

73 6	II	5.2.5.4 Data Archival & Retrieval Solution	Data Archival & Retrieval Solution	Please provide details of following NFRs ? No of Source Systems Source Data Storage Types Data Size for each source Uptime Retention Period Retrieval SLA YoY Growth	No of Source Systems: 3 to 15 Source Data Storage Types: Oracle, PostgreSQL, MSSQL, Files (PDF/JPEG) etc. Uptime: 99.5%-99.9% Retention Period: As per DoP Data Archival Policy Retrieval SLA: <5 sec (indexed data) < 30-60 sec (large datasets) YoY Growth: 15 to 30%

Response to the Pre-Bid Queries

73 7	II	5.2.5.1 cKYC	cKYC	Please provide details of following NFRs ? No of Concurrent Users Upload Time Uptime YoY Growth	No of Concurrent Users: 200-1,000+ users Upload Time: Currently done through batch processing. CERSAI will implement APIs in CKYC 2.0. It should be 2 seconds to 5 seconds. Uptime: 99.5%-99.9% YoY Growth: 15 to 30%

Response to the Pre-Bid Queries

73 8	II	5.2.5.11	vKYC	Please provide details of following NFRs ? No of Concurrent Users Upload Time Uptime YoY Growth	Refer #735

Response to the Pre-Bid Queries

73 9	II	5.2.4 Detailed Scope of Work	The SI is required to guarantee a Recovery Time Objective (RTO) of 30 minutes and a Recovery Point Objective (RPO) of ZERO minutes for all hosted solutions in DR and NDC	This will inflate the BOM if RTO and RPO is same for all the applications. Can you provide specific RTO and RPO for each of the applications to have right sizing.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

74 0	II	Annexure M – Tech Stack	8. Mobile Banking - License Type Licensed	What license are required for Mobile Banking and PSP App ? Does it has any dependancy on Finacle m-banking? If dependancy, which functionality has dependancy on m-banking? With Winjit new application, will Finacle mobile banking discarded or will still be used as backend	Refer #453

Response to the Pre-Bid Queries

74 1	II	x.Reports	The SI shall be responsible for ensuring the seamless, accurate, and timely flow of all POSB-related data from the respective source systems into the DoP Data Lake/Data Mart environment. The SI shall develop, customise, and deliver reports as required by DoP, including but not limited to periodic, operational, performance, security, compliance and exceptional reports. The exact formats, content, frequency, and delivery mechanisms for these reports shall be finalised collaboratively between DoP and SI after project commencement, ensuring alignment with the DoP's business objectives and regulatory requirements. The SI shall also provide the capability to generate ad-hoc and custom reports as requested by DoP throughout the contract term.	Do we need new Data Lake, ETL, Report solution? Please confirm the expected number of dashboards, & reports to be created as a part of the solution Please confirm on the total number of viewers, users, editors and administrators of such reports (average and concurrent) Please confirm expected number of integration, integration types and storage requirement.	Data Lake solution shall be implemented by DoP. Selected Bidder has to integrate and provide necessary data.

Response to the Pre-Bid Queries

74 2	II	Annexure O – Key Statistics	Key Statistics	What is % of non-financial transactions per day in Finacle core	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

74 3	II	5.1.3 Upgrade of Finacle CBS and Alert Solution	Execution of thorough SIT, UAT, and performance testing for critical use cases to validate the correctness, stability, and performance of the upgraded system and submit a detailed report	CBS upgrade UAT is expected from SI?	As per RFP

Response to the Pre-Bid Queries

74 4	II	5.2.5.1 cKYC	cKYC	Why is scanning facility required by cKYC application, ckyc application acquired data from different applications and format and upload to CERSAI	Bidders may refer to the Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

74 5	II	5.2.5.1 cKYC	Windows7 server	What is the Chrome version available on windows 7 servers	As per RFP

Response to the Pre-Bid Queries

74 6	II	5.2.5.10, Page Number 117, Point no 2	The solution must handle a sustained throughput of at least 20,000 transactions per second (TPS) with the capacity to scale up to 50,000 TPS to accommodate future growth over the contract period	1. It is written Sustained TPS of 20000 - or middleware should support upto 20000 TPS. Assumed this TPS is for WebSphere Application Serve. Please confirm? 2. Please confirm the 20000 TPS is sustained on WebSphere Application Server as its not aligned with Annexure O - Where Online + Offline and TPS comes around to be 2000? 3. Please give me the expected TPS required for ESB and WebSphere Application Server sepearately?	Refer #6

Response to the Pre-Bid Queries

74 7	II	Annexure O	User Metrics	Can TPS advised for Online and Offline TPS be used for TPS for API Gateway?	Refer #7

Response to the Pre-Bid Queries

74 8	II	Annexure J Middleware Tab	Cross-language client SDKs with support for programming languages including but not limited to Java, C, C++, C#, Ruby, Perl, Python, PHP, and VB6.	Assume Cross Language SDKs are required to develop microservices? Are you looking to modernize WebSphere Application Server Services to microservices on Kubernetes Environment?	Refer #8

Response to the Pre-Bid Queries

74 9	II	Annexure J Middleware Tab	Support for multiple messaging protocols including OpenWire, STOMP, AMQP, MQTT, and JMS.	Assume this requirement is for services running on WebSphere Application Server. Please confirm ? Also, Please specify the number of interfaces using these messaging protocols in current environment	Refer #9

Response to the Pre-Bid Queries

75 0	II	Annexure J Middleware Tab	Support for pluggable transport protocols such as In-VM, TCP, SSL, NIO, UDP, multicast, JGroups, and JXTA.	Assume, this requirement is for services running on WebSphere Application Server. Please confirm? Also, if you can specify if you are willing to use it in microservices ?	Refer #10

Response to the Pre-Bid Queries

75 1	II	Annexure J Middleware Tab	The ESB shall allow integration with multiple programming environments, including Java, .NET (C#, VB, F#, etc.), PHP, ESQL, and C++.	Is there any requirement to run PHP In ESB or Can it be removed ?	Refer #11

Response to the Pre-Bid Queries

75 2	II	Annexure J Middleware Tab	Guaranteed and assured message delivery.	It seems there is requirement for IBM MQ. Can you please specify if you have MQ or needs to be supplied as part of middleware? If needs to be supplied then please specify the number of interfaces which will depend on MQ with approximate size of message	Refer #12

Response to the Pre-Bid Queries

75 3	II	Annexure J API Gateway Tab	It shall support active-active clustering to provide high availability and resiliency.	Assuming Active-Active DR is required and High Availability is being considered through Container native solutions ? Please confirm	Refer #13

Response to the Pre-Bid Queries

75 4	II	Annexure J API Gateway Tab	Support for runtime policy enforcement, circuit breakers, hard timeouts, service discovery, and load balancing of microservices is required.	Do you need to implement circuit breaker on API Gateway ? Can you please explain the use case of Circuit breaker ?	Refer #14

Response to the Pre-Bid Queries

75 5	II	Annexure J API Gateway Tab	It shall enable bi-directional data format conversion between multiple widely used formats such as ISO, JSON, XML, CSV, and flat files.	Can the conversion be achieved using ESB as supplementary tool for some complex scenarios?	Refer #15

Response to the Pre-Bid Queries

75 6	II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	Since the Middleware Server used as WebSphere Application Server along with ESB- (TIBCO). Can you please share the number of interfaces implemented on WebSphere Application Server and TIBCO separately?	Refer #16

Response to the Pre-Bid Queries

75 7	II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	There are single specifications given for Middleware. Can you please help me with ESB Particulars?	Refer #17

Response to the Pre-Bid Queries

75 8	II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	The Environments are not defined in Scope and Compliance Sheet. Do you require separate Environment for all these multiple Environments ?	Refer #20

Response to the Pre-Bid Queries

75 9	II	Annexure J Middleware Tab	Environments are not defined	Can I assume the environment similar to API Gateway tab? If yes, then can you please specify the TPS required for ESB	Refer #21

Response to the Pre-Bid Queries

76 0	II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	Can you please define TPS for these environments separately?	Refer #22

Response to the Pre-Bid Queries

76 1	II	Annexure J API Gateway Tab	Facilities for seamless integration with developers' IDEs and support for issue resolution workflows must be provided.	Can you please specify the workflows for issue resolution in IDE? Do you mean API Debugging ?	Refer #23

Response to the Pre-Bid Queries

76 2	II	Annexure J API Gateway Tab	Compliance with relevant regional, national, and international regulations such as the Reserve Bank of India (RBI) guidelines, ISO 27001, Financial Data Exchange (FDX), and data privacy laws including the Indian Personal Data Protection Bill (PDP Bill) shall be ensured.	This requirement should be for complete API Solution instead of just API Gateway. API Gateway may work with other products to implement these framework. Can you please update the statement according to API Gateway as API Gateway only store information as defined by the solution	Refer #24

Response to the Pre-Bid Queries

76 3	II	Annexure L Container mgmt	The container platform should be one that provides a developer portal, plugins, middleware and inbuilt integrated IDE for developers to easily work on the same container platform to bring consistence and faster application lifecycle.	There is a separate requirement of middleware in the rfp with API gateway and ESB. Are you also planning to leverage a separate middleware of the container platform?	Refer #25

Response to the Pre-Bid Queries

76 4	II	Annexure B	Microsoft Biztalk	Assuming all Biztalk interfaces can be migrated or modernized to new ESB Solution. Please confirm?	Refer #26

Response to the Pre-Bid Queries

76 5	II	Infra- Software Pg 238	IBM WebSphere Application Server Network Deployment	Are you looking to modernize WASND runtime?	Refer #27

Response to the Pre-Bid Queries

76 6	II	Annexure L Container mgmt		What is the total worker node core that you are expecting for container mgmt platform to manage?	Refer #28

Response to the Pre-Bid Queries

76 7	II	Annexure J Archival	SI must include and provide the Solution capacity sizing, which shall include sizing for Hardware and Software based on the requirement in Annexure- Bill of Material (BoM). For the Database, DoP shall provide Oracle licenses, and SI need not factor the cost for the database licenses.	Should Database not be considered for any of the module mentioned in the RFP? Will this be taken care by DoP?	Refer #29

Response to the Pre-Bid Queries

76 8	II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Leverage AI/ML techniques with no-code/low-code interfaces, enabling business users and data scientists to develop and refine fraud detection models.	Does DoP expect business users to independently configure and retrain fraud models using no-code/low-code interfaces, or should such activities be restricted to SI or data-science teams? If yes then please confirm on the number of such developers from DOP.	Refer #41

Response to the Pre-Bid Queries

76 9	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Support real-time case management features, including alert assignment, prioritized queues, case notes, attachments, escalation, reminders, and reporting.	DoP is expecting a full-featured case management system with configurable workflows, SLAs, escalations and document management system. Please confirm	Refer #42

Response to the Pre-Bid Queries

77 0	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	We understand that DoP expects EFRM reporting to be delivered via an embedded reporting layer, which should be a part of the overall solution. Please confirm	Refer #43

Response to the Pre-Bid Queries

77 1	II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm average and peak daily transaction volumes across all channels to enable accurate sizing of real-time fraud detection infrastructure.	Refer #44

Response to the Pre-Bid Queries

77 2	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Please indicate expected daily fraud alert volumes and number of concurrent investigation users for case management sizing(workflow management)	Refer #45

Response to the Pre-Bid Queries

77 3	II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	What is the historical data window in years or TB expected to be provided for fraud model training and back-testing?	Refer #46

Response to the Pre-Bid Queries

77 4	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm the expected number of dashboards, & reports to be created as a part of the solution	Refer #47

Response to the Pre-Bid Queries

77 5	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm on the total number of viewers, users, editors and administrators of such reports	Refer #48

Response to the Pre-Bid Queries

77 6	II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Incorporate continuous model lifecycle management, including development, deployment, monitoring, model governance, retraining, and scorecarding.	If AI/ML or Generative AI solutions are proposed, are there any specific governance, explainability, auditability or model-risk requirements expected by DoP beyond standard RBI, CERT-In and DPDP compliance?	Refer #49

Response to the Pre-Bid Queries

77 7	II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Does DoP intend to standardize document management, records retention and audit evidence on a centralized Enterprise Content Management (ECM) platform and scanning solution(for physical documents), or should existing document repositories continue without transformation? If a new solution is needed, kindly confirm on the average number of documets to be digitized and number of concurrent users for the platform.	Refer #50

Response to the Pre-Bid Queries

77 8	II	Section 5.2.5, Page number 116, Clause number NA	Application Development & Integration of new functionalities	For use cases involving forms, certificates, KYC documents or regulatory submissions, should the solution propose ntelligent Document Processing (OCR + AI classification and extraction) capabilities. If yes, then please confirm the average document volume to be extracted in a year.	Refer #51

Response to the Pre-Bid Queries

77 9	II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm the expected no. of machine learning or scoring models that will be deployed for the solution	Refer #52

Response to the Pre-Bid Queries

78 0	II	Section 5.2.5, Page number 115, Clause number 5.2.5.9 EFRM	Rule Management and Scenario Tuning	Pleasee confirm on the concurrent number of rules which can be triggered for seamlessly running the various transactions related to eFRMS.	Refer #53

Response to the Pre-Bid Queries

78 1	II	Annexure N / Database Activity Monitoring	Solution should provide functionality to test policies before enabling	Ideal method to test security policies are in UAT enviornment and not on production setup , it is thus requested to remove the clause and leverage UAT for testing purpose	Refer #54

Response to the Pre-Bid Queries

78 2	II	Annexure N / Database Activity Monitoring	The solution should have an agentless DAM architecture that can monitor database activity without the need for deploying agents on the database servers or enabling native logging eliminating performance impacts on database.	We understand the expectation is to have solution which support both agent based and agent less solution. Since one method is required atleast for collection or generation of logs	Refer #55

Response to the Pre-Bid Queries

78 3	II	Annexure N / Database Activity Monitoring	The solution should be able to integrate with the existing Data Activity Monitoring and Governance solution into a consolidated dashboard.	Dam solution allow forwarding security logs to technology such as siem and ticketing solution to help in overall security monitoring and governance. Hope the same is acceptable to the client.	Refer #56

Response to the Pre-Bid Queries

78 4	II	Annexure N / Database Activity Monitoring	The proposed consent management solution should be capable of being deployed On-prem.	Consent management is not part of the DAM solution it is thus requested to move this clause to the relevant solution such as IAM.	Refer #57

Response to the Pre-Bid Queries

78 5	II	Annexure N / Database Activity Monitoring	The solution SAAS platform should be hosted in India.	The RFP talks about On-prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Refer #58

Response to the Pre-Bid Queries

78 6	II	Annexure N / Database Activity Monitoring	The SAAS platform must be SOC2 type 2,SOC type 3, ISO/IEC 27001:2022, 27018:2019 and 27017:2015 compliant	The RFP talks about On- prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Refer #59

Response to the Pre-Bid Queries

78 7	II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if the existing hardware will be used while performing the upgrade and during parallel run	Refer #61

Response to the Pre-Bid Queries

78 8	II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if PLI Application will also be part of this application upgrade. Since PLI is running on EOSL hardware, upgrade of hardware may require PLI application upgrade also, please confirm if PLI application version is EOSL or not, if under mainstream support, will it support the upgraded hardware.	Refer #62

Response to the Pre-Bid Queries

78 9	II	C. Ongoing Support Services, Page 45	10. The incumbent vendor, HPE, is currently responsible for the Operations and Maintenance of certain common infrastructure and security solutions deployed at the existing DC/DR locations, which are shared between POSB and PLI. The SI shall work in conjunction with HPE to maintain the existing IT infrastructure and services specific to POSB till the new DCF is setup and operational, post which the SI shall be responsible for providing the same as mentioned in the RFP. The details of the common solutions are listed in Annexure B.	Please clarify this point. If PLI is not under scope of this RFP, then how the shared resources will be divided between POSB & PLI	Refer #60

Response to the Pre-Bid Queries

79 0	II	5.2.4 Detailed Scope of Work, Page 82	22. The SI is required to follow the below matrix for installing the application instances in DC, DR and NDR environments within the infrastructure.	Please confirm the current availability of - Development/SIT/PREPROD of CBS Resources in DC - Training/PREPROD/UAT of CBS Resources in DR	Refer #70

Response to the Pre-Bid Queries

79 1	EFRM FRS	FRS doc_EFRM_DOP-RFP - point 10	Support IPV6 addressing and broad device/browser compatibility.	Could you please elaborate clarify the requirement as the solution nature is more of internal application and not over wider network.	IPv6 support and broad device/browser compatibility shall be ensured for all applicable applications, including both internal systems and external/customer-facing or internet-based interfaces, wherever relevant. Any prerequisites or minimum configuration requirements shall be clearly specified and communicated to DoP in advance.

Response to the Pre-Bid Queries

79 2	EFRM FRS	FRS doc_EFRM_DOP-RFP - point 47	Support for embedding web content and interactive visualizations (D3.js, Google Charts).	Could you please elaborate clarify the requirement in the context of google charts and D3.js. Is these charts are indicative in nature?	Indicative. Solution should have the capability as asked in the RFP requirements.

Response to the Pre-Bid Queries

79 3	EFRM FRS	FRS doc_EFRM_DOP-RFP - point 28	NLG capabilities to auto-generate insights.	Could you please clarify more on NLG capabilities?	As per RFP

Response to the Pre-Bid Queries

79 4	EFRM FRS	FRS doc_EFRM_DOP-RFP - point 83	Continuous enrichment with new data sources and third-party intelligence feeds.	Please clarify if subscription to third party intelligences will be provided by DOP?	Bidder to ensure any such subscription (if required).

Response to the Pre-Bid Queries

79 5	Sizing Statistics_D OP-RFP	Annexure O – Key Statistics	User metrics	Request to provide following details with respect to AML & FRMS - 1. Total number of AML users (analyst who will work on alerts) 2. Total number of AML users (including branch users if alerts are assigned for EDD) 3.Total number of EFRMS users (analyst who will work on alerts) 4. Number of AML rules 5. Number of Fraud rules 6. Number of AML reports 7. Number of Fraud reports	Refer Annexure E AML Solution for details.

Response to the Pre-Bid Queries

79 6	II	page 93	The SI is required to commit the transaction in Near DC storage first, then on getting acknowledgement from Near DC storage, the transaction will get committed in DC storage. The SI is required to ensure that the database in DC and Near DC Site is always synchronized. The entire process should be completed within 2 milliseconds or less time-period	This is required for all systems or only for CBS ? This will increase the transaction latency due to commit transaction in two DC. Can we choose other solution like DB synchronization two provide near realtime synchronization?	Bidder to propose in accordance with the RFP requirements. Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

79 7	II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	15. CTS - An online image-based cheque clearing system where cheque images and Magnetic Ink Character Recognition (MICR) data are captured at the collecting branch and transmitted electronically, eliminating the actual cheque movement.	"The Cheque Truncation and Clearing System handles sensitive financial instruments and mandates secure exchange of cheque images, MICR data, transaction metadata, and settlement files between Participating Banks, the Clearing House, and Core Banking Systems. To ensure integrity, authenticity, confidentiality, and non-repudiation of these transactions, a FIPS certified HSM is required. CTS specifications mandate digital signing of cheque images/data packets and HSM enables compliance by ensuring tamper-resistant key lifecycle management, auditability, and legally defensible digital signatures. To comply with the CTS security requirements, a separate requirement of HSM must be defined with the industry standard	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

79 8	II	Page 41: 5.1.4.5 Operations and Maintenance Support for the Centralised Cheque Clearing System (CTS)	DoP has an ongoing contract with M/s Oritso Pvt. Ltd. for Monitoring and Maintenance Support for the Centralised Cheque Clearing System (CTS), valid until June 2026. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format.	specifications such as but not limited to: - HSM should have FIPS 140-3 Level 3 with certification in the name of OEM (Proposing third party FIPS 140-3 L3 certification will not be considered) - The solution must support AES (128-256), ARIA, ECC(224- 512), HMAC , SEED, TDES, RSA (1024-4096) and the Crypto mode (CBC, CBC-CS1, ECB, GCM) etc. - The solution must support asymmetric encryption algorithms including RSA (2048/3072/4096-bit) and ECC (P-256, P-384). - HSM Host Interface: Should have at least 4x1 Gigabit Ethernet ports with port bonding. Should have IPv4 and IPv6 support - HSM should have Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature - The appliance and HSM cryptocard should be from the same OEM only and not as a bundled or assembled device. - Proposed HSM should support - Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM - HSM should be PQC ready with the capabilities to evaluate Kyber key generation and encapsulation functions as	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

				well as the hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations. - HSM should support secure key backup and recovery process direct on hardware device or file in encrypted form. - HSM should be configurable to communicate only with authenticated servers using strong cryptographic technique and the secure channel should be terminated at the cryptographic processor and not to the HSM chassis. - Should support clustering, load balancing without the need of external load balancer Please include a dedicated HSM technical specification as part of this requirement. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 5,000 RSA-2048 signing operations per second. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

79 9	II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	eKYC/ADV - Applications integrated with UIDAI to enable Aadhaar-based authentication and KYC services, with secure storage of Aadhaar data in compliance with UIDAI guidelines.	The eKYC and Aadhaar Data Vault solution processes and stores Aadhaar numbers, reference IDs, demographic data, and authentication outcomes. As per UIDAI Security Guidelines and Aadhaar Regulations, entities handling Aadhaar must implement strong cryptographic controls to ensure confidentiality, integrity, and non-repudiation. A Hardware Security Module is required to securely perform, enforce, and protect cryptographic operations and key material used for encryption, tokenization, authentication, and signing within the Aadhaar ecosystem. UIDAI mandates encryption of Aadhaar numbers and related sensitive attributes. To comply with UIDAI mandate, a separate requirement of HSM must be	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

80 0	II	5 destinations and approximately 30 attractions	DoP has an existing contract with M/s Integra Micro Solutions for the Maintenance of Aadhaar-compliant eKYC and Data Vault, valid until November 2029. Both functionalities have been implemented and are currently being maintained by Integra's resources. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines, or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format. This includes support for Aadhaar Data Vault (ADV), an eKYC Solution, and a Hardware Security Module (HSM), in compliance with the guidelines issued by UIDAI and relevant regulatory bodies.	defined with the industry standard specifications such as but not limited to: - HSM should have FIPS 140-3 Level 3 with certification in the name of OEM (Proposing third party FIPS 140-3 L3 certification will not be considered) - The solution must support AES (128-256), ARIA, ECC(224- 512), HMAC , SEED, TDES, RSA (1024-4096) and the Crypto mode (CBC, CBC-CS1, ECB, GCM) etc. - The solution must support asymmetric encryption algorithms including RSA (2048/3072/4096-bit) and ECC (P-256, P-384). - HSM Host Interface: Should have at least 4x1 Gigabit Ethernet ports with port bonding. Should have IPv4 and IPv6 support - HSM should have Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature - The appliance and HSM cryptocard should be from the same OEM only and not as a bundled or assembled device. - Proposed HSM should support - Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM - HSM should be PQC ready with the capabilities to evaluate Kyber key generation and encapsulation functions as	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

			well as the hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations. - HSM should support secure key backup and recovery process direct on hardware device or file in encrypted form. - HSM should be configurable to communicate only with authenticated servers using strong cryptographic technique and the secure channel should be terminated at the cryptographic processor and not to the HSM chassis. - Should support clustering, load balancing without the need of external load balancer Please include a dedicated HSM technical specification as part of this requirement. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 5,000 RSA-2048 signing operations per second. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

80 1	II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	3. The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-2 Level 3 or higher standards.	As FIPS 140-2 validation certificates will be moved to the Historical List in September 2026, they will no longer be considered active for regulated compliance or new procurements. Request: Replace the existing clause with the following updated compliance requirement: "The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-3 Level 3 or higher standards."	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

80 2	II	Page 17: 4. Current State Overview Table 4: Functional Blocks of POSB	9. Card Management System - Card Management System is a solution that manages the complete ATM/Debit Card Issuance cycle for DoP customers.	The Card Management System and ATM Switch handle issuance, lifecycle management, authorization, and verification of payment card transactions. These systems must securely perform sensitive cryptographic operations, including PIN processing, card data encryption, EMV cryptograms, key exchange, and secure key management. To ensure compliance with global payment security standards, these cryptographic operations must be executed within a certified payment HSM. Please add the below clause: The solution shall integrate with a certified Payment HSM to securely perform cryptographic functions related to PIN processing, EMV card issuance, transaction authorization, message authentication, and	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

80 3	II	Page 16: 4. Current State Overview	13. ATM Switch - ATM Switch is required to handle all ATM transactions of the customers	secure key management, in compliance with PCI PIN Security Requirements, EMV Standards, and card scheme mandates. It must follow the industry standard specifications such as but not limited to: - Capable of translating up to 10000 PIN triple DES Pin block Per second and minimum of 25 PIN triple DES Pin block Per second - Should have GUI/CLI available with 2 factor Authentication using USB Tokens/smart cards. - HSM Must have two dedicated port for host communication and atleast one dedicated management port. - The proposed payment HSM must be PCI v3 certified. - HSM should support variant and keyBlock LMK. - HSM must support cryptographic separation of application keys using different LMK and should be capable of storing up to 20 LMKs. - HSM remote management solution must have PCI HSM v3 Remote Access Platform (RAP) certification - HSM should support remote access technology with encrypted connection to maintain security in all configuration and remote key loading processes. Kindly confirm whether DOP looking to secure the	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

				transactions as per PCI guidelines using a payment HSM? if yes, please help to add a seperate section for the technical requirements of payment HSM. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 1,000 TPS. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

80 4	II	Page 98: 5.2.4.8.3 Other Security Requirements c) Data at Rest	1. The SI shall ensure that the data at rest, which is stored other than in the hardened application or database production systems, is protected by encryption that is consistent with recommendations from DoP /other Government agencies and NIST/SANS/OWASP.	Industry best practices and NIST/OWASP recommendations for data-at-rest encryption require not only the application of cryptographic algorithms, but also secure generation, storage, lifecycle management, access control, and rotation of encryption keys. Without a centralized and secure Key Management System (KMS), encryption implementations become fragmented, difficult to audit, and may not meet compliance expectations of Government / DoP frameworks for critical data protection. Kindly confirm whether the intent of the above clause includes deployment of a centralized enterprise Key Management Solution to ensure: - Cryptographic key generation, storage, and lifecycle management - Key rotation and revocation policies - Separation of roles and access controls - Auditability of cryptographic operations - Secure integration with applications, storage, virtualization, and cloud platforms - Compliance with NIST recommendations for key management. please help to add a	Corrigendum Annexure HSM

Response to the Pre-Bid Queries

				seperate section for the technical requirements of Key Management Solution. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT KMS. Kindly confirm if this understanding is correct. Please also confirm the number of servers and databases that fall within the scope of this requirement.	

Response to the Pre-Bid Queries

80 5	II	Database Activity Monitoring	The solution should support rich analytics and provide options to view activities on a specific databases, activities from a specific user, activities on sensitive content etc.	Please confirm whether DOP is expecting a Database Risk Analytics mechanism that provides behavioral analytics, user risk profiling, threat indicators, compliance reporting, and incident investigation capabilities.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

80 6	II	Database Activity Monitoring	The solutions should provide customisable policies using algorithms as well as algorithmic validators wherever possible to discover and classify sensitive records in MySQL.	Our understanding is that DOP have 2 core 36 on-prem MS SQL databases, and there are no other databases. Considering the expansion, please confirm if the number of databases can go up to 100?	Refer #428

Response to the Pre-Bid Queries

80 7	II	Database Activity Monitoring	The solution should be able to integrate with the existing Data Activity Monitoring and Governance solution into a consolidated dashboard.	Our understanding is that the existing DAM solution is from Thales/Imperva, please confirm if this understanding is correct.	Refer #56

Response to the Pre-Bid Queries

80 8	II	5.2.2 Shifting of IT Infrastructure components from the existing DCF to the new DCF		Please confirm only the applications listed in App Details sheet need to be migrated to new DCF and provide details as required in sheet.	As per RFP

Response to the Pre-Bid Queries

80 9	II	5.2.2 Shifting of IT Infrastructure components from the existing DCF to the new DCF		Please confirm these are the only external/internal systems need to be integrated in new solution ? ATM Switch POS SFMS Cheque Book PLI (Postal Life Insurance) Card Management System NSDL NPCI UIDAI BBPS IVR POSB POST Debit Credit SMSC - SMS SMTP - Email Data Lake NACH	As per RFP

Response to the Pre-Bid Queries

81 0	II	Annexure J - IMPS point 7	Provide intuitive and user-friendly interfaces to accommodate various devices and accessibility needs.	IMPS switch is a backend switch without UI interface. IS DOP expecting a UI for IMPS?	As per RFP

Response to the Pre-Bid Queries

81 1	II	6.CA Arcot	CA Strong Authentication for Business Users	Please confirm CA Arcot is not in scope of change or migrate,	CA Arcot is part of RBA solution.

Response to the Pre-Bid Queries

81 2	II	Annexure O – Key Statistics - Page 268	User Metrics	Please check Finacle sizing questionair sheet and current hardware sheet in this excel. Volumetrics information required with breakups	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

81 3	II	5.1.5.1 General A. Core Responsibilities	Ensure uninterrupted availability and reliability of IT services in compliance with applicable regulatory and security standards, including RBI, CERT-In, and PMLA.	PLs provide which RBI and ISO standards needs to be additionally provided for existing system for bidder to plan. There is no mention of which particular standards that need to be followed as a priority for compliance standards.	Bidders are expected to ensure adherence to relevant RBI, CERT-In, DPDP Act, and any other applicable regulatory and statutory compliances.

Response to the Pre-Bid Queries

81 4	II	5. Detailed Scope of Work	Track 2: Operations and Maintenance of IT Infra at new DC, NDC and DR	RFP asks for Zero RPO - but when the operations transfer to DR then how will Zero RPO be maintained without a NDR site. We request Zero RPO to be removed when moving to DR site.	Refer #529

Response to the Pre-Bid Queries

81 5	II	3.2 Broad Scope of Work <u>Sub Point</u> : 3. Application Development and Enhancements Page 14	Establishment of separate environments for development, user acceptance testing (UAT), and sandbox/pre-production. Each environment should simulate a near-production network, security, and data flows.	There needs to be percentages defined for each environment for app Non production (in relation to production)else there will be no way to assess and compare one Bidder's Sizing to another objectively. Typicall in any Banking set up - percentages are defined for each enviornment like (for example:) 10% of Prodcution for Development (example) 30% for UAT (example only) 100% for Pre Prod (example only) 100% for Load Testing (with say 60% utilisation) - example only 100% for DR	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

81 6	II	Page 24	Figure II: Existing Contract(s) Timeline (Apr 2026 onwards)	Request here in increasing the upgrade timelines	Refer #361

Response to the Pre-Bid Queries

81 7	II	Page 241	Annexure D – Mobile Banking	Is DoP using Finacle mBanking and to what extent. Also please confirm the integration with Finacle MBanking.	Refer #453

Response to the Pre-Bid Queries

81 8	II	Page 261	Annexure M – Tech Stack	Is CSIS configured in DOP?	As per RFP

Response to the Pre-Bid Queries

81 9	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall provide a unified view of all UPI transactions initiated across various platforms.	Does DOP support UPI merchant transactions?	Refer #458

Response to the Pre-Bid Queries

82 0	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall support digital self-onboarding processes for new customers (e.g., Savings Accounts) and existing customers for new products/schemes (e.g., FD/RD) through an OTP-based eKYC/vKYC mechanism within the Internet Banking platform.	Are loan/CCA/ODA accounts present?	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

82 1	Volume II - Scope of Work	Page 261	Annexure M – Tech Stack	Please share current finacle architecture diagram in DOP.	Refer #460

Response to the Pre-Bid Queries

82 2	Volume II - Scope of Work	Page 209	Annexure A – Existing Infrastructure	What is the current size of the Finacle DB	Refer #461

Response to the Pre-Bid Queries

82 3	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall provide a unified view of all UPI transactions initiated across various platforms.	1) What is the current UPI solution used by DOP or it has a link with IPPB for processing UPI transactions 2) Kindly elaborate on the processes ?	Refer #458

Response to the Pre-Bid Queries

82 4	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: system shall provide comprehensive functionalities for fund transfers, including intra-bank (POSB to POSB) and interbank (NEFT, RTGS, IMPS)	1) What is the process for handling cross border inward remittances ? 2) What are the channels for processing this ?	Refer #463

Response to the Pre-Bid Queries

82 5	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: Seamless Integration between Internet & Mobile Banking Platform.	1) Assuming current mobile app is Winjit , what is the process followed to connect with online Banking 2) How we are envisaging cross channel experience	1. Refer #453 2. Bidder to propose

Response to the Pre-Bid Queries

82 6	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system shall support digital self-onboarding processes for new customers (e.g., Savings Accounts) and existing customers for new products/schemes (e.g., FD/RD) through an OTP-based eKYC/vKYC mechanism within the Internet Banking platform.	Kindly provide more details on the existing Origination system/intermediary onboarding system(if any) in the Bank to be able to complete the flow between Channels, Origination and Core banking solution.	Refer #465

Response to the Pre-Bid Queries

82 7	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system should provide functionalities for Integration with DMAT Accounts (up to 4 Demat account providers)	1) What is the process for access and integration of internet (online) with DMAT account 2) What are the related use cases	Refer #466

Response to the Pre-Bid Queries

82 8	Ref Annexures	Annexure J	Refer to Internet banking sheet in the xls: The system should provide functionalities for NACH mandate/ e-mandate management.	1) What are the scenarios for NACH mandate considering loan EMI from DOP is not there ? Is this for insurance, utility bill or any other mandate	Refer #467

Response to the Pre-Bid Queries

82 9	Volume II	Annexure O – Key Statistics	Online transactions per day 10,00,000	Please mention whether these are business transaction volume or individual credits/debits (part-trans) In Finacle terms, please clarify whether this volume is referenced from HTD table or HTH table.	Refer #468

Response to the Pre-Bid Queries

83 0	Volume II	Annexure O – Key Statistics	Offline transactions per day (peak) 1,50,00,000	Please provide breakup of these transactions as system generated (interest/fees/charges/etc.) or customer generated (transfer/deposit/withdrawal/ etc.)	Refer #469

Response to the Pre-Bid Queries

83 1	Volume II	5.2.5.10 Middleware	Performance and Scalability Metrics: • The solution must handle a sustained throughput of at least 20,000 transactions per second (TPS) with the capacity to scale up to 50,000 TPS to accommodate future growth over the contract period.	Please clarify whether Hardware capacity estimations are to be provided for 20,000 TPS, 50,000 TPS or 300 TPS	Refer #6

Response to the Pre-Bid Queries

83 2	Volume II	Annexure O – Key Statistics	8. Online transactions per second (TPS) 300		Refer #471

Response to the Pre-Bid Queries

83 3	Volume II	Annexure O – Key Statistics	User Metrics:	Please provide year wise business volume projections as per adjacent sheet "Finacle Sizing Questionnaire"	Refer #472

Response to the Pre-Bid Queries

83 4	Volume II	7. Physical Server Details Annexure M – Tech Stack	3. E-Banking 4. FAS (Finacle Alert Solutions) 5. Finacle CBS	Please provide details of Current Hardware provisions as per adjacent sheet "Current Finacle HW Details"	Refer #473

Response to the Pre-Bid Queries

83 5	Volume I	5.20 Form 20: Manufactures'/Producers Authorization Form		The proforma provided is more onerous than we typically agree. We suggest using a template that has been pre-approved other central government entities and PSUs.	Refer #474

Response to the Pre-Bid Queries

83 6	Volume 1	5.22 Form A 22: Proforma for Individual Non-Disclosure Agreement		The NDA format provided is designed for individual employees. Please provide revised NDA format that applies to subcontractor entities. Moreover, please note that it may be operationally difficult to enter into individual NDAs with employees. Hence, we request that at least with respect to a subcontractor entity, the NDA be restricted to an organizational level as the organization will be responsible for all acts and omissions of its employees.	Refer #475

Response to the Pre-Bid Queries

83 7	Volume 3	1.20.1 (ii): Insurance Cover	The above insurance policies shall be of appropriate values so as to cover risks of SI under this Agreement.	We suggest specifying limits on insurance claim for all types of insurance policies to be maintained as per the MSA, in the following manner: USD 1 Million per occurrence and USD 2 Million on annual aggregate of the claims.	Refer #476

Response to the Pre-Bid Queries

83 8	Volume II - Scope of Work	Page 14	Upgrade of Finacle Core Banking solution from version 10.2.13 to 10.2.25 and Finacle Alerts Solution, incorporating the most recent service packs to ensure optimised system performance and capabilities.	We recommend DoP to change 10.2.25 to 10.2.25 or higher version available during the solutioning.	Refer #477

Response to the Pre-Bid Queries

83 9	BOQ_93745 7	For Example in "Tab : 2.4 New Development" and similarly to other tabs		The level of breakup required as per the format may not be possible for a few items.	Refer #478

Response to the Pre-Bid Queries

84 0	II	page 40	Finacle IVR/CRM/Chatbot	What Finacle IVR and Chatbot systems are and it's scope.	It has been discontinued. Bidder has to integrate with DoP contact centre.

Response to the Pre-Bid Queries

84 1	Volume of the RFP I	Section 2.2 Purpose, Page - 15, Clause No. - 2	All the material/information shared with the Bidders during the course of this procurement process as well as the subsequent resulting project following this process with the successful Bidder, shall be treated as confidential and should not be disclosed in any manner to any unauthorized person under any circumstances. The Bidders shall furnish a Non-Disclosure Agreement (NDA) as per the format provided in Form A 21. The bidders shall also ensure that all its employees and agents and sub-contractors involved in the Project, execute individual non-disclosure agreements as per Form A 22, which have been duly approved by DoP. Copy of such individual NDAs to be provided to DoP by the SI as and when demanded.	Does Bidder need to furnish NDA if bidder engages with existing vendors of POSB as mentioned in Volume II. Please clarify	As per RFP

Response to the Pre-Bid Queries

84 2	Volume of the RFP I	Section 3 Criteria for Evaluation, Page - 36, Clause No. - 3.1(b)	Technical presentation shall be a part of the process for evaluation of the bids.	Bidder seek clarification on the Days we get for Technical presentation post submission of bid.	Bidders shall be given reasonable notice before scheduling of technical presentation post submission of bid.

Response to the Pre-Bid Queries

84 3	Volume of the RFP II	Section 3.2 Broad Scope of Work, Page - 12, Clause No. - Solution Architecture IT 2.0	Collectively, the components of the banking system as covered in this RFP scope are also referred to as POSB IT Systems. The SI selected through the RFP shall be responsible for the following: Figure I: Solution Architecture IT 2.0	In Figure I: Solution Architecture IT 2.0, there is a Layer of End Point Infrastructure/Peripheral Devices. Bidder needs detailed clarification as this is not covered in Volume 2 of RFP. We understand End Point Infrastructure/Peripheral Devices will be taken care by DoP and Bidder has no role to in End Point Infrastructure/Peripheral Devices. Please confirm is Bidder Understanding Correct.	Endpoint infrastructure/ Peripheral Devices are already in place.

Response to the Pre-Bid Queries

84 4	Volume of the RFP II	Section 3.2 Broad Scope of Work, Page - 14, Clause No. - 5 IT Infrastructure Setup and Transition	Assess existing infrastructure at current DC, DR sites to identify components for migration or replacement. Ensure DC, DR readiness with failover and recovery capabilities and prepare migration documentation.	To carry out Assessment, this will require Physical visit at current DC and DR. Bidder's Teams would need permission along with existing POSB Infrastructure SME's at existing DC & DR. Please clarify will permission be allowed by DoP in Existing DC and DR.	Interested bidders may request for physical visits to the existing DC and DR upon request. Such requests should be submitted via email to pmu-fsdivision@indiapost.gov.in within three (3) days from the release of the corrigendum.

Response to the Pre-Bid Queries

84 5	Volume of the RFP II	Section 3.2 Broad Scope of Work, Page - 14, Clause No. - 5 IT Infrastructure Setup and Transition	Execute lift-and-shift migration of infrastructure from existing DCF's to the new facilities with minimal disruption. Perform comprehensive infrastructure and application-level testing post-migration.	Bidder understands Lift and shift migration is limited to the infrastructure under warranty/AMC. Pls clarify	No EOS/EOL hardware shall be utilized at new DCF.

Response to the Pre-Bid Queries

84 6	Volume of the RFP II	Page 14 Section 5	Assess existing infrastructure at current DC, DR sites to identify components for migration or replacement. Ensure DC, DR readiness with failover and recovery capabilities and prepare migration documentation.	Share the complete inventory details with configuration/ATS warranty details for DC and DR. Also highlight the approach for capturing the finding in assessment and translation into BOQ for consideration	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

84 7	Volume of the RFP II	Section 5.1 Track 1: Takeover and Transition, Page - 21, Clause No. - VDA	POSB IT Infra Refresh (IBM P10 Servers, SAN Switch & Tape Library)	Please provide LPAR level information application wise deployment on Power 10. Pls share detailed IBM power server,storage,Tape library inventory covering capacity and warranty details currently managed by VDA.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

84 8	Volume of the RFP II	Section 5.1.5.2 Scope of Work for Operations and Maintenance, Page - 47, Clause No. - Mail Messaging, Archival and Bulk Mail Table 8: Roles and Responsibilities of the SI	Coordinate with OEMs, monitor mail queues, and perform upgrades. The solution deployed is in the Hosted Environment. SI needs to do coordination work with POSB and Mail messaging OEM.	Please provide Technology Stake Information of Mailing along with where it has been hosted. Additionally RFP does not have information of Mail messaging OEM. Request POSB to provide	NIC mail, only integration is in Bidder scope.

Response to the Pre-Bid Queries

84 9	Volume of the RFP II	Section 5.1.5.2 Scope of Work for Operations and Maintenance, Page - 47, Clause No. - End Point Patch Management Table 8: Roles and Responsibilities of the SI	Perform proactive patch management for all infrastructure components, including servers, databases, middleware, and end-user endpoints.	Please provide complete details/inventory of end- user endpoints nos per location Additionally RFP does not have clarity on O&M Support for end- user endpoints, please clearly expectation from Bidder on end- user endpoints	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

85 0	Volume of the RFP II	Section 5.1.5.2 Scope of Work for Operations and Maintenance, Page - 47	DoP's ongoing Operations are broadly classified under three (3) categories of services that the SI is required to offer: 1. Domain Services 2. Additional Services 3. Cross-Functional Services	Under this section RFP does not have clarity on 2.Additional Services. Request POSB to provide	As per RFP

Response to the Pre-Bid Queries

85 1	Volume of the RFP II	Section 5.2.1.1 Facility Requirements, Page - 52, Clause No.5.2.1.1.1 General Requirements (8)	The buildings housing the DC and all infrastructures therein should be covered under comprehensive insurance on an ongoing basis, including risk related to but not limited to earthquake, floods, fire, lightning, terrorist attack, etc. A copy of the valid comprehensive insurance should be submitted every year during the contract period.	We understand all the Infrastructure deployed into new DCF's will be on the name of DoP throughout the contract period, hence cost of insurance for all infrastructure will be through DoP appointed insurance company Request to confirm.	The assets shall be in the name of DoP. Insurance coverage for all proposed and deployed IT infrastructure components—including servers, racks, cabling, and related equipment— under this contract shall be provided by the Bidder. SI shall provision for comprehensive insurance coverage on its own.

Response to the Pre-Bid Queries

85 2	Volume of the RFP II	Section 5.2.1.1 Facility Requirements, Page - 52, Clause No.5.2.1.1.2 Seating Space (1) and Annexure I	The SI shall provide seating space for 5 DoP personnel at the DC sites. The seating space should be at least 30 Square feet of work area per seat. Annexure I - Seating space for a minimum of 10 representatives of DoP and for SI shall be provided by the DCF Provider at DC.	Seating space in Volume 2 and Annexure I is contradictory. We understand this seating space only required at the DC site Mumbai.- Pls confirm DoP to confirm if any seating space requirement in DR & NDC. The seating space requirement is within dedicated Cabin or shared seating space. Request DoP to please clearly and amend accordingly	The revised clause to be read as: "The SI shall provide seating space for 5 DoP personnel at the DC sites and 3 personal at DR site. The seating space should be at least 30 Square feet of work area per seat."

Response to the Pre-Bid Queries

85 3	Volume of the RFP II	Section 5.2.1.1 Facility Requirements, Page - 52, Clause No.5.2.1.1.2 Seating Space (4)	Dedicated Fireproof storage Cabinets with a lock should be provided, preferably adjacent to the seating area/within the seating area.	Request DoP to provide specifications of Dedicated Fireproof storage Cabinets within the seating area	Bidder to propose as per RFP requirements.

Response to the Pre-Bid Queries

85 4	Volume of the RFP II	Section 5.2.4 Detailed Scope of Work, Page - 82, Clause No.22	The SI is required to follow the below matrix for installing the application instances in DC, DR and NDR environments [Development SIT Training UAT PREPROD PROD (WEB, APP, DB)]within the infrastructure.	Request DoP to provide existing Applications instances details of deployments in DC, DR Development SIT Training UAT PREPROD PROD (WEB, APP, DB) This is required to see if any of the above mentioned environment is not deployed so the SI can factor as in Proposal.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

85 5	Volume of the RFP II	Section Annexure A – Existing Infrastructure, Page - 208, Clause No. Network Integration (NI)	Network infrastructure at DC, DRC & other locations is provided and managed by BSNL.	Request DoP to please confirm Network Integration (NI) for new DCF (DC, DR and NDC) will be provided and Managed by BSNL through DoP. SI have to do coordination with BSNL throughout contract period	DoP NI shall provide connectivity till DCF locations.

Response to the Pre-Bid Queries

85 6	Volume of the RFP II	Section Annexure A – Existing Infrastructure, Page - 208, Clause No. Bandwidth Connectivity	Primary Connectivity is provided by BSNL, & Secondary connectivity is provided by Sify.	We understand that Primary and Secondary will be same as per this clause and bandwidth will be directly taken care by DoP with BSNL & Sify. SI does not have any role on Bandwidth Connectivity. Please Confirm.	DoP NI shall provide connectivity till DCF locations.

Response to the Pre-Bid Queries

85 7	Volume of the RFP II	Section Annexure A – Existing Infrastructure, Page - 208, Clause No. As-Is Building Blocks: DoP's Network Infrastructure	Network Operation Center Chennai	As per As-Is Building block, we understand existing NOC is at Chennai and will continue the same till Contract Period. As-Is Services ordered through Chennai NOC. - Network Management. - DC IT Infrastructure Management. Request DoP to confirm so that Bidder will not include NoC location into Proposal.	NOC location is not part of SI scope.

Response to the Pre-Bid Queries

85 8	Volume of the RFP II	Section Annexure A , Page - 211 to 214, Clause No. Bill of Quantity, Compute	The inventory list of IT infrastructure currently deployed at the existing DoP DC and DR sites under the scope of the project is provided below. This list includes servers, storage, network equipment, and associated components supporting POSB and PLI operations. The configuration and utilization may change during the course of the bid process as per the requirements. 1. Compute: The following categories of servers have been installed and configured in the Data Centre and DR site to implement the DoP business applications and supporting system software. The common infrastructure layer is also used by some of the business applications. The key types of compute infrastructure are provided below: • Database servers • Application servers • Web servers • Mail & Messaging, Active Directory and Antivirus on x86 servers. • Backup servers • Internal DNS and proxy servers • SSO/ID Management servers • ESM on Blade servers • Management Servers for security, Network, EMS, Storage and backup • Infrastructure Servers for Proxy DNS and others	Bidder would need additional details of Physical Servers, virtualization servers, OS, application mapping deployed on Server Model/Make Version provided in annexure A Request DoP to provide comprehensive inventory details with segregation across existing DC and DR	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

85 9	Volume of the RFP II	Section Annexure A , Page - 221, Clause No. Current Utilisation Levels	Current Utilisation Levels " CPU Utilisation (%)" and Memory Utilisation (%)"	Request DoP to confirm weather mentioned utilization of " CPU Utilisation (%)" and Memory Utilisation (%)" is "Average or Peak"	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

86 0	Volume of the RFP II	5.2.1.1.13 Page 60	The SI shall ensure deployment of dedicated experienced manpower, including management and support staffing for maintaining and operating their data centre non-IT infrastructure.	DCF will cover colocation and assoiated services managed by common Datacenter services team of DCF provider for entire facility selected for DoP.Bidder suggest to modify the clause accordingly	As per RFP

Response to the Pre-Bid Queries

86 1	Volume of the RFP II	5.1.5.2 Page 48	The SI shall be responsible for taking centralised backups from DC, NDC and DR for all the servers	Centralised backup will be at DC locations for all workloads deployed across DC,NDC and DR .NDC location wil have only storage and severs required to maintain RPO ~ zero , backup infrastructure must be limited to DC and DR location only.Pls clarify	NDC location will have only storage required to maintain RPO ~ zero

Response to the Pre-Bid Queries

86 2	Volume of the RFP II	5.2.4Pg 83	The deployment of the backup solution should guarantee continuous operation of Core Banking databases and other databases during daily, weekly, monthly, and quarterly backup processes. If additional hardware and software are deemed necessary for this purpose, the SI is mandated to include them in this RFP. Additionally, the SI is required to present a usable all-flash disk-based backup solution.	Do DoP looking for backup capacity entirely on ALL flash disk at DC and DR site.DoP must allow SI to factor the backup solution basis the backup and retention policy as the industry best practices using Tiered storage with different disk type.pls clarify and amend NFR accordingly	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

86 3	Volume of the RFP II	5.2.4Pg 84	The SI is required to provide, implement, and maintain all proposed hardware components, including servers, storage, SAN, backup solution, NAS, disk-based backup, and both hardware and software components of the Load Balancer. Additionally, the SI is responsible for managing these hardware components.	Pls share the specific use case for software load balancer requirement.Can SI provide the hardware load balancer for providing LB functionality.Pls clarify or amend tech sepcifications for SLB	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

86 4	Volume of the RFP II	5.2.4 Page 81	The SI is required to showcase adaptability in addressing dynamic sizing needs, aligning seamlessly with POSB's growth. Additionally, the SI is obligated to consider a minimum of 20% Year-on-Year growth in infrastructure to accommodate the future projections. It is expected that the SI acknowledges POSB's discretionary authority to procure the necessary delta sizing as required. If the quota for the current year is surpassed before the year-end, the subsequent year will commence, and the SI is required to make provisions to accommodate the required delta sizing. The SI is further required to present a comprehensive plan detailing how they intend to scale the infrastructure to meet the specified growth rate.	20% year on year growth in infrastructure is not applicable for non-prod environment (Dev,SIT,Training,UAT,PRE PROD) as per %age of production?Pls calrify	For all non-production environments, an initial infrastructure baseline should be established proportionate to the percentage provided. This baseline should be subsequently enhanced with the introduction of new functionalities. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

86 5	Volume of the RFP II	5.2.1.1.1 Page 94	The SI is required to ensure that the database in DC and Near DC Site is always synchronized. The entire process should be completed within 2 milliseconds or less time-period.	DC-NDC link will have network latency ranging between 2-10ms ,therefore entire process should be completed within 2-5ms milliseconds.Pls amend	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

86 6	Volume of the RFP II	Annexure B ,Page 225	SMS relay, Mail relay	SI need to factor ,provision and manage VM with required OS for installing SMS relay ,mail relay application. DoP existing vendor(sms and mail realy) will deploy and manage the SMS relay and mail relay application in new DC,NDC ,DR ,SI will do the vendor management in case of any application issue.Pls clarify	DoP shall provide the SMS and mail relay services. Provisioning and management of the virtual machines, including installation of the required operating system to host SMS relay and mail relay applications, shall be the responsibility of the SI. SI has to integrate with SMS and Email providers.

Response to the Pre-Bid Queries

86 7	Volume of the RFP II	Detailed Scope of Work-Page 21	Shifting of IT Infrastructure components from the existing DCF to the new DCF	Please provide the following details 1) Existing DC, DR network architecture 2) Existing DC, DR traffic flow 3) No of links and their connectivity types and bandwidth	As per RFP

Response to the Pre-Bid Queries

86 8	Volume of the RFP II	Special Considerations-Page 78	Arranging rental hardware (cost to be included in the bid; no additional payments will be made).	Suggest client to provide the hardware along with associated requirement for upgrade part of Track 1.Pls clarify	As per RFP

Response to the Pre-Bid Queries

86 9	Volume of the RFP II	Scalability- Page 90	The SI is expected to ensure the adaptability of the solution, meeting the existing and anticipated customer and account growth across the entire geographical scope of the nation.	Please provide the utilization, CPU, memory, Link utilization of network devices including SLB, LLB in existing DC & DR and provide the future growth.Pls clarify	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

87 0	Volume of the RFP II	Bill of Quantity-Page 218	Routers	As per the inventory shared only existing replication router model is mentioned, please provide the other routers which are used in the existing infra	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

87 1	Annexure L	Leaf Switch	Hardware and Interface Requirement: There must be 300+ 1G Port and 150+ 10/25G ports required for DoP device connectivity. Bidder must configure Fibre/Copper Leaf switches accordingly. The rest of the vacant ports are to be populated as per DoP requirement.	Does we need to provide additional switches as mentioned in the annexure. Also this will be same for both DC and DR. Please confirm	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

87 2	Volume of the RFP II	Annexure B – Common Infra and Security solutions maintained by HPE, Page 225	Active Directory & Domain Name Server Microsoft Windows Server User / Device Authentication and Domain Name Resolution CAL/Devices: 125,837	What is the version of AD Servers and Forest functional Level.	The current Active Directory environment comprises Windows Server 2012 Datacenter and Windows Server 2016 Datacenter versions. The Forest Functional Level is Windows Server 2008 R2

Response to the Pre-Bid Queries

87 3	Volume of the RFP II	Annexure B – Common Infra and Security solutions maintained by HPE, Page 225	Active Directory & Domain Name Server Microsoft Windows Server User / Device Authentication and Domain Name Resolution CAL/Devices: 125,837	Is Domain Controller upgrade supposed to be considered? If Yes, Please share the count of Domain controllers and their locations	Yes, Domain Controller upgrade is required. 8 Domain Controllers each are deployed in DoP DC (DAKC Mumbai) & DoP DRC (CEPT Mysuru).

Response to the Pre-Bid Queries

87 4	Volume of the RFP II	Annexure B – Common Infra and Security solutions maintained by HPE, Page 225	Database Microsoft SQL Server Database Database of ESB, EMS and Security Solution Enterprise SQL 2 Core – 36 Nos	Do we have any Existing EA / SA agreement with Microsoft / MS distributor. If YES share the below details. . Type of Agreement (EA/SA) . Name of Distributor . Discount Level.	As per RFP

Response to the Pre-Bid Queries

87 5	Volume of the RFP II	Annexure B – Common Infra and Security solutions maintained by HPE, Page 225	Database Microsoft SQL Server Database Database of ESB, EMS and Security Solution Enterprise SQL 2 Core – 36 Nos	These License should be perpetul only or with Software Assurance subscription. If with SA, should the tenure be for 5 Years or 7 Years.	As per RFP

Response to the Pre-Bid Queries

87 6	Volume of the RFP II	Annexure B – Common Infra and Security solutions maintained by HPE, , Page 230	1 Microsoft Windows Server Standard 50 Windows Server 2012/2012 R2 10-Oct-23 Physical -Windows Server 2012/2012 R2 (BL685c, DL 120), Windows server 2016 (BL 465c, DL 360 P, DL 380P) Virtual - Windows Server 2022	License count is mentioned as 50, is this 2 core ,8 core or 16 core license each.Pls clarify	As per RFP

Response to the Pre-Bid Queries

87 7	Volume of the RFP II	5.2.1.1 Facility Requirements, Page 55	5.2.1.1 Facility Requirements 5.2.1.1.5 Cooling Requirement 5. Design of cooling system shall follow guidelines of ASHRAE 62.1 2013 (American Society of Heating, Refrigerating and Air-Conditioning Engineers) and ISHRAE (Indian Society of Heating, Refrigerating and Air-conditioning Engineers). • The server area should have precision air conditioning with redundancy, and maintain the ambient temperature of 22°C with +/- 2°C in the entire area. Three sensors are desired in each row - two at both ends and one in the middle. • The server room should have Cold aisle containment to avoid the mixing of cold and warm air.	Amendment in Clause: The Temperature maintained is 24 +/- 2 deg C. And an ASHARE recommended Relative Humidity of 30% to 70%	As per RFP

Response to the Pre-Bid Queries

87 8	Annexure I.xls	A. GENERAL, Row-6	A. GENERAL 6. The DC site should be fully operational, and some DoPs should be functional at the proposed site.	Request to kindly elaborate " <i>some DoPs should be functional at the proposed site.</i> " for better understanding of the requirement.	Clause is omitted.

Response to the Pre-Bid Queries

87 9	Annexure1.xls	A. GENERAL, Row-20	A. GENERAL 15. There should not be any unplanned power outage for more than 15 minutes in the proposed data centre facility during the last 3 years from the date of bid submission. Submit a self-declaration	Bidders proposing New data centers or the DCs currently under construction will not be in position to submit the Self-Declaration asked here. Request to kindly provide an alternate way to the bidders who are proposing Newly Built or Under Construction data centers	For newly commissioned data centres, submission of historical outage self-declaration is not applicable. A self-declaration confirming redundant power design and compliance post-commissioning shall be accepted.

Response to the Pre-Bid Queries

880	Annexure1.xls	C. GENERAL, Row-53	C. POWER 3. Backup generators (Redundant) should be capable of providing power backup for 72 hours. Backup generators should be capable of providing power continuously for at least 72 hours, and even during the refilling period of fuel tanks. The capacity of each set of diesel generators should be sufficient to take care of the entire power load of the Data Centre. The DCF Provider should ensure an uninterrupted supply of diesel to the DG with an adequate storage facility. The Diesel Generators shall be of Data Centre Continuous (DCC) rating type.	. As per Tier-III/Rated 3 standards, the DC is equipped with DG backup and onsite fuel storage up to 48 hours. The Diesel storage onsite is for 48 Hrs of runtime on Full load. Hence request to kindly revise this to 48hrs	Refer #381

Response to the Pre-Bid Queries

88 1	Annexurel.xls	F. GENERAL, Row-115	F. SERVER ROOM AREA 26. Perimeter Wall and Doors should have at least 1 1-hour fire Rating.	Kindly clarify if this is 1 hour or 11 hours?	Refer #387

Response to the Pre-Bid Queries

88 2	Annexure I.xls	J GENERAL.Row-182	J. SEATING SPACE 1. Seating space for a minimum of 10 representatives of DoP and for SI shall be provided by the DCF Provider at DC.	Could you please confirm whether there are any seating requirements for the DR and NDC? If so, kindly share the complete details	The revised clause to be read as:: "The SI shall provide seating space for 5 DoP personnel at the DC sites and 3 personal at DR site. The seating space should be at least 30 Square feet of work area per seat."

Response to the Pre-Bid Queries

88 3	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 9: Backup Scheduling : Multi-site scheduling with automated copy to NDC and replication to DR; Parallel job execution supported.	Request DoP to correct the understanding as " Primary Backup Copy of DC site to be replicated to NDC and DR Site as well " accordingly Backup Solution will be define.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

88 4	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 20: High Availability: Backup server clustering for DC and NDC; Failover capability so backups continue even if DC is unavailable.	Request DoP to correct the understanding as " The expectation is to define a backup server and storage architecture that is available at both the DC and NDC sites to back up DC site data."	The revised clause to be read as: High Availability: Backup server clustering for DC and DR; Failover capability so backups continue even if DC/DR is unavailable. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

88 5	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 3: Backup Types: Tiered retention policies supporting: short-term backups at DC, operational copy at NDC, long-term archival at DR.	Request DoP to define the short-term, operational, and archival copy retention periods, along with the backup window and throughput requirements, to enable accurate backup storage sizing.	Retention policy to be designed as: Weekly backups: 3 months. Monthly: 1year. Annual backups: 7or 7+ years. The revised clause to be read as: Backup Types: Tiered retention policies supporting: short-term backups at DC & DR on disk, operational copy at DC & DR over tapes, long- term archival at DC & DR over tapes.

Response to the Pre-Bid Queries

88 6	Volume of the RFP II	Annexure A – Existing Infrastructure: Page no 211 : As-Is Storage Deployment Architecture: DC and DR	4. For the Backup Solution, the IBM TS 3500 Tape Library is being implemented	Request DoP to provide details of the existing backup solution, including backup software and its version, backup policies, backup storage at DC and DR sites, and the backup window, to help define the new architecture	Please refer As-Is Infra details: Annexure B – Common Infra and Security solutions and Annexure C – BoQ of Existing Licenses

Response to the Pre-Bid Queries

88 7	General			Request DoP to provide allocation and Peak CPU/Memory/Storage utilization details for each Physical and Virtual Server, as well as Storage Systems, in order to design the required solution along with the final Bill of Material.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

88 8	General			Request DoP to provide Operating System and version details (Windows / Linux) along with the licensing information for each Physical and Virtual Server. This information is required to design and finalize the required Operating System licenses, the number of OS instances, and the final Bill of Material. .	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

88 9	Volume of the RFP II	5.2 Track 2: Platform Modernization and Feature Development : 5.2.1 Implementation of On-Premise Colocation Data Centre at the New DCF Page No.: 82	13. the SI is obligated to consider a minimum of 20% Year-on-Year growth in infrastructure to accommodate the future projections.	Kindly confirm if Year-on-Year (YoY) growth needs to be considered as part of the licensing calculation for the number of OS instances/servers.	The growth rate provided is indicative, envisaged keeping in consideration the growth rate and the new functionalities which are to be implemented. Selected Bidder to adequately size the Infra as per the actual growth rate during the engagement.

Response to the Pre-Bid Queries

89 0	Volume of the RFP II	5.2.2.1 Indicative Migration Strategy : 2. New DC/DR/NDC Setup : Page No 73	Based on the findings of the assessment, the SI shall plan, provision, and commission the new DC, DR and NDC infrastructure at the proposed sites. The new infrastructure setup must be completed as per the timelines defined in this RFP.	Request DoP to provide the final Compute sizing (covering both Physical and Virtual instances) and Storage sizing requirements so that the new Server, Storage, and Operating System licenses can be finalized as part of the migration. Without the confirmed sizing inputs, it will be difficult to plan and finalize the design after the assessment phase, especially for the new procurement.	Bidder to propose.

Response to the Pre-Bid Queries

89 1	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : x86 Server Compliance	2 TB DDR5 RAM- Minimum 32 DDR5 DIMM slots RDIMMS 8TB Max, supporting speeds of min 4800MT/s	The current AMD EPYC DDR5 server platform supports a maximum of 24 DDR5 RDIMM slots per 2-socket system due to the CPU memory-controller and channel architecture. Request you please update requirement to accommodate AMD processor	Refer #99

Response to the Pre-Bid Queries

89 2	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : x86 Server Compliance	Sr. NO. 2 Processor: Intel Platinum/ AMD processor @ 2.0 GHz or higher 64 Cores in 2 Sockets	Request you to please mention that latest generation Intel Xeon Platinum or AMD EPYC processors to be quoted meeting or exceeding the following minimum specifications: 1. Base frequency 2.0 GHz or higher 2. Total 64 cores in dual- socket configuration (i.e., combination of 2 processors whose combined core count is at least 64)	Refer #98

Response to the Pre-Bid Queries

89 3	Volume of the RFP II	5.2.4.3 Integration, page no 89,Clause 11	11. The SI is required to deploy engineers from the OEM for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	We understand that the OEM will be responsible for the implementation of the newly proposed solution under this RFP, and the OEM will not be involved in migration activities.	As per RFP

Response to the Pre-Bid Queries

89 4	Volume of the RFP II	5.2.4.4 Scalability, Page 91, clause 5	The SI is required to guarantee that the solution accommodates fluctuations in load patterns, considering factors such as month ends, quarter ends, year-ends, and regulatory changes.	Please share the following data for Servers,Storage,backup solution, network.SLB.LB, Security devices , this information is require for the sizing the solution Peak load during: Month-end processing Quarter-end & year-end financial closures Regulatory reporting windows Audit & reconciliation periods	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

89 5	Volume of the RFP II	6.7.4.1 Performance Service Levels , a) SLA for Infra Availability , Page 151	1. Infra Availability (Availability of the infra components for at least 99.95% of the time, measured every month.)	Amendment in Cluase(Defination: Availability of the over all Infra Solution for at least 99.95% of the time, measured every month.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

89 6	Volume of the RFP II	6.8.4 SLA for Infrastructure, Page 153	1. Infra Availability (Availability of the infra components for at least 99.95% of the time, measured every month.)	Amendment in Cluase(Defination: Availability of the over all Infra Solution for at least 99.95% of the time, measured every month.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

89 7	Volume of the RFP II	General	Ticket Data	Please provide last 6 months incident, service request ticket data - severity and domain wise	Refer sheet "Additional details on applications"

Response to the Pre-Bid Queries

89 8	Volume of the RFP II	General	SLA Report	Please provide last 6 months SLA reports	The requested SLA reports are internal and confidential in nature and will not be shared. Bidders are expected to propose their solution and services in accordance with the SLA requirements specified in the RFP.

Response to the Pre-Bid Queries

89 9	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 9: Backup Scheduling : Multi-site scheduling with automated copy to NDC and replication to DR; Parallel job execution supported.	Request DoP to correct the understanding as " Primary Backup Copy of DC site to be replicated to NDC and DR Site as well " accordingly Backup Solution will be define.	Refer #883

Response to the Pre-Bid Queries

90 0	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 20: High Availability: Backup server clustering for DC and NDC; Failover capability so backups continue even if DC is unavailable.	Request DoP to correct the understanding as " The expectation is to define a backup server and storage architecture that is available at both the DC and NDC sites to back up DC site data."	Refer #884

Response to the Pre-Bid Queries

90 1	Volume of the RFP II	Annexure L – Page No 260 - Indicative Specifications for IT Infrastructure and Racks : Backup Solution	Sr. NO. 3: Backup Types: Tiered retention policies supporting: short-term backups at DC, operational copy at NDC, long-term archival at DR.	Request DoP to define the short-term, operational, and archival copy retention periods, along with the backup window and throughput requirements, to enable accurate backup storage sizing.	Refer #885

Response to the Pre-Bid Queries

90 2	Volume of the RFP II	Annexure A – Existing Infrastructure: Page no 211 : As-Is Storage Deployment Architecture: DC and DR	4. For the Backup Solution, the IBM TS 3500 Tape Library is being implemented	Request DoP to provide details of the existing backup solution, including backup software and its version, backup policies, backup storage at DC and DR sites, and the backup window, to help define the new architecture	Refer #886

Response to the Pre-Bid Queries

90 3	Volume of the RFP II	5.2.4.3 Integration, page no 89,Clause 11	11. The SI is required to deploy engineers from the OEM for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	We understand that the OEM will be responsible for the implementation of the newly proposed solution under this RFP, and the OEM will not be involved in migration activities.	Refer #893

Response to the Pre-Bid Queries

90 4	Volume of the RFP II	5.2 Track 2: Platform Modernization and Feature Development	5.2.1.1.2 Seating Space 2. The seating space should be provisioned with UPS and Generator backup power, comfort air conditioning, and telephone extensions for communication between the server cage area and the seating area. The cost should be provided per seat per annum by the SI and factored in the commercial bid.	1. We kindly request DoP to clarify the requirement for telephone extensions. 2. The Telecom connection subscriptions is to be procured by DoP - pls advise.. 3. Please confirm whether one telephone in the server hall and one telephone in the seating area is required.	The revised clause to be read as: The seating space shall be provisioned with basic connectivity to enable operational communication between the server cage area and the seating area, as per the RFP requirements. Provisioning of required telecom connectivity and associated arrangements for the seating space shall be in the SI's scope as part of the facility services. The RFP does not prescribe a fixed number of telephone instruments. Bidders are expected to propose an appropriate arrangement to meet the stated communication requirement.

Response to the Pre-Bid Queries

90 5	Volume of the RFP II	5.2 Track 2: Platform Modernization and Feature Development Pg53	5.2.1.1.2 Seating Space 3. Adequate locker facility should be provided in the seating area for the safekeeping of DoP records and stationery.	We request DoP to specify the number, 3 approved make, size and dimension requirement for the lockers.	As per RFP

Response to the Pre-Bid Queries

90 6	Volume of the RFP II	<u>5.2 Track 2: Platform Modernization and Feature Development Pg53</u>	5.2.1.1.2 Seating Space 4. Dedicated Fireproof storage Cabinets with a lock should be provided, preferably adjacent to the seating area/within the seating area.	We request DoP to confirm the preferred make and capacity / dimensions of the fireproof storage cabinets to be provided.	As per RFP

Response to the Pre-Bid Queries

90 7	Volume of the RFP II	<u>5.2 Track 2: Platform Modernization and Feature Development Pg53</u>	5.2.1.1.3 Physical Security Requirements The storage of CCTV feeds shall be as per the defined process and legal requirements for such critical infrastructure deployment. A basic requirement of a minimum of 90 calendar days of live and further 90 calendar days of archival storage should be considered for the areas where DoP infrastructure would be installed.	We shall provision : 90 calendar days of live feed shall be available at our servers and DoP shall provide appropriate storage device for further storing the 90 calendar days of archival in its own safe custody.	The revised clause to be read as: The storage of CCTV feeds shall be as per the defined process and legal requirements for such critical infrastructure deployment. A basic requirement of a minimum of 90 calendar days of live feed to be factored in by the SI.

Response to the Pre-Bid Queries

90 8	Volume of the RFP II	5.1 Track 1: Takeover and Transition Pg 28	5.1.2.5 Transition Activities and Deliverables	he SI is required to perform a validation and handover of software licenses for all in- scope applications during the transition phase (Track 1). In the event that existing licenses are found to be non-compliant or insufficient during this validation, will the cost of regularizing these legacy licenses be borne by the DoP or the SI?	The SI shall validate the licensing position of all in- scope applications and identify any non- compliance or gaps. In case regularization of legacy licenses is required, the SI shall submit its assessment and recommendations. Procurement of additional/regularized licenses, if approved, shall be undertaken by DoP, or through CR with implementation support from the SI.

Response to the Pre-Bid Queries

90 9	II	Section 6- Page 167,	b) Common: Support Service Levels	Please confirm on the service window by application category. Gold: 1) P1-24X7; 9am-5pm Mon-Fri in office, remianing on call 2) P2-24X7;9am-5pm Mon-Fri in office, remianing on call 3) P3- 9am-5pm Mon-Fri in office Silver: 1) P1-24X7; 9am-5pm Mon-Fri in office, remianing on call 2) P2, P3- 9am-5pm Mon-Fri in office Bronze: 1) P1, P2, P3: 9am-5pm Mon-Fri in office	As per RFP

Response to the Pre-Bid Queries

91 0	II	Section 6- Page 167,	b) Common: Support Service Levels	Sheet 2 has the list of in scope applications inventory to be supported by the selected vendor. Please confirm . Request following information against each (marked in green in sheet 2) 1) Application Category 2) Associated OEM vendor, Type of support provided by vendor (L1,L2,l3), SLAs signed by the vendor, Any other specific terms that we need to know 3) Please provide number of application tickets for last 1 year in terms of L1/L2/L3/L4/Service Requests. And the percentage of P1/P2 categories.	Refer sheet "Additional details on applications"

Response to the Pre-Bid Queries

91 1	II	Section 5.1.4, Page 31	5.1.4 Operations and Maintenance of Existing Applications	Please define minor enhancements. What should be the monthly capacity (hours/ month) to be considered for baselining	As per RFP

Response to the Pre-Bid Queries

91 2	II	5.2.1.1, Page 52	5.2.1.1 Facility Requirements	Please provide the work location from where team will be providing application support	Refer #232

Response to the Pre-Bid Queries

91 3	II	6.2, page 129	6.2 General Terms and Terminology	Please provide the application for which monitoring is getting provided today and how (existing tool)	Existing monitoring and operational support mechanisms are implemented through custom scripts, reports, schedulers, and batch jobs.

Response to the Pre-Bid Queries

91 4	II	Page 19, Table 4	Table 4	In RFP we have some applications like ATM Switch, DMS, PLI, Card Management System, NACH, IVR, GST, SFTP file utility, DOP digital signer etc. which are not included in the AMS section. Do we need to consider such applications for AMS support? Please provide the list of applications needs to be supported by AMS and Technology details.	As per RFP

Response to the Pre-Bid Queries

91 5	II	5.1.1, Page 21	5.1.1 Details of existing vendors	As per the RFP, Vendors where the Manpower contract will continue till 2028/2029 like Integra - 2029, Inspira - 2028. We understand that the ownership of these Vendors/ services and SLAs will remain with DOP till expiry of the current contract. Please confirm.	As per RFP

Response to the Pre-Bid Queries

91 6	II	5.1.1, Page 24	5.1.1 Details of existing vendors	As per the RFP, some of the OEM Vendors contracts will continue till 2028/2029 like Integra - 2029, Inspira - 2028. Please confirm what kind of OEM licences DOP has taken from the Vendors - Integra, Alstonia, Winjit For example Perpetual, subscription based, user based and the type of services provided (e.g. AMC, L3 etc.) We understand that the ownership of these Vendors and SLAs will remain with DOP till expiry of the current contract. Please confirm.	As per RFP

Response to the Pre-Bid Queries

91 7	II	5.2.5.2, Page 106	5.2.5.2 FINnet 2.0	How many reports are currently prepared for Finnet or similar, what is the frequency of these reports and run window . How many data sources are there? Please provide all the batch jobs running today and the service window, frequency of run for the same.	Finnet 2.0 automation is not implemented, raw data is extracted manually and frequency of extraction is monthly. · Cash Transaction Report (CTR) on Monthly Basis · Suspicious Transaction Report (STR) as and when any transaction found suspicious · Counterfeit Currency Report (CCR) on Monthly basis · Watchlist/PEP Reports · Sanction screening while onboarding of Customer. · Human Trafficking · Wildlife Trade

Response to the Pre-Bid Queries

91 8	II	Annexure D – Mobile Banking, 241	Annexure D – Mobile Banking	As per RFP, for Mobile Banking and PSP application the manpower to start from Feb 2027. Who is going to support before that and own the SLA?	SLA for existing Mobile Banking app to be owned by SI till go-live of new App. SLA for new MB App to be owned by Winjit till Jan 2027.

Response to the Pre-Bid Queries

91 9	II	5.1.1, Page 24	5.1.1 Details of existing vendors	Can we know the existing number of people supporting the applications?	As per RFP

Response to the Pre-Bid Queries

92 0	II	Annexure D – Mobile Banking, 241	Annexure D – Mobile Banking	It is stated that Mobile Banking 1.0.35 is UAT version. Please confirm if it is available in production and when.	The App is envisaged to be deployed in Production after procurement of required infra for MB by the selected bidder. The SI shall size, provision, configure, and maintain the required hardware infrastructure for hosting the revamped Mobile Banking Application across the environments for go-live activities and the following O&M phase. The infrastructure shall include compute, storage, and network components necessary to ensure high performance, scalability, and fault tolerance. The required hardware shall be provisioned at the existing DC to facilitate timely completion of the implementation of the revamped MB application.

Response to the Pre-Bid Queries

92 1	II	Annexure G - 3. Misc Activities, 256	3. Misc Activities	Please provide # & details of utilities to supported	As per RFP

Response to the Pre-Bid Queries

92 2	Volume II	AnnexureN-Appln Performance Monitoring-1	Solution should support automatic javascript injection for real user monitoring, by simple installation of Agent on the following web server technologies and should not require any manual changes in web pages or any configuration files : IBM HTTP Server, Java Servlet based web applications, ASP.Net core, Microsoft IIS, NGINX, Node.JS, Oracle HTTP SERVER, APACHE HTTP SERVER	We would like to seek clarification regarding the requirement for fully automatic JavaScript injection for real user monitoring (RUM) by simply installing an agent on various web server technologies—such as IBM HTTP Server, Java Servlet-based applications, ASP.Net Core, Microsoft IIS, NGINX, Node.js, Oracle HTTP Server, and Apache HTTP Server—without any manual changes to web pages or configuration files. In industry practice, this level of automation is highly OEM-specific and typically not supported natively by most observability platforms, including Elastic. Elastic's RUM solution requires a one-time manual insertion of the JavaScript agent into web pages or templates, which is a standard and widely accepted approach. We recommend that the RFP language remain open to solutions that support streamlined and well-documented RUM agent deployment, rather than mandating fully automated injection across all web server technologies, to ensure flexibility and compatibility with best-in-class observability platforms.	Refer #393

Response to the Pre-Bid Queries

92 3	Volume II	AnnexureN-AppIn Performance Monitoring-2	Solution should automatically discover all the deployed applications on a server or a virtual machine, and automatically enable the code level monitoring for all applications without any changes to the code or configuration files. It should not require manual placement of jar files, or any other libraries or files to enable monitoring.	The requirement for the solution to automatically discover all deployed applications on a server or virtual machine and enable code-level monitoring for all applications without any changes to code or configuration files, and without manual placement of agent libraries or files points to zero-touch instrumentation which is highly OEM-specific and typically not supported natively by most observability platforms, including Elastic. Elastic provides streamlined onboarding and automation tools—such as the Elastic APM agent attacher for Kubernetes and automated deployment scripts—to simplify agent installation and minimize manual steps. However, enabling deep code-level monitoring generally requires an initial agent deployment or minimal configuration, which is standard across leading observability solutions. We recommend that the RFP language remain open to solutions that support automated discovery and simplified agent deployment, rather than mandating fully native, zero-configuration code-level instrumentation, to ensure flexibility and access to best-in-class observability platforms.	Refer #394

Response to the Pre-Bid Queries

92 4	Volume II	AnnexureN-AppIn Performance Monitoring-8	Solution should support automated detection of new applications or microservices and enabled monitoring be default. In a monitored environment, if any new microservice or application service is deployed, solution should discover it automatically, enabled deep monitoring with code and query level insight and discover the dependence and relationships without any manual action or configuration change of any kind.	We request you to clarify regarding the requirement for fully automated detection and deep monitoring of new applications or microservices—specifically, the expectation that any newly deployed service is automatically discovered, instrumented for code- and query-level insights, and mapped for dependencies and relationships, all without any manual action or configuration change. In industry practice, such zero-touch, deep instrumentation is typically an OEM-specific capability, often requiring proprietary hooks or platform-specific integrations. Elastic provides robust automated discovery and default monitoring for new services at the infrastructure and log level, and offers tools to streamline application-level instrumentation—especially in orchestrated environments like Kubernetes. However, enabling comprehensive code-level and query-level monitoring for all new services generally requires an initial agent deployment or minimal configuration. We recommend that the RFP language remain open to solutions that support automated discovery and streamlined onboarding, rather than mandating fully native, zero-configuration	Refer #395

Response to the Pre-Bid Queries

				deep instrumentation, to ensure flexibility and access to best-in-class observability platforms.	

Response to the Pre-Bid Queries

92 5	Volume II	AnnexureN-Appln Performance Monitoring-10	Solution should support comprehensive monitoring of cloud services. It should support monitoring of all cloud managed services, baseline the metrics automatically and alert when cloud services behave abnormally. Additionally it should establish automatic cause and effect relationship between application service and cloud service for accurate root cause analysis.	We request clarification regarding the requirement for comprehensive monitoring of all cloud-managed services, including the automatic baselining of metrics, anomaly alerting, and the establishment of automatic cause-and-effect relationships between application and cloud services for root cause analysis. While Elastic offers extensive integrations for monitoring a wide range of cloud services and provides advanced machine learning features for automatic baselining and anomaly detection, it is important to note that fully automated root cause analysis—where the platform independently determines and presents definitive cause-and-effect relationships—is generally a specialized capability found in certain OEM or AIOps solutions. Elastic excels at correlating application and cloud service metrics, visualizing dependencies, and surfacing likely contributing factors, but we request that the RFP remain open to solutions that provide strong correlation and integration capabilities, rather than mandating native, fully automated root cause analysis. This approach ensures flexibility and allows organizations to leverage best-in-class	Refer #396

Response to the Pre-Bid Queries

				observability and analytics tools.	

Response to the Pre-Bid Queries

92 6	Volume II	AnnexureN-Appln Performance Monitoring-11	Solution should capture process crashes (JVM Crash, .NET crash or any other process). The provided crash details include the signal that killed the process (for example, Segmentation fault or Abort), the execution stack frame that crashed, and more. The crash type—such as a native core dump, Java core dump, or abnormal program exit due to an exception should be available.	The requirement for the solution to natively capture and analyze process crashes (such as JVM or .NET process terminations), including details like the signal that killed the process, execution stack frames, and crash type (e.g., native core dump, Java core dump, or abnormal program exit)., such deep crash diagnostics and core dump analysis are typically provided by specialized OEM tools or platform-specific profilers, rather than by general-purpose observability platforms. Elastic's observability suite can ingest and analyze crash-related logs and events from external sources, enabling centralized alerting, correlation, and visualization of crash incidents. We request that the RFP language remain open to solutions that support integration with leading crash analysis tools, rather than mandating native core dump or stack frame analysis, to ensure flexibility and leverage best-in-class capabilities for both observability and crash diagnostics.	Refer #397

Response to the Pre-Bid Queries

92 7	Volume II	AnnexureN-AppIn Performance Monitoring-14	Solution should support mobile app monitoring and crash analytics for mobile applications developed for iOS and Android frameworks (e.g. ReactNative, Flutter, Cordova or equivalent). It should offer analytics like Device types impacted by crash, OS version and app versions where crashes are observed, stacktrace of crash, and users impacted by crash.	We request for clarification on the requirement for native mobile app monitoring and crash analytics for iOS and Android frameworks (including React Native, Flutter, Cordova, or equivalent). In the observability industry, comprehensive crash analytics—such as automatic capture of device types, OS versions, app versions, stack traces, and user impact—are typically provided by specialized OEM solutions like Firebase Crashlytics, Sentry, or Bugsnag, rather than by general-purpose observability platforms. Elastic's observability suite offers robust backend and API monitoring, and can ingest and analyze crash data from third-party mobile analytics tools, enabling unified visualization and reporting. We recommend that the RFP language remain open to solutions that support integration with leading mobile crash analytics platforms, rather than mandating native SDK support, to ensure flexibility and access to best-in-class capabilities for both mobile and backend monitoring.	Refer #401

Response to the Pre-Bid Queries

92 8	Volume II	AnnexureN-AppIn Performance Monitoring-18	CPU Overhead of the monitoring agent should be less than 3%. To maintain this, solution should not toggle sampling rate and should be able to offer highest data capture rates. Solution should not revert to high sampling for maintaining overhead	Regarding the requirement that the monitoring agent's CPU overhead must remain below 3% at all times, without toggling sampling rates and while maintaining the highest data capture rates. In the observability industry, it is common for leading solutions to provide configurable sampling options, allowing customers to balance data fidelity with resource consumption based on their unique workloads and environments. Agents are engineered for low overhead and can be configured for full data capture (100% sampling) while typically maintaining CPU usage well below 3%. However, it is important to note that the ability to guarantee fixed, ultra-low overhead at the highest data capture rates—without any adaptive sampling or data throttling—is highly OEM-specific and may not reflect standard industry practice. We recommend that the RFP language allow for solutions that offer transparent, configurable sampling and resource controls, ensuring both performance and flexibility, rather than mandating a fixed approach that could limit the range of best-in-class observability offerings.	Refer #402

Response to the Pre-Bid Queries

92 9	Volume II	AnnexureN-Appln Performance Monitoring-20	Solution should offer a common agent both for applications and Server Infrastructure monitoring (including VM/Containers/Kubernetes/EC 2 etc). This would help the operations team to minimize administrative overhead of managing multiple agents, and also ensure that infrastructure and application services dependencies are automatically discovered and mapped.	Please Clarify the requirement for a "common agent" that supports both application and server infrastructure monitoring (including VMs, containers, Kubernetes, EC2, etc.) within a single binary. In the observability industry, it is standard practice for leading platforms—including Elastic—to provide specialized agents: Elastic Agent for infrastructure and cloud resource monitoring, and language-specific APM agents for deep application instrumentation. This approach ensures optimal performance, security, and flexibility for diverse technology stacks. Elastic's tightly integrated agents work seamlessly together to provide unified visibility, automatic discovery, and dependency mapping across both infrastructure and application layers, while minimizing administrative overhead. We request that the RFP language remain open to solutions that deliver unified observability through integrated agents, rather than mandating a single OEM agent, to ensure the best fit for modern, heterogeneous environments and to leverage the strengths of best-in-class monitoring technologies.	Refer #403

Response to the Pre-Bid Queries

93 0	Volume II	AnnexureN-Appln Performance Monitoring-21	Solution should capture and replay the user interactions like a movie. This would help the teams to understand and reproduce UI related usability issues and frustration points present in the application interface and help them teams to improve overall usability. The video capture should be anonymized to protect user privacy	We would like to seek clarification regarding the requirement for the solution to "capture and replay user interactions like a movie," enabling teams to visually reproduce UI-related usability issues and frustration points. While this feature is highly valuable for usability analysis, it is important to note that such session replay capabilities—where user interactions are recorded and replayed as a video—are typically provided by specialized OEM solutions (e.g., FullStory, Glassbox) rather than core analytics or observability platforms. Elastic's observability suite offers comprehensive real-time analytics, user journey tracking, and anomaly detection across web and mobile applications, and can be seamlessly integrated with leading session replay tools to deliver a unified experience. We request that the RFP language remains open to solutions that provide native or integrated support for session replay, rather than mandating this as a core specific OEM feature, to ensure the broadest and most flexible range of offerings and to leverage best-of-breed capabilities in both observability and session replay domains.	Refer #404

Response to the Pre-Bid Queries

93 1	II	5.2.4.8 Security Requirements / Page # 96	General Query	Please confirm if bidder can use cloud-delivered / SaaS based security controls, as per specifications mentioned in the RFP	All solutions shall be deployed on-premise within India unless explicitly stated otherwise. The proposed solution must comply with data localization requirements, and no data shall be stored, processed, or shared outside India. The Successful Bidder shall not share any data, including customer data, with any third party without prior approval of DoP and shall comply with the Digital Personal Data Protection Act, 2023 (DPDP Act), and amendments thereto.

Response to the Pre-Bid Queries

93 2	II	5.1.1 Details of existing vendors / Page # 24	General Query	Bidder understanding is that Existing AMC / licensing / product support would be owned & provided by DOP - for first 11 months (IT 1.0) of this program. Please confirm	Bidder to analyze the information given on existing landscape and propose accordingly.

Response to the Pre-Bid Queries

93 3	II	5.2.3.2 Integrated IT Security layer & (b) Infrastructure Security (Host & End Point)) / Page # 79 & 5.2.4.8.1 Security Requirement Page # 96	Various security tools and techniques are to be utilized in POSB IT systems cutting across all business applications and would include but not limited to SSO, IAM, ATP, DLP, PAM, Anti-Virus, Syslog, DAM, SIEM, UEBA, SSL Certificates, TLS encryption, Unified Threat Intelligence, Two Factor Authentication etc. b) Infrastructure Security (Host & End Point) c) Data Security & Endpoint Security : For Endpoint Security, the requirement is to provide granular visibility and control over all connected devices to prevent breaches at the edge. Additionally, the solution must incorporate Data Security Posture Management to continuously assess and enforce security configurations, ensuring that endpoint vulnerabilities are identified and mitigated proactively.	Bidder understanding is security controls required for endpoint (DOP employee/contractors - laptop/desktop) will be provisioned & managed by DOP, except DLP, secured Internet access, secured browser. Please confirm the understanding	As per RFP

Response to the Pre-Bid Queries

93 4	II	Annexure B – Common Infra and Security solutions maintained by HPE (page #225)	Average EPS utilisation of RSA ranges between 15K	Please confirm the Sizing of Existing SIEM & SOAR, ie. Total EPS, Number of devices integrated, Number of Correlation Rule, Number of Play book in SOAR.	SIEM SOAR to be implemented at new DCF for POSB as per the requirements given in the RFP/ Corrigendum.

Response to the Pre-Bid Queries

93 5	II	5.2.3.2 Integrated IT Security layer / Page # 79	Various security tools and techniques are to be utilized in POSB IT systems cutting across all business applications and would include but not limited to SSO, IAM, ATP, DLP, PAM, Anti-Virus, Syslog, DAM, SIEM, UEBA, SSL Certificates, TLS encryption, Unified Threat Intelligence, Two Factor Authentication etc.	Please mention number Of public SSL Certificate presently operational for in-scope applications for this program	Currently, a single public wildcard SSL certificate (*.indiapost.gov.in) is used for EB, MB, and NEFT services

Response to the Pre-Bid Queries

93 6	Volume II Annexure N	Secured Internet Access / DLP	Web Protection Security	The RFP - Annexure N seeks compliance with "Secured Internet Access" as well as "Web Protection Security" controls - which seem to be serving the same purpose. Does DOP intend to have both controls in the IT 2.0 platform ? Kindly elaborate the purpose	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

93 7	Volume II	Annexure B – Common Infra and Security solutions maintained by HPE (page #229)	2FA Tokens (Hardware)	RFP intends the SI to provide IDAM solution to support integration with existing 2FA hardware tokens. These tokens are EOSL in Jan-24. Please confirm if intends to continue using these 2FA hardware tokens in IT2.0. If so - please mention OEM / make / firmware details of these hardware tokens	As per RFP

Response to the Pre-Bid Queries

93 8	II	5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	DoP has an existing contract with M/s Integra Micro Solutions for the Maintenance of Aadhaar-compliant eKYC and Data Vault, valid until November 2029.) Page # 42,	We have not found HSM compliance in RFP, please elaborate existing HSM solution, TPS & future requirements (if any)	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

93 9	II	5.2.4.8.1 Security Requirement Page 94	The SI is required to provide a collaborative SOC team for mitigating potential security threats. The SI is required to provide below product stack to run SOC:	What are the existing solution/size/license. Our understanding, these solution as part of this RFP is New ? a. DAM solution b. DNS Security c. SOAR operational Status, Solution d. Threat Intel Solution e. NTA solution f. EndPoint DLP g. SandBox h. Link Load Balancers i. WAF j. Decoy-based Threat Detection k. SSL Certificate l. Remote Access Solution / SSE m. Attack Surface Management	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

94 0	II Annexure N	Security and Threat Management, (14)	The proposed solution should be complied with ISO27K and SOC 2 TYPE II compliance adherence.	"We understand the importance of compliance standard SOC 2 TYPE II, which are key indicator of strong security controls and operational assurance. Our organization holds ISO 9001 and ISO 27001 certifications, reflecting our strong commitment to quality and information security - core pillars in delivering effective cybersecurity solutions. We assure you that our solution adheres to high standards of quality and security, and we remain committed to continuous improvement and alignment with global best practices. SOC 2 Type-2 would be required for SIEM, incase of Cloud-delivered solution. Would the same be applicable for on-premises solution ? By considering this we kindly request that the clause be amended to allow participation from companies that demonstrate robust security practices and hold internationally recognized certifications, such as ISO 27001."	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

94 1	Volume II Annexure N	Security and Threat Management, (14)	The solution should have source code available for review for automations, playbooks, integrations	Since majority of OEM's has developed the platform from scratch. Kindly requesting you to remove the clause completely, as the Source code belongs to Individual OEMs and developers	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

94 2	Volume II Annexure N	Security and Threat Management, Network Traffic Analysis (NTA) (2)	The proposed NDR should have centralized sandboxing component and sandboxing should be done on the MeitY compliant cloud hosted in India.	This requirement appears to be from a proprietary OEM specification. We kindly recommend removing this clause from the RFP.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

94 3	Volume II Technical Specification s	Volume II Page 96	The SI is required to provide a collaborative SOC team for mitigating potential security threats. The SI is required to provide below product stack to run SOC: 1. Data & Database Activity Monitoring 2. Multi Factor Authentication (MFA) & Single Sign On (SSO) 3. Identity and Access Management (IDAM) 4. Domain Name System (DNS) 5. Secured Internet Access 6. Security Information and Event Management (SIEM) 7. User and Entity Behaviour analysis (UEBA), 8. Security Orchestration, Automation and Response (SOAR), 9. Threat Intel Management (TI) 10. Network Traffic Analysis (NTA) 11. Application Performance Monitoring 12. Next-Gen Firewall 13. Data Loss Protection (DLP) 14. Distributed Denial of Service (DDoS) 15. Host based Intrusion Prevention System (HIPS) 16. Network Intrusion Prevention System (NIPS) 17. Privileged Identity Management (PIM) 18. Privileged Access Management (PAM) 19. Sandbox 20. Link Load Balancer (LLB) 21. Server Load Balancer (SLB) 22. Web Application Firewall	Justifications : We have observed a discrepancy in the tender documents. Annexure N specifically outlines requirements for a 'Secure Browser,' yet this component is missing from the main Scope of Work (SOW) and Bill of Material (BoM). To ensure alignment and avoid ambiguity, we request that the DOP incorporate the 'Secure Browser' into the primary SOW and BoM as a mandatory line item. Conversely, regarding the 'Decoy-based Threat Detection' & "PAM" requirement, we note that the current specifications are proprietary to a single OEM. To ensure wider participation and fair competition, we respectfully request the removal of this specific section, as the intended security outcomes are effectively achieved through standard PIM Endpoint Protection and SOC integrations. Change Request : The SI is required to provide a collaborative SOC team for mitigating potential security threats. The SI is required to provide below product stack to run SOC: 1. Data & Database Activity Monitoring 2. Multi Factor Authentication (MFA) &	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

			(WAF) 23. Attack Surface Management (ASM) 24. Decoy-based Threat Detection	Single Sign On (SSO) 3. Identity and Access Management (IDAM) 4. Domain Name System (DNS) 5. Secured Internet Access 6. Security Information and Event Management (SIEM) 7. User and Entity Behaviour analysis (UEBA), 8. Security Orchestration, Automation and Response (SOAR), 9. Threat Intel Management (TI) 10. Network Traffic Analysis (NTA) 11. Application Performance Monitoring 12. Next-Gen Firewall 13. Data Loss Protection (DLP) 14. Distributed Denial of Service (DDoS) 15. Host based Intrusion Prevention System (HIPS) 16. Network Intrusion Prevention System (NIPS) 17. Privileged Identity Management (PIM) 18. Privileged Access Management (PAM) 19. Sandbox 20. Link Load Balancer (LLB) 21. Server Load Balancer (SLB) 22. Web Application Firewall (WAF) 23. Attack Surface Management (ASM) 24. Secure Browser	

Response to the Pre-Bid Queries

94 4	Volume II Technical Specifications BOQ_937457.xls	Page 96, Volume II Technical Specifications BOQ_937457.xls	Clarification :	Problem Statement : We have thoroughly reviewed the RFP, Scope of Work, and the provided Bill of Quantity file (BOQ_937457.xls). We observe that none of the mandatory security components described in the Technical Scope are captured in the commercial BOQ. Recommendations : To ensure transparency and accurate commercial bidding, we respectfully request that the Authority update the BOQ to include these line items, providing specific sizing and quantity details for the DC, DR, and NDR locations for each component.	Refer #430

Response to the Pre-Bid Queries

94 5	Volume II Scope of Work	Page 89 5.2.4.3 Integration, Clause No. 11	The SI is required to deploy engineers from the OEM for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	Operation Challenger Change Request : To ensure the successful and holistic execution of this project, the System Integrator (SI) must retain primary ownership of the overall solution design and delivery. While we will strictly adhere to OEM best practices, we respectfully request that the mandatory requirement for direct 'OEM Professional Services' be modified to accept 'OEM Certified Engineers' deployed by the SI. The responsibility for end-to-end integration, project management, and cross-component execution should remain with the SI's dedicated Project Manager. Engaging multiple OEM service teams creates a 'project within a project,' adding significant coordination overhead and complexity. By utilizing OEM-certified SI resources, the Department ensures a clear chain of command, cost-efficiency, and a single point of accountability for the entire ecosystem. Hence we proposed to update the clause : The SI is required to deploy manpower from the OEM or OEM certified engineer for the installation and maintenance of the proposed hardware and software at DC, DR, and	Refer #431

Response to the Pre-Bid Queries

				NDC. Furthermore, the bidder must guarantee the continuous availability of the implementation team until the installation and commissioning of the equipment/software are completed and receive sign-off from DoP.	

Response to the Pre-Bid Queries

94 6	Volume II Technical Specification s	Volume II Scope of Work	Recommendations	With the dynamic security landscape and the rise of sophisticated AI-based threat vectors, protecting the network pipe via Secure Internet Access is important but not sufficient for critical POSB applications layer. Attacks increasingly occur at the presentation layer (where data is rendered for the user), bypassing traditional network-level inspection. While the RFP currently mandates Secure Internet Access, we respectfully request that the scope be enhanced to include 'Secure Browser' to creates a secure workspace for accessing applications (SaaS, web apps, private apps) . This will ensure Last-Mile Data Protection—specifically enforcing granular controls such as clipboard restrictions, anti-screen capture, and watermarking directly within the application session. This approach effectively extends Zero Trust controls from the network down to the user interface, preventing AI-driven data scraping and exfiltration at the point of access.	As per RFP

Response to the Pre-Bid Queries

94 7	Volume II Technical Specification s	Scope of Work	Recommendations	Risk Management & Problem Statement : Relaying on a single OEM for both connectivity and security creates a significant Single Point of Failure—a critical vulnerability where a supply chain attack or software bug could compromise the entire infrastructure simultaneously. Recommendations : Consistent with standard practices in various large-scale Indian government projects, we request that the Network and Security components be decoupled. Mandating different OEMs for these layers ensures a heterogeneous environment, providing a necessary fail-safe and ensuring that the organization benefits from the widest spectrum of specialized technologies	As per RFP

Response to the Pre-Bid Queries

94 8	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Secure Internet Access" SN. 5	There are known or documented "restrictive clause" in decoy-based threat detection technology that restricts OEM from participating in secure internet access	There are known or documented "restrictive clause" in decoy-based threat detection technology that restricts OEM from participating in secure internet access	As per RFP

Response to the Pre-Bid Queries

94 9	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Secure Internet Access" SN. 5	Clarification : Kindly confirm number of user / number of license for Secure Internet Access	Clarification : We have thoroughly reviewed the specifications and Scope of Work but are unable to locate the specific sizing requirements. Could you kindly confirm the total number of users or licenses required for the Secure Internet Access solution?"	Refer #432

Response to the Pre-Bid Queries

95 0	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM" SN. 1	Solution must provide capabilities of SIEM, SOAR, NTA, TIP, Threat hunting, AI/ML Analytics and UEBA OOTB within a single unified frontend and datalake solution.	Clarification : We understand that the proposed solution is required to provide a single, unified management dashboard for the operation of all specified modules, including SIEM, SOAR, NTA, TIP, Threat Hunting, AI/ML Analytics, and UEBA.	Refer #433

Response to the Pre-Bid Queries

95 1	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM" Security Information and Event Management (SIEM) SN. 4	The proposed solution should support min 800+ OOB integration with 3rd party solutions and OOB Parser availability.	Problem Statement : Considering large numbers of exiting OEM and proposed OEM, the number of integrations specified in the RFP seems insufficient. Having more integrations would provide flexibility for the DOP to adopt new products and services. Therefore, we request to update the clause to specify that the solution should have at least 1000+ out-of-the-box integration. Change Request : The proposed solution should support min 1000+ OOB integration with 3rd party solutions and OOB Parser availability.	Refer #125

Response to the Pre-Bid Queries

95 2	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM" Security Orchestration, Automation and Response (SOAR) SN. 6	The solution should support 800+ out of the box playbooks. The playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case. - conditional decision trees - User surveys for input from various stake holders in the usecase/reviews - time based actions - escalation actions	Problem Statement : Considering large numbers of exiting OEM and proposed OEM, the number of integrations specified in the RFP seems insufficient. It is foresee that the DOP and SI team is spending months to manually create a playbook for automation. Therefore, we request to update the clause to specify that the solution should have at least 1000+ out-of-the-box playbooks. Change Request : Requesting to update the clause : The solution should support 1000+ out of the box playbooks. The playbooks should support: - nested playbooks to deploy multiple automations as part of a single use case. - conditional decision trees - User surveys for input from various stake holders in the usecase/reviews - time based actions - escalation actions	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

95 3	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM" Threat Intel Management (TIM)) SN. 27	The solution should have 800+ prebuilt playbook with customization option	Problem Statement : Considering large numbers of exiting OEM and proposed OEM, the number of integrations specified in the RFP seems insufficient. It is foresee that the DOP and SI team is spending months to manually create a playbook for automation. Therefore, we request to update the clause to specify that the solution should have at least 1000+ out-of-the-box playbooks. Change Request : The solution should have 1000+ prebuilt playbook with customization option	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

95 4	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM" Network Traffic Analysis (NTA) SN. 3	The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the NPCL's environment. Integration to be ensured by the bidder.	Justification : We note that there appears to be a typographical error in this requirement. We respectfully request that the specification be updated to reflect the intended meaning. Change Request : The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the POSB's environment. Integration to be ensured by the bidder.	Refer #434

Response to the Pre-Bid Queries

95 5	Volume II Technical Specification s	Page 96, Volume II AnnexureN "SIEM"	Clarification	We have reviewed the specifications and Scope of Work but observe that the SIEM sizing requirement (in GB/day) is missing. Kindly confirm the exact daily data volume to allow for an accurate proposal.	As per RFP

Response to the Pre-Bid Queries

956	Volume II Technical Specifications	Page 96, Volume II AnnexureN "External NGFW" SN. 24	NGFW solution support with 15 or higher Virtual Firewall instances from day 1 and expandable up to 50 with license.	Justification : Considering that the Department of Post (DOP) currently operates with fewer than 10 departments, the requirement for 15 virtual firewalls (scalable up to 50) appears disproportionate to the actual infrastructure needs. To ensure cost-efficiency and maximize vendor participation, we respectfully request that the quantity be rationalized to 10 virtual firewalls from Day 1, with scalability up to 20. This revision would better align the specifications with the actual organizational scope Change Request : NGFW solution support with 10 or higher Virtual Firewall instances from day 1 and expandable up to 20 with license.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

95 7	Volume II Technical Specification s	Page 96, Volume II AnnexureN "External NGFW"	Clarification : Kindly confirm quantity of firewall in DC, DR and NDR	Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for firewalls at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	Refer #436

Response to the Pre-Bid Queries

95 8	Volume II Technical Specification s	Page 96, Volume II AnnexureN "NIPS"	Clarification : Kindly confirm quantity of NIPS in DC, DR and NDR	Clarification : After a thorough review of the specifications and Scope of Work, we note that the specific quantity requirements for NIPS at the DC, DR, and NDR locations are not defined. Kindly confirm the exact number of appliances required for each location to ensure accurate sizing and proposal submission.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

959	Volume II Technical Specifications	Page 96, Volume II AnnexureN "Attack Surface Mgmt"	Clarification : Kindly confirm number IP to be scanned	Clarification : We note that the specific volume for Attack Surface Management is not defined in the scope. Kindly confirm the total number of public IP addresses that require scanning	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

96 0	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Attack Surface Mgmt"	Recommendations	Recommendations : We recognize that this is a prestigious project for the Department of Post (DOP) and POSB, requiring highly robust and compliant solutions. However, we note that the current specifications for 'Attack Surface Management' do not define specific OEM eligibility criteria or data regulatory guidelines (such as data localization or MeitY-empaneled Data Center requirements). To ensure full compliance with Indian banking and data sovereignty standards, we respectfully request that the authority incorporate specific OEM selection criteria and data residency guidelines into the tender > The OEM must be a registered legal entity in India > The proposed OEM should have own support center in India > OEM must be in security bussiness for last 20 years gobally > OEM must be in security bussiness for last 10 years in India > OEM must be public listed company > The proposed solution must be hosted in MIETY empanelled data center > OEM should be ISO certificates ISO 27701, ISO	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

				27032, ISO 27018, ISO 27017, ISO 27001 > OEM Should have SOC 2 or SOC 3 type cerficate > Data Residency - OEM should have an India Data Center for the proposed solution	

Response to the Pre-Bid Queries

96 1	Volume II Technical Specification s	Page 96, Annexure N, Tab "IDAM", Clause No. 11	Solution should be able to automate authentication token enrollment while a user joins in to organization.	Restrictive (OEM Baised) : Request to remove this clause.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 2	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 1	The proposed SSE endpoint software agent deployed on user devices for secure internet and private application access should have the capability to support decoy based threat from the same agent or solution.	Request to Remove (VENDOR-SPECIFIC): The RFP currently mandates a unified solution for both "Secure Internet Access" and "Decoy/Lure-based Threat Detection." Technical Justification: According to industry standards (e.g., Gartner/Forrester), Secure Service Edge (SSE) and Deception Technology are treated as distinct architectural categories. Bundling these niche capabilities limits the solution to a proprietary feature set of a single OEM, rather than allowing for "Best of Breed" technologies. This creates a vendor lock-in scenario that excludes the majority of market-leading Secure Internet Access providers. Request: We request the removal of the Deception/Decoy-based parameters from this section to align with standard market capabilities and ensure a competitive bidding process.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 3	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 2	The solution must have the ability to embed lures on real critical endpoints in the form of unique dummy credentials that lead attackers on to decoy systems to detect privilege escalation and lateral movement	Request to Remove (VENDOR-SPECIFIC): We respectfully submit that modern Endpoint Security solutions, when integrated with SIEM and SOAR, achieve the functional equivalent of standalone 'Decoy-based Threat Detection.' By leveraging high-confidence alerts and TTP analysis, these integrated systems effectively disrupt sophisticated threats—such as ransomware—without requiring a separate digital maze or lure infrastructure. Currently, the specification for 'Decoy-based Threat Detection' combined with 'Secure Internet Access' restricts compliance to a single OEM, thereby limiting fair competition. To ensure a vendor-neutral evaluation and maximize participation, we request the removal of the specific 'Decoy-based Threat Detection' mandate, allowing for broader functional equivalency.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 4	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 3	The solution must have the ability to visually replay past events on an interactive fluid dashboard that show all decoy elements and attacker details.	Request to Remove (VENDOR-SPECIFIC): The requirement for a "visual replay" on a "fluid dashboard" utilizes marketing terminology specific to a single OEM's proprietary interface. 1. The security objective of understanding an attack's history is effectively achieved through Forensic Timeline Reconstruction provided by modern Endpoint Detection & Response (EDR) and SIEM platforms. 2. Storing data for high- fidelity visual replays creates significant unnecessary storage overhead. Standard forensic logging (JSON/Syslog) used by EDR/SIEM is far more efficient, searchable, and scalable for retaining historical attack data over long periods. Request: We request the removal of the Deception/Decoy-based parameters from this section to align with standard market capabilities and ensure a competitive bidding process.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 5	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 4	Solution must allow visual dissection of the PCAP (packet capture) traffic and preserve all network traffic to and from the decoys while having the ability to export PCAPs based on a time filter.	(VENDOR-SPECIFIC) (Duplicate solution): Legacy & Inefficient: Mandating full packet capture (PCAP) storage for all events is a legacy approach that creates massive, unnecessary storage overhead. Restrictive: The requirement for "visual dissection" inside the dashboard describes a specific proprietary feature of a single vendor, restricting fair competition. Equivalent: Industry- standard EDR and SIEM solutions utilize Network Flow Logs and Process- Network Telemetry (metadata). This provides actionable forensic detail (Source, Destination, Port, Protocol, Process ID) without the resource burden of preserving full payload traffic.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 6	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 5	Solution must use a numeric risk score for each attacker based on dynamic analysis of attacker behaviour. Solution should not just use basic critical / high / medium / low buckets.	Restrictive Specification (VENDOR-SPECIFIC BIAS Duplicate solution) : Mandating a proprietary "numeric scoring" algorithm limits competition to vendors using that specific methodology. Equivalent: Risk scoring is most effectively handled by SIEM / UEBA platforms that analyze the entire attack surface, not just decoy interactions. Standard severity buckets (Critical/High/Medium) mapped to MITRE ATT&CK are the industry standard for interoperability.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 7	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 6	Decoy services like SSH, HTTP / HTTPS, FTP, SMB, MySQL, telnet should be individually unique services and not just a few VMs offering the same service on multiple IP addresses	Restrictive Specification (VENDOR-SPECIFIC BIAS Duplicate solution) : Inefficient Architecture: This clause dictates a specific, resource-intensive architecture (requiring unique service instances or 1:1 virtualization) rather than focusing on the security outcome.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 8	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 7	The solution should have automatic backup/restore of events and configuration data, with no manual intervention required from the customer.	Restrictive Specification (VENDOR-SPECIFIC) : While automation is positive, the phrase "no manual intervention" implies a strict SaaS-only "black box" architecture, excluding robust on-premise or hybrid solutions that may integrate with an enterprise's existing backup strategies (like snapshots or NAS targets).	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

96 9	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 8	The solution must have the ability to reconstruct raw attack data into plain English attack analysis. It must also provide attacker / APT group attribution, mitigation recommendations, MITRE mapping within the user interface for the analyst.	Restrictive Specification Vendor Lock-In (VENDOR- SPECIFIC) : The requirement for "Plain English" analysis and specific APT attribution inside the decoy UI describes the specific feature set of one OEM (Smokescreen). Operational Fragmentation: Threat Intelligence and attribution should be centralized in the SIEM/SOAR layer to correlate with all security events, rather than siloed within a specific decoy product's dashboard.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

970	Volume II Technical Specifications	Page 96, Volume II AnnexureN "Decoy-based Threat Detection" SN. 9	The solution should have a central management console to manage the deployment and event notifications. All other components should be controlled and configured through the central management console only.	Restrictive Specification Anti-Competitive (VENDOR-SPECIFIC): This "single pane of glass" requirement prevents the use of modular, best-of-breed architectures where sensors or agents might be managed via standard enterprise IT tools (e.g., SCCM, Intune, or MDM) or via API integrations. It enforces a monolithic proprietary ecosystem.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 1	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 10	The endpoint agent should be able to deploy custom endpoint decoys on different types of end-users. For this, the solution should be able to identify different types of users (finance/IT/Government/HR/ etc.)	Restrictive Specification Redundant & Intrusive (VENDOR-SPECIFIC): Categorizing users and deploying policy-based controls is a core function of EDR/EPP and Identity solutions. Duplicating this functionality in a decoy agent adds unnecessary complexity and agent bloat. Functional Equivalent: EDR solutions already protect specific user groups (e.g., Finance) with stricter policies and canary files without needing a separate decoy configuration.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

97 2	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 11	The solution should be capable of creating decoy processes on the endpoint with custom name and path.	Restrictive Specification Stability Risk (VENDOR- SPECIFIC): Injecting fake "decoy processes" into production endpoints introduces performance overhead and stability risks. Modern endpoint security relies on Behavioral Analysis to detect when real processes are abused (e.g., Process Injection), rather than confusing attackers with fake processes, which is a legacy technique.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 3	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 12	The platform must be capable of creating file decoys that are deployed on real systems and trigger alerts not only when opened but also when copied, modified and deleted	Functional Equivalent (VENDOR-SPECIFIC): This capability is identical to the Ransomware Protection / Canary Files feature standard in almost all modern EDR/EPP platforms. Request: We request this clause be removed as it mandates a redundant feature that is already covered by the organization's existing Endpoint Protection suite.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 4	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 13	The solution should have the ability to capture commands executed for hi-interaction SSH connections on Linux decoys without any instrumentation processes or agents running within the decoys.	Restrictive Specification (VENDOR-SPECIFIC): This requirement mandates a specific "agentless" architectural approach unique to niche honeypot vendors. Functional Equivalent: Modern security relies on Endpoint Detection & Response (EDR) agents on real assets. EDR provides superior, kernel-level visibility into command execution (bash history, process trees) across the entire estate, rather than just on limited decoy nodes.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 5	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 14	The solution should be able to deploy built in application decoys that look like webmail portals, vpn login portals, network printer, PIM login, HRMS etc.	Restrictive Specification (VENDOR-SPECIFIC): Creating fake "login portals" is a highly specific deception technique that adds operational complexity. Access to real Webmail and VPN portals should be secured via Secure Service Edge (SSE) and Identity Access Management (MFA/SSO). Detecting failed logins on real portals via SIEM is more effective than waiting for an attacker to find a fake one.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 6	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 15	Decoy web-applications should include the ability to easily upload templates for high- interaction (login / browsing of the decoy application).	Operational Overhead (VENDOR-SPECIFIC): Customizing fake web templates is resource- intensive and offers diminishing returns. Alternative: Standard Web Application Firewalls (WAF) and Vulnerability Scanners are the industry standard for protecting web assets. This clause excludes vendors focusing on prevention and detection over manual deception configuration	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 7	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 16	All Windows high interaction activity should be logged, not just code execution attempts. High-interaction should not involve transfer of malicious code to a separate analysis VM, but should provide full interactive access to the attacker.	Restrictive & Security Risk (To be removed) : Mandating "full interactive access" without sandboxing (transfer to analysis VM) runs the risk of giving attackers a pivot point. Restrictive: This specifically excludes vendors who use safe Sandboxing technologies to detonate threats. We request acceptance of "Safe Detonation / Sandboxing" as a valid method for high- interaction analysis.	Refer #439

Response to the Pre-Bid Queries

978	Volume II Technical Specifications	Page 96, Volume II AnnexureN "Decoy-based Threat Detection" SN. 17	Solution should include high-interaction Windows decoys that are accessible over the following channels: WMI, RDP etc.	Restrictive & Functional Equivalent (To be removed): Attacks utilizing WMI and RDP (like Lateral Movement) are best detected by EDR (Behavioral Analysis) and Identity Threat Detection (ITDR) on production systems. Dedicated decoys for these protocols are redundant when the real environment is properly monitored.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

97 9	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 18	The solution should have the ability to record the screen in a video (NOT screenshots) and must also capture keystrokes and mouse movements for hi-interaction remote desktop connections on Windows decoys and provide a downloadable video replay with keystroke capture of the attacker's activity in the decoy.	Proprietary & Privacy Risk (VENDOR-SPECIFIC): "Video replay" is a marketing feature specific to a single OEM (Smokescreen). It introduces significant storage overhead and data privacy/compliance liabilities (recording user sessions). Standard Equivalent: EDR Process Timelines provide a searchable, text-based audit trail of every command and keystroke (metadata), which is the industry standard for forensic validity.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

980	Volume II Technical Specifications	Page 96, Volume II AnnexureN "Decoy-based Threat Detection" SN. 19	Solution should have the ability to create specialised Internet facing decoys to detect external reconnaissance of Internet facing websites. These decoys should only respond to requests on HTTP/HTTPS and only for their requests to the configured domain names. The Internet facing decoys should consume backscatter threat intelligence from platforms like MISP, Greynoise, Shodan etc.	Restrictive & Functional Equivalent (To be removed): Better Approach: External reconnaissance is safely detected using Threat Intelligence Feeds (MISP, etc.) integrated into the Firewall/SSE logs, without needing to host and manage public-facing honeypots.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

98 1	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 20	The solution must support deep protocol inspection of network traffic such as DCE/RPC for detection of exploits.	Redundancy: Deep Packet Inspection (DPI) for protocols like DCE/RPC is the primary function of Network Detection & Response (NDR) or IPS, not an endpoint decoy solution. Request: Remove this clause as it duplicates capabilities already present in the network security stack.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

98 2	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Decoy- based Threat Detection" SN. 21	For authenticity, Linux high- interaction decoys should be one-to-one (the solution should not re-use of a few internal VMs configured with multiple IPs to show multiple decoys).	Restrictive & Functional Equivalent (To be removed): This mandates a "Heavy Honeypot" architecture requiring significant compute resources (1 VM per decoy). Restrictive: It explicitly excludes modern, cloud- native vendors who use Containerization or Emulation to provide high- fidelity decoys at a fraction of the hardware cost.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

98 3	Volume II Technical Specification s	Page 96, Volume II AnnexureN "Secure Browser" SN. 5	Clarification : The proposed solution must be licensed to support all specified features from Day 1 for a total of 5000 users.	Clarification : Please clarify the Day 1 licensing requirement for the Secure Browser. Is the initial scope fixed at 5,000 users, or is there a phased deployment schedule?	The referenced solution/component is not part of the scope as per the finalized solution architecture of the RFP.

Response to the Pre-Bid Queries

98 4	Volume II Technical Specification s	Page 96, Annexure N PIM and PAM	Duplication and Vendor specific specification for PAM	Recommendations : We have reviewed the technical specifications for Privileged Identity Management (PIM) and Privileged Access Management (PAM). We observe that the PIM specifications already comprehensively cover the functional requirements for securing privileged access (credential vaulting, session management, and rotation). However, the separate PAM TAB appears to contain redundant and OEM-specific proprietary clauses (e.g., specific workflow terminology) that restrict fair competition. To ensure a vendor-neutral evaluation and avoid functional duplication, we respectfully request that the Authority remove the separate PAM TAB entirely. We recommend evaluating the solution based on a single, unified 'Privileged Access Management' set of requirements (as already defined in the PIM section) that aligns with industry-standard open protocols	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

98 5	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 26	The proposed solution must support the below listed workflows. Justification for Access (user must submit a reason/comment before accessing) Access Approval (single and/or multi-tiered). Just-in-Time Administration Secret Erase Workflow	Restrictive (OEM Baised) : The requirement for a 'Secret Erase Workflow' appears to utilize terminology specific to a single OEM. Standard PAM solutions typically handle this via 'Secret Deletion,' 'Account Deprovisioning,' or 'One-Time Password (OTP)' workflows. We request that the authority to remove the clause	Refer #441

Response to the Pre-Bid Queries

98 6	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 29	Password check in/checkout must support execution of external powershell script immediately before or after the action	Restrictive (OEM Baised) : As per our understanding, there should be a powershell script that should execute as soon as a session is established via proposed PAM solution to be automatically initiated at the event of login. We request that the authority to remove the clause	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

98 7	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 52	The proposed solution must support a configuration where RDP & SSH sessions are brokered through PAM's own "jumpbox"/proxy component without Microsoft Remote Desktop Service Infra	Restrictive (OEM Baised) : For any solution initiating RDP sessions, MS RDS services are used. This is a Microosoft protocol and will be used for RDS sessions. Request to remove this clause.	Refer #442

Response to the Pre-Bid Queries

98 8	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 64	The proposed solution's account discovery function must allow for application owners to add custom discovery objects for systems, platforms, and devices not supported out-of-the-box through Windows native powershell.	Restrictive (OEM Baised) : Request to remove this clause.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

98 9	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 79	The 2nd layer encryption must be Quantum Safe. It must be able to protect data against current and foreseeable future Quantum Computers as recommended by NIST. Refer to NIST for description of Quantum Safe. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers	Restrictive (OEM Baised) : Request to remove this clause.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

99 0	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. 101	Solution must support real-time reputation checking	As per our understanding, the requirement is around risk analysis of the application and recommending actions to be evaluated.	Refer #39

Response to the Pre-Bid Queries

99 1	Volume II Technical Specification s	Page 96, Annexure N, Tab "PIM", Clause No. X	General query	Please let us know the count of Privilege Administrators to be considered for PAM requirements	Refer #444

Response to the Pre-Bid Queries

99 2	Volume II Technical Specification s	Page 96, Annexure N, Tab "PIM", Clause No. X	General query	Please let us know the concurrency of privilege sessions for recommending optimal hardware sizing	Refer #445

Response to the Pre-Bid Queries

99 3	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. X	General query	Please let us know the count of endpoints to be considered for PIM requirements	Refer #446

Response to the Pre-Bid Queries

99 4	Volume II Technical Specification s	Page 96, Annexure N, Tab "MFA & SSO", Clause No. X	General query	Please let us know the count of workforce used to be considered for MFA & SSO requirements.	Refer #447

Response to the Pre-Bid Queries

99 5	Volume II Technical Specification s	Page 96, Annexure N, Tab "MFA & SSO", Clause No. 9 and 14	The proposed solution should support multifactor authentication for Windows, Mac, Linux Operating systems	As per our understanding, the count of endpoints to be considered here are same as the count of endpoints to be considered for endpoint protection in the "PAM" tab requirements. Please confirm.	Refer #448

Response to the Pre-Bid Queries

99 6	Volume II Technical Specification s	Page 96, Annexure N, Tab "PAM", Clause No. X	General query	Please share the number of users and applications this solution will be utilized for?	Refer #449

Response to the Pre-Bid Queries

99 7	Volume II Technical Specification s	Scope of Work	Recommendations	Risk Management & Problem Statement : Relaying on a single OEM for both connectivity and security creates a significant Single Point of Failure—a critical vulnerability where a supply chain attack or software bug could compromise the entire infrastructure simultaneously. Recommendations : Consistent with standard practices in various large-scale Indian government projects, we request that the Network and Security components be decoupled. Mandating different OEMs for these layers ensures a heterogeneous environment, providing a necessary fail-safe and ensuring that the organization benefits from the widest spectrum of specialized technologies	As per RFP

Response to the Pre-Bid Queries

99 8	Volume II	Annexure N ; Secure Internet Access ; Clause No. 4	<i>Solution should facilitate remote users to securely access Internet and internal applications through Web Browsers, Desktop Clients, Mobile Clients, and Secured Browser etc.</i>	<i>We understand that Secure Internet Access requirement is for remote users only. Please confirm if the understanding is correct.</i>	Refer #2

Response to the Pre-Bid Queries

99 9	Volume II	Annexure N ; Secure Internet Access ; Clause No. 8	The proposed SECURE INTERNET ACCESS endpoint software agent deployed on user devices for secure internet, ZTNA and DLP should have the capability to support packet capture and digital experience Monitoring from the same agent.	DLP is already mentioned dedicatedly as separate section in the RFP. Hence, we request department to remove the DLP requirement from this section. Aside DLP tools perform deep content inspection and combining the requirement in Secure Internet Access which primarily focus to inspect traffic will Increase latency as well as Impact User experience. Hence, request department to remove DLP requirement and keep only Secure Internet and ZTNA under purview of Secure Internet Access.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 00	Volume II	Annexure N ; Secure Internet Access ; Clause No. 9	The endpoint agent of the proposed SECURE INTERNET ACCESS should have a packet capture capability as a built-in feature for ease of troubleshooting with a better user experience. In case this is not available as a built-in feature, bidders can include additional packet capture tools in their solution for the user endpoints with the required license, support, and services and the tool needs to be tightly integrated with the SECURE INTERNET ACCESS endpoint agent to deliver the mentioned functionality. To ensure security best practices are followed, the bidder must avoid using freeware tools and ensure proper patching and upgrades of the provided packet capture tool. SECURE INTERNET ACCESS, ZTNA and DLP must have single unified agent so that there is no overhead on the user system performance.	DLP is already mentioned dedicatedly as separate section in the RFP. Hence, we request department to remove the DLP requirement from this section. Also,DLP should be Data Centric as Modern data loss happens via Personal Cloud Storage, SaaS sharing links, AI tools, Enpoints (copy, paste screen capture), API based access. However SSE only controls network paths. Asking for a single unified agent will limits the participation of pure play DLP vendors.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 01	Volume II	Annexure N ; Secure Internet Access ; Clause No. 31	The DLP Solution should be Browser Agnostic and support non-browser generated Web Traffic and solution should not have dependency on Browser Extensions to function correctly.	DLP is already mentioned dedicatedly as separate section in the RFP. Hence, we request department to remove the DLP requirement from this section as combining DLP requirement in Internet Access will defeat the purpose of DLP. Since DLP requires Full content reconstruction, OCR & ML classifications, Context beyond the session (user role, data owner, business process)	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 02	Volume II	Annexure N ; Secure Internet Access ; Clause No. 32	Prevent Data Loss with Inline scanning across multiple classifiers and engines. Solution must have capability to define custom classifiers/engines, advanced DLP capabilities (fingerprinting, OCR, EDM, and Incident Management).	DLP is already mentioned dedicatedly as separate section in the RFP. Hence, we request department to remove the DLP requirement from this section as combining DLP requirement in Internet Access will defeat the purpose of DLP as DLP protect data at rest, in use, and in motion; Maintain consistent classification across channels, support forensic reconstruction and evidence preservation. However SSE DLP typically operates inline, has file size, protocol and encryption limits.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 03	Volume II	Annexure N ; Secure Internet Access ; Clause No. 33	Ability to apply DLP Rules for users performing uploads/downloads and attempt to exfiltrate data using screenshots of blocked data.	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP. Also as per DPDP Act, DLP should able to work on all data exfiltration channels viz endpoint, web, email and cloud and it should prevent Unauthorized data exfiltration, Accidental data leakage, Insider threats.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 04	Volume II	Annexure N ; Secure Internet Access ; Clause No. 34	DLP Solution must support data exfiltration attempts detection made via compressed files	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP. Also under DPDP Act, organization should demonstrate compliance, maintain auditability, prove controls were in place. Dedicated DLP solution can provide policy enforcement evidence, Incident logs, User activity tracking, Forensic Data.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 05	Volume II	Annexure N ; Secure Internet Access ; Clause No. 38	The solution should be able to perform DLP scanning for Private Applications as well	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP. Also as per DPDP Act, DLP can help customer in protecting personal data which includes Account numbers, Transaction Data, Contact Information, Financial Profiling data, Employee Personal Data.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 06	Volume II	Annexure N ; Secure Internet Access ; Clause No. 40	The remote user must not be able to see the Private Application Local IP even if they are authorized to access the application (if application access is based on FQDN via ZTNA, the real Application IP must be masked)	We understand that Secure Internet Access requirement is for remote users only. Please confirm if the understanding is correct.	As per RFP

Response to the Pre-Bid Queries

10 07	Volume II	Annexure N ; Secure Internet Access ; Clause No. 42	End Point DLP must protect USB Channel and allow data to be transferred to only authorized USB's. Block sensitive data from being copied to a Removable Storage Media (USB, Smartphone, External Harddisk etc.)	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP. Aside, DLP should do following functions for DPDP compliance viz; Granular Data Classification, Policy Enforcement, Contextual Awareness, Real - Time Monitoring and Blocking Violations, Coverage should be comprehensive (for Endpoints, Web, Network and Cloud), Incident Reporting and Management, Auditing and Logging.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 08	Volume II	Annexure N ; Secure Internet Access ; Clause No. 43	End Point DLP must protect Printing Channel, Network Sharing and Personal Cloud Storages [eg. Google Drive, Box, DropBox etc.]	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP as dedicated DLP will do consistent enforcement across Email, Endpoint, SaaS, Cloud and On Premise.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 09	Volume II	Annexure N ; Secure Internet Access ; Clause No. 47	The Solution should have the flexibility of configuring DLP Classifiers using Multiple AND, OR Logic Operators	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP. As dedicated DLP will give a single data taxonomy (Public/Internal/Confidential/ Restricted) along with consistent enforcement across Email, Endpoint, SaaS, Cloud and On Premise.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 10	Volume II	Annexure N ; Secure Internet Access ; Clause No. 52	Any component installed in Data Centers (on-premises or IaaS) must not need any inbound ACL rule in Customer DCs Firewall / Router to provide access to Private Application for remote users.	We understand that Secure Internet Access requirement is for remote users only. Please confirm if the understanding is correct.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 11	Volume II	Annexure N ; Secure Internet Access ; Clause No. 55	The Solution should be able to help with Optimization, Automation, consolidation of DLP Incidents via a Workflow Solution	DLP is already mentioned dedicatedly as separate section in the RFP, combining DLP requirement in Internet Access will defeat the purpose of DLP as both technologies have different role to play. Also as per DPDP Act, regulators and auditors expect DLP controls across: Endpoint DLP (printing, clipboard, USB/removable media, Local File access, Network shares) Email & Collaboration (Email attachments, Web uploads, Messaging tools) Cloud & SaaS (Personal Cloud Storage, Unauthorized SaaS usage) Monitoring & Response (Alerts, Incident workflows, Evidence retention)	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 12	Volume II	Annexure N; Secure Internet Access, Point No. 3	The solution provider should have achieved DoD Impact Level 5 (IL5) and FedRAMP High Authorization to reflect better security standards. The offered solution must be certified with CSA STAR, FedRamp, ISO 27001, ISO 27017, ISO 27018, SOC 2 / 3, FIPS 140-2, certification and Zero Trust Architecture designed by NIST (National Institute of Standards and Technology).	The DOD Impact Level 5(IL5) and Fedramp High Authorization both compliances refer to strict regulation from Govt perspective hence we request to modify the clause as "The solution provider should have achieved DoD Impact Level 5 (IL5) or FedRAMP High Authorization to reflect better security standards. The offered solution must be certified with CSA STAR, FedRamp, ISO 27001, ISO 27017, ISO 27018, SOC 2 / 3, FIPS 140-2, certification and Zero Trust Architecture designed by NIST (National Institute of Standards and Technology)."	Refer #588

Response to the Pre-Bid Queries

10 13	Volume II	Annexure N; Secure Internet Access, Point No. 46	The solution must have the ability to apply data masking controls to hide PII information on the web browser for sensitive applications accessed via Secured Browser or Remote Browser Isolation.	This is duplicate point as its already mentioned in secured Browser specifications Point No 24 so we request you to remove this from Secure Internet Access	Refer #589

Response to the Pre-Bid Queries

10 14	Volume II	Annexure N; Secure Internet Access, Point No. 65	The solution must have control to restrict access to camera, microphone, provide read-only access to secure application accessed via Secured Browser or Remote Browser Isolation.	This is duplicate point as its already mentioned in secured Browser specifications Point No 35 so we request you to remove this from Secure Internet Access	Refer #590

Response to the Pre-Bid Queries

10 15	Volume II	Annexure N; Secure Internet Access, Point No. 66	The solution must have file encryption capabilities to encrypt the files downloaded from the sensitive applications accessed via Secured Browser or Remote Browser Isolation.	This is duplicate point as its already mentioned in secured Browser specifications Point No 25 so we request you to remove this from Secure Internet Access	Refer #3

Response to the Pre-Bid Queries

10 16	Volume II	Annexure N; Secure Internet Access,Point No. 58	The solution must have NGFW, IPS for both web and non-web, Advanced Threat Protection, Advanced Sandbox and DNS Security feature from day 1 to secure internet traffic. The DNS Security solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc. extended for all DNS over HTTPS (DoH).	DOH can be blocked at client level using Inline policies so hence we request you to modify the clause for wider participation "The solution must have NGFW, IPS for non-web, Advanced Threat Protection, Advanced Sandbox and DNS Security feature from day 1 to secure application traffic. The DNS Security solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc."	Refer #592

Response to the Pre-Bid Queries

10 17	Volume II	Annexure N; Secure Internet Access, Point No. 18	Proposed solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc. extended for all DNS over HTTPS (DoH) regardless of DoH resolver used (no bypass)	DOH can be blocked at client level using Inline policies so hence we request you to modify the clause for wider participation "Proposed solution for Application access (not internet) should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries etc."	Refer #593

Response to the Pre-Bid Queries

10 18	Volume II	Annexure N; Secure Internet Access, Point No. 4	Solution should facilitate remote users to securely access Internet and internal applications through Web Browsers, Desktop Clients, Mobile Clients, and Secured Browser etc.	Since securely access the internet is already in the section in DLP as Web Protection Security for internet as majority of the web users are on prem aand taking entire internet traffic cloud will create dependency for the organisation around someone else datacenter, it will also require to publish the entire AD/LDAP to be published in the cloud, Hence request you to please amend the clause as : Solution should facilitate remote users to securely access internal applications through Web Browsers, Desktop Clients, Mobile Clients, etc	Refer #2

Response to the Pre-Bid Queries

10 19	Volume II	Annexure N; Secure Internet Access, Point No. 8	The proposed SECURE INTERNET ACCESS endpoint software agent deployed on user devices for secure internet, ZTNA and DLP should have the capability to support packet capture and digital experience Monitoring from the same agent.	DLP for endpoint, network channel including web and email are already asked in the RFP for outbound control, Asking same thing at multiple places will increase the cost, more importantly forensics data should never sent out on the 3rd party vendor, it creates chances of data exposures, Hence request you to please amend this clause as : The proposed Internal ACCESS endpoint software agent deployed on user devices for secure internal access via ZTNA have should have the capability to support packet capture and digital experience Monitoring for internal apps, if required.	Refer #999

Response to the Pre-Bid Queries

10 20	Volume II	Annexure N; Secure Internet Access, Point No. 9	The endpoint agent of the proposed SECURE INTERNET ACCESS should have a packet capture capability as a built-in feature for ease of troubleshooting with a better user experience. In case this is not available as a built-in feature, bidders can include additional packet capture tools in their solution for the user endpoints with the required license, support, and services and the tool needs to be tightly integrated with the SECURE INTERNET ACCESS endpoint agent to deliver the mentioned functionality. To ensure security best practices are followed, the bidder must avoid using freeware tools and ensure proper patching and upgrades of the provided packet capture tool. SECURE INTERNET ACCESS, ZTNA and DLP must have single unified agent so that there is no overhead on the user system performance.	This is OEM Specific clause, and considering already Internet access and DLP is already covered as on prem solution, considering all the majority of the user being the Organisation network and also DLP critical component containing all the sensitive information, and exposing that on someone else cloud always may create issues, More importantly in cases where machine not connected to SSE platform data exfiltration will happens, hence Organisation keep application access separate from Internet and DLP solution for good overall protection. Hence Request you to please delete this clause or amend it as : The endpoint agent of the proposed Secure application ACCESS should have a packet capture capability as a built-in feature for ease of troubleshooting with a better user experience. In case this is not available as a built-in feature, bidders can include additional packet capture tools in their solution for the user endpoints with the required license, support, and services and the tool needs to be tightly integrated with the proposed solution to deliver the mentioned functionality. To ensure security best practices are followed, the bidder must avoid using freeware tools	Refer #1000

Response to the Pre-Bid Queries

				and ensure proper patching and upgrades of the provided packet capture tool.	

Response to the Pre-Bid Queries

10 21	Volume II	Annexure N; Secure Internet Access, Point No. 11	The solution must operate in a full-proxy architecture (Hide user and application IP address) and should perform 100% SSL inspection of the internet traffic at scale without performance degradation	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	As per RFP

Response to the Pre-Bid Queries

10 22	Volume II	Annexure N; Secure Internet Access, Point No. 12	The proposed solution must allow administrator to define actions for handling untrusted server certificates, Unencryptable Traffic and define minimum client and server TLS versions	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

10 23	Volume II	Annexure N; Secure Internet Access, Point No. 13	The proposed solution must have following Web Security features – · URL Filtering and Dynamic content classification for unknown URLs · Inline Antivirus and Anti-spyware with full content inspection · SSL content inspection/HTTPS Proxy	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

10 24	Volume II	Annexure N; Secure Internet Access, Point No. 14	The solution should have strong content filtering database with 70+ categories and must have the ability to configure custom categories.	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money. Also solution having so less categories database will result ineffective web protection. Modern day solution should have categories for AI, Crypto currency, crypto minning as well.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 25	Volume II	Annexure N; Secure Internet Access, Point No. 16	The proposed solution shall be updated automatically with the new signatures at near real time basis for: A) Virus, B) Global Allow list/Block list URLs database C) Botnet D) Root kits E) Malware	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	As per RFP

Response to the Pre-Bid Queries

10 26	Volume II	Annexure N; Secure Internet Access, Point No. 17	The proposed solution should provide protection against advanced threats like cookie stealing, XSS and malicious active content, prevent malicious botnet and C&C communications, block outdated web browsers to reduce organisation risk, block malicious file downloads using https and https, blocking destinations in selected countries, blocking obfuscated javascripts, capabilities to inspect malware embedded in PDF, word, PPT files, protection against exploitation of web browser vulnerabilities, detect/block uploading/downloading of a malicious archived file.	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

10 27	Volume II	Annexure N; Secure Internet Access, Point No. 19	All DNS security should be applied to standard DNS (UDP, TCP) and DNS over HTTPS (DoH) regardless of DNS resolver targeted and regardless of location of user	Already covered in clause 18, hence request you to please delete this clause.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 28	Volume II	Annexure N; Secure Internet Access, Point No. 20	SECURE INTERNET ACCESS solution must provide the granular control for below or equivalent category:- · AI & ML Applications · Collaboration & Online Meetings · Consumer · Customer Applications · DNS over HTTPS Services · File Sharing · Finance · Health Care · Hosting Resources · Human Resources · Instant Messaging · IT Services · Legal · Productivity & CRM Tools · Sales & Marketing · Social Networking · Streaming Media · System Development · Webmail	This is already covered under the web protection section, hence request you to please delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also create the huge amount traffic towards the internet wasting resources and money.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

10 29	Volume II	Annexure N; Secure Internet Access, Point No. 23	SECURE INTERNET ACCESS solution must provide inspection like stateful filtering, access control list for workload traffic or unauthenticated traffic (Minimum 200GB data volume traffic per month or 200 MBPS Internet bandwidth)	This is already covered under the web protection section and also why should organisation have restriction on data volume or internet bandwidth, this reduces the Organisations ability to scalable hence request you to please the delete this clause for better ROI of RFP, otherwise organisation will purchase redundant solution and will also restrict the scalability of the solution.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

10 30	Volume II	Annexure N; Secure Internet Access, Point No. 24	The proposed solution must provide Virtual SECURE INTERNET ACCESS engine to deploy at customer DC/Cloud for threat inspection. There should not be restriction on number of virtual SECURE INTERNET ACCESS engine to be deployed at customer DC/Cloud for threat inspection.	This is already is the Web protection component of the solution, Hence request you to please drop the same.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 31	Volume II	Annexure N; Secure Internet Access, Point No. 30	The solution should have a unified agent delivering all the critical services [SECURE INTERNET ACCESS, Data Protection, Internet Security, Digital Experience Monitoring, and Secure Private application access] from the same agent and single unified management console.	OEM specific, Hence request you to please delete this clause	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 32	Volume II	Annexure N; Secure Internet Access, Point No. 31	The DLP Solution should be Browser Agnostic and support non-browser generated Web Traffic and solution should not have dependency on Browser Extensions to function correctly.	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1001

Response to the Pre-Bid Queries

10 33	Volume II	Annexure N; Secure Internet Access, Point No. 32	Prevent Data Loss with Inline scanning across multiple classifiers and engines. Solution must have capability to define custom classifiers/engines, advanced DLP capabilities (fingerprinting, OCR, EDM, and Incident Management).	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1002

Response to the Pre-Bid Queries

10 34	Volume II	Annexure N; Secure Internet Access, Point No. 33	Ability to apply DLP Rules for users performing uploads/downloads and attempt to exfiltrate data using screenshots of blocked data.	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1003

Response to the Pre-Bid Queries

10 35	Volume II	Annexure N; Secure Internet Access, Point No. 34	DLP Solution must support data exfiltration attempts detection made via compressed files	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1004

Response to the Pre-Bid Queries

10 36	Volume II	Annexure N; Secure Internet Access, Point No. 35	Prevent users from performing upload/downloads based on file type using File Type Control.	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 37	Volume II	Annexure N; Secure Internet Access, Point No. 36	Ability to block upload/download based on Document Classification Labels or identifiers	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 38	Volume II	Annexure N; Secure Internet Access, Point No. 37	The Solution should be able to protect sensitive data while being access from Unmanaged/3rd party devices	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 39	Volume II	Annexure N; Secure Internet Access, Point No. 39	The Solution should Monitor and Restrict sensitive data content leakage to Generative AI URL categories	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 40	Volume II	Annexure N; Secure Internet Access, Point No. 42	End Point DLP must protect USB Channel and allow data to be transferred to only authorized USB's. Block sensitive data from being copied to a Removable Storage Media (USB, Smartphone, External Harddisk etc.)	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1007

Response to the Pre-Bid Queries

10 41	Volume II	Annexure N; Secure Internet Access, Point No. 43	End Point DLP must protect Printing Channel, Network Sharing and Personal Cloud Storages [eg. Google Drive, Box, DropBox etc.]	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1008

Response to the Pre-Bid Queries

10 42	Volume II	Annexure N; Secure Internet Access, Point No. 54	The incident should specify the medium for the data transmission or violated file, including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 43	Volume II	Annexure N; Secure Internet Access, Point No. 55	The Solution should be able to help with Optimization, Automation, consolidation of DLP Incidents via a Workflow Solution	Already covered in the DLP section, hence request you to delete this clause as this DLP is cloud based and entire forensics will via cloud, and might result into data exposure	Refer #1011

Response to the Pre-Bid Queries

10 44	Volume II	Annexure N; DLP, Point No. 2	The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files.	Our understanding of the clause is that the solution should be able monitor applications defined in the system, to check if those are not used to exfiltrate the sensitive data, if confirm if the understanding is correct.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 45	Volume II	Annexure N; DLP, Point No. 7	DLP for Web – Proposed solution must block sensitive data from outbound web communications if they violate security policy. DLP for Network – Proposed solution must passively inspect network traffic for confidential data that is being sent in violation of security policy. The solution should be able to block outbound emails sent via SMTP if it violates the policy	Hope the ask here is to passively inspect the traffic via auditing the transaction inline to the violation action, please confirm.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 46	Volume II	Annexure N; DLP, Point No. 23	Solution should support compliance with global standards such as PCI DSS, SAMA, etc. It must provide continuous monitoring of data assets with immediate alerting mechanisms for policy violations.	The word Immediate is little ambiguous, hence request you to please remove the same.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 47	Volume II	Annexure N; DLP, Point No. 24	Solution must offer an intuitive interface and real-time dashboards for ease of use. It should allow us to define and apply specific data sensitivity levels and handling protocols. Also, it must facilitate the assignment of data owners for each asset to ensure accountability.	Our understanding of the term protocols, is SMTP, HTTP, HTTPS. Please confirm if its correct.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 48	Volume II	Annexure N; DLP, Point No. 41	The solution should have ability to block anonymizer sites or proxy avoidance tools. The solution should have an application program interface (API) to create categories and populate them with URLs and IP addresses for use in policy enforcement.	Hope the ask here is to create custom categories, Create custom, API-managed categories and Add URLs and IP addresses to API-managed categories, please confirm.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 49	Volume II	Annexure N; DLP, Point No. 43	Solution vendor should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, compromised websites, key loggers, Phishing and other frauds, Spywares	Considering modern days threats request you to add Gen AI and Crypto related categories as well. Hence request you to please amend the clause as : Solution vendor should ensure to provide below mentioned security categories from day1 with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Generative AI for Multimedia, Conversation, Text, Code, Bot networks, compromised websites, key loggers, Phishing and other frauds, Spywares, and crypto currency & crypto minning.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 50	Volume II	Annexure N; NTA, Point No. 1	The proposed solution should detect and block advanced network level threats including but not limited to APT attacks, zero-day attacks, signature based or signature less attacks, file-based or file- less attacks and any malicious call-back connection in real-time / near real-time.	NTA or NDR works in promiscuous i.e TAP mode and cannot directly Block the Traffic, they are not recommended to work Inline to avoid Latency and Network Down incidents. Hence NTA solution are designed to share alerts to SOAR/Firewall/NIPS for blocking action. So please change the Clauses related to response action through NDR as follows. "The proposed solution should detect and block (through Firewall/SOAR/NIPS) advanced network level threats including but not limited to APT attacks, zero-day attacks, signature based or signature less attacks, file-based or file- less attacks and any malicious call-back connection in real-time / near real-time."	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 51	Volume II	Annexure N; NTA, Point No. 2	The proposed NDR should have centralized sandboxing component within the solution ~~and sandboxing should be done on the MeitY compliant cloud hosted in India.~~	Should not be dependent on third party sandboxing for better management and centralized approach.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 52	Volume II	Annexure N; NTA, Point No. 3	The proposed NDR component should seamlessly integrate with the proposed SIEM solution for threat detection and response in the NPCL's environment. Integration to be ensured by the bidder.	We believe its DOP and not NPCL?	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 53	Volume II	Annexure N; NTA, Point No. 4	The proposed solution should be able to detect and block any suspicious network communication including multi-stage, multi-flow, zero-day, C&C, ransomware, polymorphic or other evasive attacks in real-time regardless of ports and protocols on real-time basis. Legitimate network traffic should not be impacted.	The proposed solution should be able to detect and block (through Firewall/SOAR/NIPS) any suspicious network communication including multi-stage, multi-flow, zero-day, C&C, ransomware, polymorphic or other evasive attacks in real-time regardless of ports and protocols on real-time basis. Legitimate network traffic should not be impacted.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 54	Volume II	Annexure N; NTA, Point No. 5	The proposed solution should support multiple protocols for inspection including but not limited to HTTP, HTTPS, SFTP, SMB, DNS, POP3, FTP and P2P protocols to detect, flag and respond to malicious activity at network level. The solution should be able to analyse minimum 100+ Protocols.	NTA Should be well versed to identify and Protocol, and should have ability to analyse the behaviour of these entities, Add this aspect for better solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 55	Volume II	Annexure N; NTA, Point No. 6	The proposed solution must be able to perform network traffic analysis and inspection to identify any suspicious / malicious activities in the DOP's network and take automated response action to block such activities.	" The proposed solution must be able to perform network traffic analysis and inspection to identify any suspicious / malicious activities in the DOP's network and take automated response action to alert and block such activities through Firewall/SOAR/NIPS .	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 56	Volume II	Annexure N; NTA, Point No. 7	The proposed solution should provide signature-less, dynamic analysis to inspect suspicious objects, identify targeted, evasive and unknown threats and further provide advanced response actions to block the malicious traffic.	The proposed solution should provide signature-less, dynamic analysis to inspect suspicious objects, identify targeted, evasive and unknown threats and further provide advanced response actions to alert and block the malicious traffic through Firewall/SOAR/NIPS ..	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 57	Volume II	Annexure N; NTA, Point No. 11	The proposed solution should have advanced incident response capabilities to respond to the cyber threats including blocking the malicious network connection.	The proposed solution should have advanced incident response capabilities to respond to the cyber threats including blocking the malicious network connection through Firewall/SOAR/NIPS.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 58	Volume II	Annexure N; NTA, GENERAL	The proposed solution should support more than 100+ files types for inspection in non-evasive virtual analysis environment, the data analysis engine should have capability of 30 parallel file/ images analysis capability on the same appliance so as during execution, analysis of files, objects, flows, attachments, URL's the environment unleashes any hidden or targeted advance malware attacks. The attacks should not be able to evade the environment leading to poor detection & false negative scenarios.	NTA Should be well versed to identify Files Type and should have ability to analyse the behaviour of these files entering into via network traffic, Add this aspect for better solution.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 59	Volume II	Annexure N; NTA, GENERAL	The solution should be provided with sustained throughput of 10 Gbps. Should support Network traffic capture using a SPAN port, and/or port mirror, should be able to analyze East-West and North-South Segments, Should utilize packet capture to perform the detailed analysis and forensics as per the defined criterias	NTA throughput is not been asked in the specification.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 60	Volume II	Annexure N; NTA, GENERAL	The Solution components must be a purpose build dedicated Hardware Appliance/appliances and should not be the part of NGFW/UTM/DDOS appliances and firmware and should be different from firewall OEM for Layered security.	Its must for layered security approach	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 61	Volume II	Annexure N; NTA, GENERAL	Solution should provide automated payload analysis, Network Traffic analysis covering entire network landscape, the solution should have support for major Operating Systems (Windows and Linux) as a part of the execution environment. The analysis environment must be deployed, built, maintained, and delivered by the OEM to minimize risk of any dependency on managing or creating the environment manually by Security administrators who may not have relevant skills.	Traffic analyzer should support payload analysis for holistic security requirement.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 62	Volume II	Annexure N; NTA, GENERAL	The proposed solution should support the integration of 3rd party intelligence feed and support STIX/TAXII and YARA.	The proposed solution should support the integration of 3rd party intelligence feed and support STIX/TAXII and YARA.	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

10 63	Volume II	Annexure N; NIPS, Point No. 1	The proposed appliance should have more than ~~35 Gbps~~ 40Gbps of real-world Intrusion Prevention System (IPS) Inspection throughput and support atleast 8 Gbps SSL throughput.	Preventing Vulnerability attack is the primary functionality of NIPS solution hence it has to be distinctly asked in the RFP specs. NIPS throughput should always be taken in reference to Firewall. Here Firewall throughput is 50Gbps so NIPS throughput should be atleast 80% of FW throughput ie 40Gbps. "The proposed appliance should have more than 40 Gbps of real-world Intrusion Prevention System (IPS) Inspection throughput and support atleast 8 Gbps SSL throughput. The OEM shall provide capabilities of interim compensatory control which shall prevent exploitation of various remotely exploitable vulnerabilities & exploits. Solution should provide protection from all known vulnerability-based attacks from day one"	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 64	Volume II	Annexure N; NIPS, Point No. 2	The proposed solution should be a standalone independent IPS appliance. The OEM of the proposed NIPS solution should be different from the OEM of the Internal Firewall solution. The proposed appliance should have minimum of 8 x 10G BaseT ethernet ports, 8 x 1/10 Gigabit SFP+ ports, 4 x 25 Gigabit SFP28 and 4 x 100 Gigabit QSFP28 with Short Range transceivers	10G Base it is Legacy connectivity which is switched to fiber over the period time, and Base-T should have been asked for the 1G connectivity. We request to change the clause as below. Also for Layered security IPS should not be the part of any firewall module but should be independent device. "The proposed solution should be a standalone independent IPS appliance. The OEM of the proposed NIPS solution should be different from the OEM of the ~~Internal~~ Firewall solution provider. The proposed appliance should support 8 x 1G BaseT ethernet ports, 8 x 1/10 Gigabit SFP+ ports, 4 x 25 Gigabit SFP28 and 4 x 100 Gigabit QSFP28 with Short Range transceivers"	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 65	Volume II	Annexure N; NIPS, Point No. 4	The proposed solution must be able to operate in symmetric/Asymmetric traffic environment with signatures/filters protection.	For better qualification of OEM it is must to mentioned the number of filters they OEM has already developed to prevent from known threats from Day one, filters are the core of any IPS solution. The proposed solution must be able to operate in symmetric/Asymmetric traffic environment with signatures/filters protection. Proposed NIPS should have inbuilt 25,000+ vulnerability/exploit filters pertaining to security and applications apart from user define signatures/filters	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 66	Volume II	Annexure N; NIPS, Point No. 5	Should have threat prevention capabilities to easily import IPS signatures from cyber security advisory bodies such as Cert-IN, NCIIPC, government entities or regulated entities.	All the Cyber security advisory bodies provides with IOC/IOA in STIX format to update the threat repository hence please change the clause as "Should have threat prevention capabilities to easily import IOC/IOA from cyber security advisory bodies such as Cert-IN, NCIIPC, government entities or regulated entities."	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 67	Volume II	Annexure N; NIPS, Point No. 7	The proposed solution should have 2 million concurrent sessions on Layer 7 and atleast 120,000 new connections per second on Layer 7 from day-one.	The Numbers asked here are very low looking at the kind of project and traffic its going to handle in future please change this clause as "The proposed solution should have 200 million concurrent sessions ~~on Layer 7~~ and atleast ~~120,000~~ 800,000 new connections per second ~~on Layer 7~~ from day-one for IMIX traffic.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 68	Volume II	Annexure N; NIPS, Point No. 9	Latency of the proposed IPS should be less than 350 microseconds and doesn't affect the overall network latency.	350 Microseconds is very high Latency which can cause application to time out if single solution generate this latency overy latency will increase exponentially, its not desirable, generally all the NIPS device does not generate latency of more than 60 microseconds hence we request to change the clause as "Latency of the proposed IPS should be less than 60 microseconds and doesn't affect the overall network latency. "	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 69	Volume II	Annexure N; NIPS, Point No. 14	The proposed solution shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: •Tap Mode •Transparent mode (IPS Mode) •Layer 2 •Layer 3 ~~Should be able to operate in mix of multiple modes.~~ This proposed solution should have bypass traffic for IPS internal issues i.e. memory hang, firmware crash etc. If bypass functionality is not available, then the bidder/ OEM should propose the NIPS solution in HA.	NIPS never been configured as a L3 Device hence this clause is not natively aligned with NIPS functionality we request to change the clause as "The proposed solution shall support Dual Stack IPv4 / IPv6 application control and threat inspection support in: •Tap Mode •Transparent mode (IPS Mode) •Layer 2 This proposed solution should have bypass traffic for IPS internal issues i.e. memory hang, firmware crash etc. If bypass functionality is not available, then the bidder/ OEM should propose the NIPS solution in HA"	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 70	Volume II	Annexure N; NIPS, Point No. 16	The proposed NIPS should have the ability to create custom application signatures and categories directly on NIPS without the need of any third party tool or technical. Also, it should have a power failure bypass module that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedure. ~~If bypass functionality is not available, then the bidder/OEM should propose the NIPS solution in HA.~~	As NIPS solution works in L2 Mode the Traffic Switchover Happens at Firewall Level in case of NIPS Failure, hence IPS HA itself does not switch over traffic, the Compliance statement need to be change as follows "The proposed NIPS should have the ability to create custom application signatures and categories directly on NIPS without the need of any third party tool or technical. Also, it should have a Internal ~~power~~ failure bypas module to ensure uninterrupted network continuity during any hardware or software failure that can support hot swappable function which allows traffic to bypass even after a module get unplugged out of IPS Box during the RMA procedure". ~~If bypass functionality is not available, then the bidder/OEM should propose the NIPS solution in HA."~~	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 71	Volume II	Annexure N; NIPS, Point No. 18	The proposed solution must be able to support GTP inspection for GPRS/3G mobile networks.	There are many different traffic types that is missing and do need indepth analysis hence please include all those traffic generally available in IMIX environment The NIPS solution should supports inspection of IPv6/v4 traffic with VLAN and MPLS tags, tunnelled traffic (i.e 4in6, 6in4 and 6in6) and P2P attacks. Solution should supports GRE and GTP inspection in asymmetric traffic environments.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 72	Volume II	Annexure N; NIPS, Point No. 19	The proposed solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score.	The NIPS Should have ability to block country based attack as soon as there is surge in any malicious activity related to state sponsored APT activity. The proposed solution must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score. Must have the ability to view attack activities base on continent and countries. The solution should provide region-wise visibility of IPS filters that received the maximum hits globally and region wise like India; to strengthen the enablement of relevant filters	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 73	Volume II	Annexure N; NIPS, Point No. 25	The proposed management system shall support dashboard for the threat insights that shows correlated data such as breached host, IoC data, 3rd party VA scan integration data and pre-disclosed vulnerability discovered etc.	The proposed management server must support the archiving and backup of events and export to SCP and s/FTP and must allow the report to be exported into other format such as PDF, CSV, XML etc. Also a centralized management server for enterprise management of the IPS devices and must be an appliance based on a hardened OS shipped by-default from factory, the management server should be provided with minimum 800 GB of storage for Reports and logs.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 74	Volume II	Annexure N; NIPS, Point No. 26	The proposed solution should be in Gartner leader's quadrant for "Intrusion Detection and Prevention Systems" as per latest report Or the OS of the IPS should be certified under Common Criteria program (global or the Indian Common Criteria Certification Scheme (IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY)) program for NDPP.	"Gartner report of IPS is not available since last 8 years hence this clause need to be change to ask for latest reports applicable to NIPS devices available in the industry, also Government of India does not have any dedicated program for NDPP rather its an international body NIAP provides with NDcPP certificate, also some more must have certifications are missing from this clause . ""The proposed NIPS appliance should have following valid certifications (Certificate copies must be submitted at the time of bidding): a. NDcPP Certification b. EAL2+ or higher c. FIPS 140-2 Compliance Certificate d. Safety: IEC62368-1:2014; IEC62368-1: 2018, EN55035:2017/A11:2020 Any OEM failing to submit above certificates for the exact proposed NIPS appliance shall be declared technically non-compliant and eliminated from further evaluation""	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 75	Volume II	Annexure N; NIPS, GENERAL	To protect the network against Zero-Day threats OEM should have a strong Zero-Day research team and must demonstrate contributions of more than 100 Zero-Day vulnerability discoveries in the past three years relevant document to be submitted along with bid.	These are the must have additional specifications for any reputed NIPS OEM as these specification ensure quality NIPS OEM to get qualified for this mission critical project.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 76	Volume II	Annexure N; NIPS, GENERAL	The NIPS shall support STIX/TAXII format to receive threat intelligence feeds from Day one. Should use STIX/TAXII for IPS enforcement of IP, DNS, and URL Indicators of Compromise (IoCs) to protect against threats like botnet, C&C servers, malware domains, proxy networks, malicious IP addresses, hosts etc. for correlation and blocking in the NIPS.	These are the must have additional specifications for any reputed NIPS OEM as these specification ensure quality NIPS OEM to get qualified for this mission critical project.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 77	Volume II	Annexure N; NIPS, GENERAL	Solution must support IP reputation intelligence feeds and custom lists of IP addresses including a global blacklist. The solution should have the capability to detect hash-based detection mechanism to detect any malicious traffic pattern	These are the must have additional specifications for any reputed NIPS OEM as these specification ensure quality NIPS OEM to get qualified for this mission critical project.	The referenced solution/component is not part of the scope of work under this RFP.

Response to the Pre-Bid Queries

10 78	Volume II	Annexure N; DDoS, Point # 1	Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance with 10 Gbps of Mitigation Throughput scalable to 20Gbps.	Restricted clause: Proposed DDOS Solution must not be part/ added functionality of any UTM or NGFW or any whitelabeled or virtual solution running on third party hardware or Router, ~~Application Delivery Controller, Firewall, Proxy based architecture or any Stateful Appliance~~ with 70 Gbps of Mitigation/Appliance Throughput	Refer #311

Response to the Pre-Bid Queries

10 79	Volume II	Annexure N; DDoS, Point # 3	The proposed appliance must provide: 1. Minimum Clean Traffic Throughput- 5 Gbps Scalable to 10 Gbps 2. Minimum SSL TPS/CPS of 40 K with RSA 2K keys via HW based Acceleration	The proposed appliance must provide: ~~1. Minimum Clean Traffic Throughput- 5 Gbps Scalable to 10 Gbps~~ 2. Minimum SSL TPS/CPS of 70 K with RSA 2K keys via HW based Acceleration	Refer #312

Response to the Pre-Bid Queries

10 80	Volume II	Annexure N; DDoS, Point # 6	The proposed DDOS solution must be able to inspect all the SSL traffic and should also have provision to only inspect first packet for Lower Latency.	Restricted clause: The proposed DDOS solution must be able to inspect all the SSL traffic ~~and should also have provision to only inspect first packet for Lower Latency.~~	Refer #313

Response to the Pre-Bid Queries

10 81	Volume II	Annexure N; DDoS, Point # 10	Inspection and prevention are to be done in same hardware. OEM must be Make in INDIA Class -1 compliant as per Government MII Guidelines & subsequent amendments.	Restricted clause: Inspection and prevention are to be done in same hardware. ~~OEM must be Make in INDIA Class -1 compliant as per Government MII Guidelines & subsequent amendments.~~	Refer #314

Response to the Pre-Bid Queries

10 82	Volume II	Annexure N; DDoS, Point # 11	The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create signatures within 20 Secs for zero-day DDoS attacks and DNS DDOS attacks.	Restricted clause: The proposed solution should have a mitigation mechanism to protect against zero-day DoS and behavioral DoS attacks without manual intervention and be able to create signatures ~~within 20 Secs~~ for zero-day DDoS attacks and DNS DDOS attacks.	Refer #315

Response to the Pre-Bid Queries

10 83	Volume II	Annexure N; DDoS, Point # 28	The Propose Appliance should Support multiple Protection option for Encrypted Attack Mitigation: a) Keyless SSL Protection b) First Request SSL Protection c) Selective Full SSL Protection d) Full SSL Protection	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #316

Response to the Pre-Bid Queries

10 84	Volume II	Annexure N; DDoS, Point # 29	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. Anti-Scanning Profile. 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection 7. Quantile DoS	The appliance should have below Security Protection Profiles: 1. BDoS Protection. 2. ~~Anti-Scanning Profile.~~ 3. SYN-Flood Protection. 4. Traffic Filters. 5. DNS Protections. 6. Https Flood Protection 7. ~~Quantile DoS~~	Refer #317

Response to the Pre-Bid Queries

10 85	Volume II	Annexure N; DDoS, Point # 33	The Proposed Solution should have User Defined Feed which should offers large scale IP or subnet blocking from an external 3rd party data feed using text file via manually update or integration with API. This should support upload of atleast 2M million IP addresses or subnets.	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #318

Response to the Pre-Bid Queries

10 86	Volume II	Annexure N; DDoS, Point # 34	The Proposed Solution should have TLS Fingerprint Reputation Feed to block high-risk malicious fingerprints providing a additional proactive layer of protection.	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #319

Response to the Pre-Bid Queries

10 87	Volume II	Annexure N; DDoS, Point # 38	Proposed Appliance should have various mitigation techniques over to protect from multi vector DNS based Attacks: 1. Allow list Enforcement – allow only legitimate FQDNs and deny random-subdomains queries (DNS water torture attacks). 2. Anti-spoofing – deny queries that originate from spoofed attack sources to deny query flood vectors. 3. Adaptive Rate-Limit – deny real sources (resolvers) that generate too many repeating queries	Restricted clause: Please delete this clause as it is specific to a single OEM.	Refer #321

Response to the Pre-Bid Queries

10 88	Volume II	Annexure N; NGFW, Point # 1	NGFW Throughput (Application Visibility and Control/Application- Identification and Logging enabled considering webmix/appmix traffic flows): 50 Gbps or higher	NGFW Throughput/ Application Control Throughput (Application Visibility and Control/Application- Identification and Logging enabled considering webmix/appmix traffic flows/enterprise mix): 80 Gbps or higher from single appliance without any stacking/cluster solution.	Refer #141

Response to the Pre-Bid Queries

10 89	Volume II	Annexure N; NGFW, Point # 2	NGTP Throughput (Enabling Firewall, IPS, URL filtering / Web Security Essentials, Application Control, Anti-Virus, Anti-Bot, DNS Security, Basic File Blocking and Logging enabled considering webmix/appmix flows): 30 Gbps or higher	NGTP Throughput (Enabling Firewall, IPS, Application Control, Anti-Virus, and Logging enabled considering webmix/appmix flows/enterprise mix)): 70 Gbps or higher from single appliance without any stacking/cluster solution.	Refer #142

Response to the Pre-Bid Queries

10 90	Volume II	Annexure N; NGFW, Point # 3	Minimum Concurrent TCP Connections post enables Application Visibility and Control (AVC) or Concurrent http sessions: 500 million TCP or 5 million http	Minimum Concurrent TCP Connections post enables Application Visibility and Control (AVC) or Concurrent http sessions: 100 million at layer 4 or 10 million at layer 7 from single appliance without any stacking/cluster solution.	Refer #143

Response to the Pre-Bid Queries

10 91	Volume II	Annexure N; NGFW, Point # 4	Minimum New TCP Connection per second post enable AVC or http sessions per second: 2,500,000 TCP or 250,000 http	Minimum New TCP Connection per second post enable AVC or http sessions per second: 1 million at layer 4 or 400,000 at layer 7 from single appliance without any stacking/cluster solution.	Refer #144

Response to the Pre-Bid Queries

10 92	Volume II	Annexure N; NGFW, Point # 5	10G RJ45 8 or higher	Kindly remove / edit the above specifications Considering scalability of project and overall incoming volume it is recommended to have higher factored external firewall solution.	Refer #145

Response to the Pre-Bid Queries

10 93	Volume II	Annexure N; NGFW, Point # 6	10G SFP+ 10 or higher	10G SFP+ 20 or higher	Refer #146

Response to the Pre-Bid Queries

10 94	Volume II	Annexure N; WAF, Point # 5	The WAF Solution should have penalty scoring mechanism to block bad actor from repeated violation of security policies configured for set amount of time	The WAF Solution should have mechanism to block bad actor from repeated violation of security policies configured/brute force attack.	Refer #203

Response to the Pre-Bid Queries

10 95	Volume II	Annexure N; WAF, Point # 8	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or IP address d. Should be able to generate unique identifier to track attack event	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity: a. Ability to drop requests and responses, b. Block the TCP session, c. Block the application user, or IP address d. Should be able to generate unique identifier/ Event ID to track attack event	Refer #204

Response to the Pre-Bid Queries

10 96	Volume II	Annexure N; WAF, Point # 10	WAF solution should have GraphQL content profile and policy template and attack signatures on GraphQL traffic	WAF solution should have GraphQL content profile/protection rules and policy on GraphQL traffic	Refer #205

Response to the Pre-Bid Queries

10 97	Volume II	Annexure N; WAF, Point # 14	The proposed device should have Hypervisor (should not use Open Source) Based Virtualization feature that virtualizes the Device resources—including CPU, memory, network, and acceleration resources. The Hypervisor used to virtualize the hardware should be a specialized purpose build hypervisor and NOT a commercially available hypervisor (like XEN, VMware, KVM etc.). (Public Available Reference Link should be shared) Each Virtual Instance contains a complete and separated environment of the Following: a) Resources, b) Configurations, c) Management, d) Operating System It should NOT use/allow 3rd party or open source software to be deployed as network functions on the same hardware.	Request for Deletion	Refer #206

Response to the Pre-Bid Queries

10 98	Volume II	Annexure N; WAF, Point # 15	Proposed WAF and DDoS Should integrate with each other. It should have a unique Messaging mechanism that efficiently mitigates attacks by sending attack information to DDoS located at the Network Perimeter.	Proposed WAF device shall have native capability to protect against DOS attacks, without relying on any 3rd party device.	Refer #207

Response to the Pre-Bid Queries

10 99	Volume II	Annexure N; WAF, Point # 16	Bidder to proposed separate Centralized Dashboard and should Provide at least following information: - Application dashboard - Per application analytics - SSL statistics (handshake & cypher breakdown, rejected handshake) - SSL CPS - System dashboard (Device CPU, Memory, Port Status etc) - Network Dashboard (CPS, Throughput, Concurrency, Real Server Availability, HA Status etc) - L4 events - Per transaction type events (delay, user agent, response, headers) - SSL Events (type of handshake, cypher and TLS version) - Attack Dashboard - OWASP Top 10 Based Attack details - Geo Based Attack Details	Bidder to proposed separate Centralized Dashboard and should Provide at least following information: - Application dashboard - Per application analytics - SSL statistics (handshake & cypher breakdown, rejected handshake) - SSL CPS - System dashboard (Device CPU, Memory, Port Status etc) - Network Dashboard (CPS, Throughput, Concurrency, Real Server Availability, HA Status etc) - L4 events - Per transaction type events (delay, user agent, response, headers) - SSL Events (type of handshake, cypher and TLS version) - Attack Dashboard - OWASP Top 10 Based Attack details - Geo Based Attack Details	Refer #208

Response to the Pre-Bid Queries

11 00	Volume II	Annexure N; WAF, Point # 17	The proposed solution should Support Elastic Licensing Model and support below flexibility : 1. A single throughput/capacity license to be shared across physical and Virtual ADCs, on premise and in the cloud, regardless of location or type 2. A complete automation of ADC services deployment and maintenance, allowing the administrator not only to seamlessly spin up new ADC instances, but also use wizards and scripts to distribute the corresponding ADC service configuration – all at the same push of a button. 3. Reclaim capacity from decommissioned instances and reallocate it to new deployments, ensuring optimal license utilization	Request for deletion	Refer #209

Response to the Pre-Bid Queries

11 01	Volume II	Annexure N; WAF, Point # 18	The proposed device should supports SSL offload for the following protocols: - HTTPS - Generic SSL - SIP - SMTP (STARTTLS) - IMAP (STARTTLS) - POP3 (STARTTLS) - LDAP (STARTTLS) - FTPS	Request for deletion	Refer #210

Response to the Pre-Bid Queries

11 02	Volume II	Annexure N; WAF, Point # 19	The proposed device should use standard VRRP (RFC – 2338) for High Availability.	The proposed device should use standard VRRP (RFC – 2338) or any propriety protocol for High Availability.	Refer #211

Response to the Pre-Bid Queries

11 03	Volume II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	15. CTS - An online image-based cheque clearing system where cheque images and Magnetic Ink Character Recognition (MICR) data are captured at the collecting branch and transmitted electronically, eliminating the actual cheque movement.	"The Cheque Truncation and Clearing System handles sensitive financial instruments and mandates secure exchange of cheque images, MICR data, transaction metadata, and settlement files between Participating Banks, the Clearing House, and Core Banking Systems. To ensure integrity, authenticity, confidentiality, and non-repudiation of these transactions, a FIPS certified HSM is required. CTS specifications mandate digital signing of cheque images/data packets and HSM enables compliance by ensuring tamper-resistant key lifecycle management, auditability, and legally defensible digital signatures. To comply with the CTS security requirements, a separate requirement of HSM must be defined with the industry standard	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

11 04	Volume II	Page 41: 5.1.4.5 Operations and Maintenance Support for the Centralised Cheque Clearing System (CTS)	DoP has an ongoing contract with M/s Oritso Pvt. Ltd. for Monitoring and Maintenance Support for the Centralised Cheque Clearing System (CTS), valid until June 2026. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format.	specifications such as but not limited to: - HSM should have FIPS 140-3 Level 3 with certification in the name of OEM (Proposing third party FIPS 140-3 L3 certification will not be considered) - The solution must support AES (128-256), ARIA,ECC(224- 512), HMAC , SEED, TDES, RSA (1024-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc. - The solution must support asymmetric encryption algorithms including RSA (2048/3072/4096-bit) and ECC (P-256, P-384). - HSM Host Interface: Should have at least 4x1 Gigabit Ethernet ports with port bonding. Should have IPv4 and IPv6 support - HSM should have Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature - The appliance and HSM cryptocard should be from the same OEM only and not as a bundled or assembled device. - Proposed HSM should support - Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM - HSM should be PQC ready with the capabilities to evaluate Kyber key generation and encapsulation functions as	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

				well as the hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations. - HSM should support secure key backup and recovery process direct on hardware device or file in encrypted form. - HSM should be configurable to communicate only with authenticated servers using strong cryptographic technique and the secure channel should be terminated at the cryptographic processor and not to the HSM chassis. - Should support clustering, load balancing without the need of external load balancer Please include a dedicated HSM technical specification as part of this requirement. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 5,000 RSA-2048 signing operations per second. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

11 05	Volume II	Page 18: 4. Current State Overview Table 4: Functional Blocks of POSB	eKYC/ADV - Applications integrated with UIDAI to enable Aadhaar-based authentication and KYC services, with secure storage of Aadhaar data in compliance with UIDAI guidelines.	The eKYC and Aadhaar Data Vault solution processes and stores Aadhaar numbers, reference IDs, demographic data, and authentication outcomes. As per UIDAI Security Guidelines and Aadhaar Regulations, entities handling Aadhaar must implement strong cryptographic controls to ensure confidentiality, integrity, and non-repudiation. A Hardware Security Module is required to securely perform, enforce, and protect cryptographic operations and key material used for encryption, tokenization, authentication, and signing within the Aadhaar ecosystem. UIDAI mandates encryption of Aadhaar numbers and related sensitive attributes. To comply with UIDAI mandate, a separate requirement of HSM must be	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

11 06	Volume II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	DoP has an existing contract with M/s Integra Micro Solutions for the Maintenance of Aadhaar-compliant eKYC and Data Vault, valid until November 2029. Both functionalities have been implemented and are currently being maintained by Integra's resources. The SI may plan to continue with the existing product stack and renew the associated licenses in accordance with their respective expiry timelines, or propose alternative software solutions along with a detailed deployment and migration plan. The SI shall factor in all applicable costs for the chosen approach and include the same in the Commercial Bid, strictly as per the prescribed format. This includes support for Aadhaar Data Vault (ADV), an eKYC Solution, and a Hardware Security Module (HSM), in compliance with the guidelines issued by UIDAI and relevant regulatory bodies.	defined with the industry standard specifications such as but not limited to: - HSM should have FIPS 140-3 Level 3 with certification in the name of OEM (Proposing third party FIPS 140-3 L3 certification will not be considered) - The solution must support AES (128-256), ARIA, ECC(224- 512), HMAC , SEED, TDES, RSA (1024-4096) and the Crypto mode (CBC, CBC-CS1, ECB, GCM) etc. - The solution must support asymmetric encryption algorithms including RSA (2048/3072/4096-bit) and ECC (P-256, P-384). - HSM Host Interface: Should have at least 4x1 Gigabit Ethernet ports with port bonding. Should have IPv4 and IPv6 support - HSM should have Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature - The appliance and HSM cryptocard should be from the same OEM only and not as a bundled or assembled device. - Proposed HSM should support - Windows, Linux. Virtual: VMware, Hyper-V, Xen, KVM - HSM should be PQC ready with the capabilities to evaluate Kyber key generation and encapsulation functions as	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

				well as the hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations. - HSM should support secure key backup and recovery process direct on hardware device or file in encrypted form. - HSM should be configurable to communicate only with authenticated servers using strong cryptographic technique and the secure channel should be terminated at the cryptographic processor and not to the HSM chassis. - Should support clustering, load balancing without the need of external load balancer Please include a dedicated HSM technical specification as part of this requirement. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 5,000 RSA-2048 signing operations per second. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

11 07	Volume II	Page 42: 5.1.4.7 Maintenance of Aadhaar-Compliant eKYC, Data Vault, and HSM Infrastructure for DoP	3. The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-2 Level 3 or higher standards.	As FIPS 140-2 validation certificates will be moved to the Historical List in September 2026, they will no longer be considered active for regulated compliance or new procurements. Request: Replace the existing clause with the following updated compliance requirement: "The HSM supports encryption, decryption, and digital signing functions and complies with FIPS 140-3 Level 3 or higher standards."	Bidders may refer to the Corrigendum Annexure HSM for additional details.

Response to the Pre-Bid Queries

11 08	Volume II	Page 17: 4. Current State Overview Table 4: Functional Blocks of POSB	9. Card Management System - Card Management System is a solution that manages the complete ATM/Debit Card Issuance cycle for DoP customers.	The Card Management System and ATM Switch handle issuance, lifecycle management, authorization, and verification of payment card transactions. These systems must securely perform sensitive cryptographic operations, including PIN processing, card data encryption, EMV cryptograms, key exchange, and secure key management. To ensure compliance with global payment security standards, these cryptographic operations must be executed within a certified payment HSM. Please add the below clause: The solution shall integrate with a certified Payment HSM to securely perform cryptographic functions related to PIN processing, EMV card issuance, transaction authorization, message authentication, and	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

11 09	Volume II	Page 16: 4. Current State Overview	13. ATM Switch - ATM Switch is required to handle all ATM transactions of the customers	secure key management, in compliance with PCI PIN Security Requirements, EMV Standards, and card scheme mandates. It must follow the industry standard specifications such as but not limited to: - Capable of translating up to 10000 PIN triple DES Pin block Per second and minimum of 25 PIN triple DES Pin block Per second - Should have GUI/CLI available with 2 factor Authentication using USB Tokens/smart cards. - HSM Must have two dedicated port for host communication and atleast one dedicated management port. - The proposed payment HSM must be PCI v3 certified. - HSM should support variant and keyBlock LMK. - HSM must support cryptographic separation of application keys using different LMK and should be capable of storing up to 20 LMKs. - HSM remote management solution must have PCI HSM v3 Remote Access Platform (RAP) certification - HSM should support remote access technology with encrypted connection to maintain security in all configuration and remote key loading processes. Kindly confirm whether DOP looking to secure the	Card Management System and ATM Switch are already implemented. Bidder has to ensure integration.

Response to the Pre-Bid Queries

				transactions as per PCI guidelines using a payment HSM? if yes, please help to add a seperate section for the technical requirements of payment HSM. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT HSM, supporting up to 1,000 TPS. Kindly confirm if this understanding is correct.	

Response to the Pre-Bid Queries

11 10	Volume II	Page 98: 5.2.4.8.3 Other Security Requirements c) Data at Rest	1. The SI shall ensure that the data at rest, which is stored other than in the hardened application or database production systems, is protected by encryption that is consistent with recommendations from DoP /other Government agencies and NIST/SANS/OWASP.	Industry best practices and NIST/OWASP recommendations for data-at-rest encryption require not only the application of cryptographic algorithms, but also secure generation, storage, lifecycle management, access control, and rotation of encryption keys. Without a centralized and secure Key Management System (KMS), encryption implementations become fragmented, difficult to audit, and may not meet compliance expectations of Government / DoP frameworks for critical data protection. Kindly confirm whether the intent of the above clause includes deployment of a centralized enterprise Key Management Solution to ensure: - Cryptographic key generation, storage, and lifecycle management - Key rotation and revocation policies - Separation of roles and access controls - Auditability of cryptographic operations - Secure integration with applications, storage, virtualization, and cloud platforms - Compliance with NIST recommendations for key management. please help to add a	Refer #804

Response to the Pre-Bid Queries

				seperate section for the technical requirements of Key Management Solution. Our understanding is that DOP intends to deploy an HA configuration across both DC and DR, along with a separate UAT KMS. Kindly confirm if this understanding is correct. Please also confirm the number of servers and databases that fall within the scope of this requirement.	

Response to the Pre-Bid Queries

11 11	Volume II	Annexure N; DAM, Point # 8	The solution should support rich analytics and provide options to view activities on a specific databases, activities from a specific user, activities on sensitive content etc.	Please confirm whether DOP is expecting a Database Risk Analytics mechanism that provides behavioral analytics, user risk profiling, threat indicators, compliance reporting, and incident investigation capabilities.	Refer #805

Response to the Pre-Bid Queries

11 12	Volume II	Annexure N; DAM, Point # 1	The solutions should provide customisable policies using algorithms as well as algorithmic validators wherever possible to discover and classify sensitive records in MySQL.	Our understanding is that DOP have 2 core 36 on-prem MS SQL databases, and there are no other databases. Considering the expansion, please confirm if the number of databases can go up to 100?	Refer #428

Response to the Pre-Bid Queries

11 13	Volume II	Annexure N; DAM, Point # 11	The solution should be able to integrate with the existing Data Activity Monitoring and Governance solution into a consolidated dashboard.	Our understanding is that the existing DAM solution is from Thales/Imperva, please confirm if this understanding is correct.	Refer #56

Response to the Pre-Bid Queries

11 14	Annexure J, EMS	Annexure J, EMS	2. EMS must provide Server Performance and Database Activity Monitoring.	Server Performance Monitoring is a standard and integral component of an EMS solution. However, Database Activity Monitoring (DAM) is typically offered as a separate and specialized security/compliance tool, and is not a native or standard capability of EMS platforms. Therefore, we request the authority to kindly remove Database Activity Monitoring from the EMS specifications, or consider it as an optional / separate requirement, to enable wider participation and ensure alignment with industry-standard EMS capabilities.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

11 15	Annexure J, EMS	Annexure J, EMS	12. EMS should support containerised deployment (Docker/Kubernetes).	While containerised deployment using Docker/Kubernetes is one of the modern architectural approaches, it is not mandatory for all EMS deployments, especially where a proven monolithic architecture is already in place and is capable of efficiently handling the required scale, performance, and availability of EMS modules. Mandating containerisation as a compulsory requirement may unnecessarily restrict participation of OEMs whose solutions are stable, scalable, and widely deployed using non-containerised architectures. We therefore request the authority to kindly remove this clause or make Docker/Kubernetes support optional. Additionally, we request further clarification on the specific use-cases or operational requirements (such as dynamic scaling, microservices-based isolation, or cloud-native deployment) that necessitate containerisation, so that OEMs can align their solutions accordingly.	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 16	Annexure J, EMS	Annexure J, EMS	13. EMS must provide a single-pane-of-glass KPI dashboard, FIPS 140-2 compliant.	While a single-pane-of-glass KPI dashboard is a standard and acceptable EMS requirement, mandating FIPS 140-2 compliance as a compulsory criterion is highly restrictive and effectively limits participation to a small set of foreign OEMs. FIPS 140-2 is a U.S. federal cryptographic module validation standard. Requiring it as the sole acceptable certification may unnecessarily exclude reputed Indian OEMs that comply with equivalent or internationally accepted security standards (such as ISO/IEC 27001, Common Criteria, or CERT-In–empanelled cryptographic implementations). As per DPIIT's Public Procurement (Preference to Make in India) Order and GFR-2017, procuring entities are encouraged to avoid technical specifications that restrict competition or discriminate against domestic suppliers when equivalent standards can meet the intended security objectives. In view of the above, we respectfully request the authority to kindly remove the mandatory FIPS 140-2 requirement from Clause 13, or alternatively, allow equivalent internationally	Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

				recognized or India-accepted security certifications, thereby enabling wider participation of compliant Indian OEMs in alignment with Make in India / Atmanirbhar Bharat objectives.	

Response to the Pre-Bid Queries

11 17	Annexure J, EMS	Annexure J, EMS	20. EMS must monitor popular Microservice platforms (Docker/Kubernetes) and applications inside containers.	Monitoring of Docker/Kubernetes-based microservices and containerized applications is applicable primarily in environments where such platforms are actively deployed in production. However, not all EMS use-cases mandate container or microservices-based architectures, and many enterprises continue to operate stable monolithic or VM-based application landscapes. Making container and in-container application monitoring a mandatory EMS requirement may unnecessarily restrict participation of OEMs whose solutions are designed for and successfully deployed in non-containerized environments, while still fully meeting the EMS objectives of performance, availability, and fault monitoring. We therefore respectfully request the authority to kindly make Clause 20 optional, or clarify the specific deployment scenarios or use-cases where Docker/Kubernetes monitoring is required. This will ensure technical relevance, avoid restrictive specifications, and enable wider participation of qualified OEMs, including Indian OEMs.	Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 18	Annexure J, EMS	Annexure J, EMS	30. NMS must support zero-touch automation via APIs, integration with NetDevOps (GitHub), and scheduled/ad-hoc scans.	The capabilities mentioned in Clause 30—such as zero-touch automation, workflow orchestration via APIs, NetDevOps integration (e.g., GitHub), and change-driven automation—are typically associated with IT Service Management (ITSM) or DevOps toolchains, rather than a core Network Management System (NMS). A standard NMS primarily focuses on network discovery, topology mapping, fault monitoring, performance monitoring, and alerting, whereas automation pipelines, version control integration, and policy-driven change workflows fall outside its traditional and essential scope. Therefore, we respectfully request the authority to kindly remove Clause 30 from the NMS specifications, or alternatively, reclassify these requirements under ITSM / NetDevOps modules or make them optional, to ensure alignment with industry-standard NMS functionality and enable wider OEM participation.	Refer #116

Response to the Pre-Bid Queries

11 19	Annexure J, EMS	Annexure J, EMS	39. DAM must monitor multiple database types (Oracle, Postgres, MySQL, SAP, Hadoop, etc.), support agent/agentless modes, and provide audit trails of user activity.	Database Activity Monitoring (DAM) is a specialized database security and compliance solution, typically deployed as a standalone product and not as part of a conventional Enterprise Monitoring System (EMS). EMS solutions primarily focus on infrastructure, server, network, and application performance monitoring, whereas DAM involves deep packet inspection, database-level auditing, privileged user tracking, and compliance reporting, which fall outside the core scope of EMS. Therefore, we respectfully request the authority to kindly remove Clause 39 related to DAM from the EMS specifications, or alternatively, specify DAM as a separate and optional solution, to ensure technical alignment with industry standards and enable wider OEM participation.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

11 20	Annexure J, EMS	Annexure J, EMS	40. DAM must support policy enforcement, threat detection, integration with SIEM/SOAR, playbooks, abnormal activity detection, user-to-data tracking, and compliance reporting.	The functionalities mentioned under Clause 40—including policy enforcement, threat detection, SIEM/SOAR integration, automated playbooks, abnormal behavior analytics, user-to-data tracking, and compliance reporting—are characteristic of advanced Database Activity Monitoring (DAM) and Database Security platforms. These capabilities extend beyond the scope of a standard Enterprise Monitoring System (EMS), which is primarily designed for performance, availability, and health monitoring of IT infrastructure and applications. Incorporating such security and compliance-centric features within EMS specifications may unnecessarily restrict participation to a limited set of OEMs. Therefore, we respectfully request the authority to kindly remove Clause 40 related to DAM from the EMS specifications, or alternatively, define DAM as a separate and optional solution to ensure alignment with industry practices and facilitate wider participation.	Clause is omitted. Bidders may refer to Corrigendum Annexure J for updated details of the requirements.

Response to the Pre-Bid Queries

11 21	Annexure N, Appln Performance Monitoring	Annexure N, Appln Performance Monitoring	Solution Architecture to address Gartner's 5 dimensions of Application Performance Management (end user experience monitoring, architecture discovery modelling and display, transaction profiling, deep-dive monitoring, analytics) while being part of Gartner's Leader Magic quadrant	The requirement to explicitly align with Gartner's defined APM dimensions and to be positioned in Gartner's Leader Magic Quadrant is a brand- and analyst-specific qualification, which is typically applicable to a limited number of large, predominantly foreign OEMs. Such a condition may inadvertently restrict participation of capable Indian OEMs, even when they technically meet or exceed the functional requirements, and may not be fully aligned with the objectives of Make in India (MII) and Atmanirbhar Bharat initiatives. We therefore respectfully request the authority to kindly remove references to Gartner Magic Quadrant positioning from the specifications and instead evaluate solutions based on objective, measurable technical and functional capabilities, thereby enabling wider participation of compliant Indian OEMs in line with MII guidelines.	Clause is omitted. Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

11 22	III	1.5.5 Liquidated Damages	Liquidated damages will be capped at 10% of the Total Contract Value (TCV).	Bidder proposes "The implementation phases penalty shall be capped to 10% of the delayed/affected implementation charges and will exclude price of application software, hardware, OS, Database, tools and peripheral applications"	As per RFP

Response to the Pre-Bid Queries

11 23	III	1.5.2 SLA Penalties	SLA section given in Vol-2 of the RFP. For the avoidance of doubt, it is expressly clarified that the DoP will calculate a financial sum and debit the same against the terms of payment as set out in Schedule IV of this Agreement as a result of the failure of the SI to meet the Timelines and/or Service Level	Bidder Proposes: The SLA/Penalties applicable shall be capped at 10% of the monthly invoice value.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 24	III	1.12.1 Payment Terms	payment shall be made within 60 working days of receipt of invoice along with supporting documents	Bidder Proposes: "Payments are due from date of receipt of invoice and payable within thirty (30) days of date of invoice. In the event of late payments, IBM reserves the right to charge a late payment fee @ 2% per month on the overdue amounts, in addition to the right of suspension of services, till the overdue amounts are paid."	As per RFP

Response to the Pre-Bid Queries

11 25	III	Billing Term		Bidder Proposes: HW Supply – 100% on Shipment SW Lic One time Supply – 100 % on Delivery (If Yearly subscription then billing is Yearly In Advance); AMS, Other Services and O&M – Quarterly In Advance HW AMC/ SW S&S – Yearly In Advance For Implementation milestones assess against project plan and Milestone Based – 100% on completion (Gap between milestones should be with in 45 days). If milestone Gap is >45days.. Please introduce additional milestones	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 26	III	1.15.3 Force Majeure	DoP may terminate the Contract / Agreement, by giving a written notice of minimum 30 (Thirty) days to SI, if as a result of Force Majeure the SI is unable to perform a material portion of the Service(s) for a period of more than 60 (Sixty) days. Notwithstanding such termination, the SI shall remain responsible for complying with its obligations under the Exit Management provisions of this Agreement.	In the event of force majeure IBM should be paid for all the work delivered up to the date of Force Majeure.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 27	III	1.13.3 Termination for cause	DoP may terminate the Agreement in full by giving the SI up to 30 days' prior written notice, if not cured, DoP can terminate and invoke other remedies (e.g., risk purchase, PBG invocation, indemnities)	Bidder Proposes : Notice period of min 30 days for cause and 180 days convenience Preferred position is that no T4C is allowed until end of Yr2. Termination charge should cover: All the work delivered up to the date of termination. Un-amortized investment (balance sheet cost), and reimbursable vendor expenses. Applicable wind down charges (subject to delivery team's assessment) in the event of termination for convenience. Termination fees (5% of remaining TCV) in the event of termination for convenience.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 28	III	1.13.4 Termination for Convenience	DoP may, by written notice of 60 (sixty) days sent to the SI, terminate the Agreement, in whole at any time for its convenience		Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 29	III	1.12.2 (b) Uncapped dispute withholding	DoP shall be entitled to delay or withhold payment... disputed/withheld amount shall be settled in accordance with Governance Schedule	Bidder proposes "Any amounts withheld must be addressed through the Dispute Resolution process. The total withheld amount shall not exceed the equivalent of two months' average billing. IBM reserves the right to suspend services or terminate the agreement in the event of non-payment of a disputed amount."	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 30	III	1.14.4 Risk Purchase Clause/ Step In	DoP reserves the right to procure same or equivalent services/Deliverables from alternative sources at the SI's risk and responsibility... incremental cost... limited to 1.5 times the amount payable	Bidder Proposes :This additional expenditure regarding defaulted service shall be subject to a maximum incremental charge of 5% of the amount paid or payable if the defaulted service were procured from the Bidder. This claim shall be payable if the Parties have failed to reach a resolution as per the governance process stated in the relevant clause of the agreement."	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 31	III	1.14.6 Risk Purchase Clause/ Step In	DoP reserves the right to step in and procure equivalent services... SI shall provide full access to project sites, systems, data, DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding 15 days) for rectification.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 32	III	1.2 Audit	DoP reserves the right to inspect and monitor... conduct routine and ad-hoc audits... security audit once each year at SI cost	Bidder is not obligated to share any information relating to Bidder's costs, Bidder proprietary data, confidential information of Bidder's other customers and internal audit reports of the Bidder.	As per RFP

Response to the Pre-Bid Queries

11 33		Sch II Assignment	SI shall not assign its rights and obligations without prior written consent of DoP... DoP may assign or novate	Assignment of the Contractor's rights to receive payments or assignment by the Contractor in conjunction with the sale of the portion of Contractor's business that includes the product or services is not restricted."	As per RFP

Response to the Pre-Bid Queries

11 34	III	1.19.1 Standard	The warranty period shall commence from the date of Go-live of the Project (as defined in Volume 2 of the RFP) and shall extend for as follows: Components Period Standard Hardware 6 months post completion of this Agreement COTS Software 6 months post completion of this Agreement Bespoke Software 6 months post completion of this Agreement	How will bidder extend warranty for additional 6 months post completion of the agreement	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 35	III	1.19.1 Standard	The warranty period shall commence from the date of Go-live of the Project (as defined in Volume 2 of the RFP) and shall extend for as follows: Components Period Standard Hardware 6 months post completion of this Agreement COTS Software 6 months post completion of this Agreement Bespoke Software 6 months post completion of this Agreement	Hardware ,COTS software OEM provide warranty period of minimum 12 months. Suggestion to extend from 6 months duration to 12 months for factoring the warranty as per industry standard.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 36	II	5.2.4.7 Testing	The SI is required to address various testing aspects through an external testing agency	Is there a pool of testing agencies which shall be contacted?	CERT-In empanelled and STQC-empanelled testing agency.

Response to the Pre-Bid Queries

11 37	II	5.4.2 Capacity Building	Master Trainers - Users who are responsible for training the end users - 2000	Please provide break up of Master trainers for application to prepare training BoQ	As per RFP

Response to the Pre-Bid Queries

11 38	III	1.14.6 Step-In-rights	the DoP reserves the right to step in and procure equivalent services or deliverables from alternate sources at the SI's risk and cost. Any additional expenses incurred shall be recoverable from pending dues, the Performance Bank Guarantee, or through legal process. DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding 15 days) for rectification	We propose to increase the rectification duration should be increased to 60-90 days. 15 days is well below the industry standards.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 39	II	Page Number - 5 Clause Number - 3 , 4 , 5	This RFP includes statements that reflect various assumptions and assessments arrived at by the DoP concerning the project. Such assumptions, assessments, and statements do not purport to contain all the information that each Bidder may require. The assumptions, assessments, statements and information contained in this RFP may not be complete, accurate, adequate, or correct. Each Bidder should, therefore, conduct their investigations and analysis and should check the accuracy, adequacy, correctness, reliability, and completeness of the assumptions, assessments, and information contained in this RFP and obtain independent advice from appropriate sources. 4) Information provided in this RFP to the Bidders is on a wide range of matters, some of which depend upon the interpretation of the law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. 5) DoP accepts no responsibility for the accuracy or otherwise of any interpretation or opinion on the law expressed herein. DoP, its employees, and its advisers make no representation or warrants and shall have no	For any bidder to solution and table the techno commercial proposal it is important to define the requirements/scope . So we request you to kindly confirm your requirements as binding document for the proposal	As per RFP

Response to the Pre-Bid Queries

			liability to any person including any Bidders under any law, statute, rules, regulations, tort, principles of restitution, unjust enrichment, or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this selection process		

Response to the Pre-Bid Queries

11 40	II	Page Number - 11 Clause Number - 2.2	DoP invites Request for Proposal (RFP) from System Integrators who have qualified through the EoI process. The term of the contract shall be for 5 years, extendable by 1 year + 1 year (i.e., up to 2 additional years) at DoP's discretion, on a year-to-year basis on the same terms and conditions. For any extension period beyond the initial 5 years, the O&M & Enhancement cost shall remain the same as that of the 5th year.	Please note that all OEMs provide binding quotes only for contract duration and there is no possibility of offering Y6 & Y7 prices at Y5 price because of inflation. To meet the above ASK Sis will be force to upfront load the bid which will not be beneficial for DoP. So we restrict to bind the commercials on fixed duration for which contract is signed .	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 41	II	Page Number - 67 Clause Number - 12	The contract tenure for the site will commence after acceptance of the site by DoP	The contract start shall be date from award of contract only , please clarify	As per RFP

Response to the Pre-Bid Queries

11 42	II	Page Number - 81 Clause Number - 13	The SI is required to showcase adaptability in addressing dynamic sizing needs, aligning seamlessly with POSB's growth. Additionally, the SI is obligated to consider a minimum of 20% Year-on-Year growth in infrastructure to accommodate the future projections. It is expected that the SI acknowledges POSB's discretionary authority to procure the necessary delta sizing as required. If the quota for the current year is surpassed before the year-end, the subsequent year will commence, and the SI is required to make provisions to accommodate the required delta sizing. The SI is further required to present a comprehensive plan detailing how they intend to scale the infrastructure to meet the specified growth rate.	We request you to please provide yearly volumetrics for each application along with guidance around peak load utilization so that solution is proposed accordingly. Providing 20% YoY infrastructure will not serve any purpose as corresponding license components wont be solutioned and it may result in oversizing	Refer #889

Response to the Pre-Bid Queries

11 43	II	Page Number - 15 Clause Number - 4	The solution is operational in over 25,000 branches under an on-premises licensing model.	Please share the branches projections where DoP wants to expand the operations	As per RFP

Response to the Pre-Bid Queries

11 44	II	Page Number - 15 Clause Number - 4	DoP focuses primarily on Retail Banking and Clearing & Payments, covering both back-office and front-office functions. Finacle core banking solution integrates with other external systems (NACH/ NPCI/ IPPB, etc.) to provide numerous services offered within the post office.	Request to please provide details of all systems where CBS is integrated with along with expected future systems where integration may be required.	As per RFP

Response to the Pre-Bid Queries

11 45	II	Page Number - 20 Clause Number - 5	Detailed Scope of Work	For is to define architecture for DoP IT 2.0 , it is essential for us to understand your existing technology environment & challenges experienced (operations , regulatory) . We request if you could take us through your current IT landscape— core platforms, integrations, data flows, and architectural considerations. It will be prudent if a common workshop can be conducted for all system integrator. Also as it will entails particiaption from various competencies / SMEs across applications , infrastructure , security , data center facility request to please allow at least 12 colleagues participating the workshop.	As per RFP

Response to the Pre-Bid Queries

11 46	II	Page Number - 23 Clause Number - 5.1.1	Figure II : Existing Contract (s) Timeline (April 2026 onwards)	With bid submission timelines of FEB'26 and 6 months bid validity , DoP will have right to sign contract by Aug'26. Since DoP has prevailing support contracts with OEMs & DCF so we request DoP to confirm that all support services will be made available for Phase 1 of delivery .	Refer #361

Response to the Pre-Bid Queries

11 47	II	Page Number - 39 Clause Number - 5.1.4.1	Core Banking Solution - Current Usage and Licensing Responsibility	We request DoP to consider buying license directly as that will help department to buy it optimally & have competitive participation	Refer #454

Response to the Pre-Bid Queries

11 48	I and III	Section 2.2(2), Page 16, Vol 1	"The bidders shall also ensure that all its employees and agents and sub-contractors involved in the Project, execute individual non-disclosure agreements as per Form A 22, which have been duly approved by DoP. Copy of such individual NDAs to be provided to DoP by the SI as and when demanded."	The individual NDA by employees and subcontractors seems to be mentioned as one of the formats to be filled in as part of submission. Request to remove the same as it is not feasible to obtain the same at the time of submission.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

11 49		Section 2.23(b), Page 34, Vol 1	The Sub-contractors shall submit the signed individual non-disclosure agreement (NDA) as per Form A.22.		As per RFP

Response to the Pre-Bid Queries

11 50		Section 5.1(d)(23), Page 57, Vol 1	d. Proposal Checklist:	In any case, we are liable for the acts of the employees and subcontractors and hence, this is not required.	As per RFP

Response to the Pre-Bid Queries

11 51		And Section 1.16.1, Page 36 of Vol III	Individual NDA	Request that employees and sub-contractors not be required to individually sign confidentiality agreements with DOP. We request that NDAs between SI and such employees and subcontractors on substantially similar terms be considered adequate.	As per RFP

Response to the Pre-Bid Queries

11 52			iv. The SI shall ... shall ensure that all its employees and agents and sub-contractors involved in the Project, execute individual non-disclosure agreements, which have been duly approved by the DoP concerning this Project. Copy of such Non-Disclosure Agreements to be provided to DoP by SI as and when demanded		As per RFP

Response to the Pre-Bid Queries

11 53	I	Section 2.8.3(j), Page 23	iv. In case of a successful Bidder, if the Bidder fails to sign the Agreement per the terms and conditions (including timelines for execution of the Agreement) of this RFP or fails to furnish the Performance Bank Guarantee per the terms and conditions (including timelines for furnishing PBG) of this RFP.	We request that EMD forfeiture be exercised only in event of material breach or willful refusal to execute Agreement, and not for delays due to good faith negotiations. Disputes regarding forfeiture shall be resolved per dispute resolution mechanism in the Agreement.	As per RFP

Response to the Pre-Bid Queries

11 54		Section 4.3(a),(c) Page 51	vii. The decision of the DoP regarding the forfeiture of the EMD shall be final and binding on the Bidders and shall not be called upon in question under any circumstances.	Further, we understand that in invoking forfeiture, DOP shall apply the principles of natural justice and equity and provide Bidder the reasons for the same. Disputes regarding forfeiture shall be resolved per dispute resolution mechanism in the Agreement	As per RFP

Response to the Pre-Bid Queries

11 55		If the contract is not executed within 21 days, their bid may be held as non- responsive and liable for rejection as per the discretion of DoP.		As per RFP

Response to the Pre-Bid Queries

11 56			If the successful bidder fails to execute the Contract or furnish the PBG within the stipulated time period (or such other extended timelines as agreed by the DoP in its sole discretion), the DoP shall have the right to forfeit the EMD of the successful bidder and award the work to the next successful bidder		As per RFP

Response to the Pre-Bid Queries

11 57	I	Sect 5.17, Form A17, Sec 4, Page 93	SECTION 4 – COMPENSATION FOR DAMAGES (1) If the Principal has disqualified the SI(s) from the bid process before the award according to SECTION 3, the principal is entitled to demand and recover the damages equivalent to Earnest Money Deposit/ Bid Security. (2) If the Principal has terminated the contract according to SECTION 3, or if the principal is entitled to terminate the contract according to SECTION 3, the principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee	The right to discontinue/terminate the Services, and any forfeiture of EMD/PBG shall be exercised only as a last resort in the event of material breach of IBM's obligations for reasons solely attributable to IBM, provided IBM has not remedied such breach within a reasonable period of time, and there are no other contractual remedies agreed in the Contract for the same.	As per RFP

Response to the Pre-Bid Queries

11 58					As per RFP

Response to the Pre-Bid Queries

11 59					As per RFP

Response to the Pre-Bid Queries

11 60		Section 4.4(b)(vii)(viii)(ix), Page 52, 53	ix. PBG may be invoked by DoP in the following non-exhaustive events: (i) If the successful Bidder fails to meet the overall penalty condition as mentioned in the RFP or any changes agreed between the parties.		As per RFP

Response to the Pre-Bid Queries

11 61					As per RFP

Response to the Pre-Bid Queries

11 62					As per RFP

Response to the Pre-Bid Queries

11 63	

		As per RFP

Response to the Pre-Bid Queries

11 64	I	Section 2.8.4(f), Page 24	"In case of conflict between provisions of the Portal with the RFP Document, provisions of the Portal shall prevail"	We understand the Portal here refers to any updated versions of this RFP or Corrigendum which may be uploaded on the Portal and not any other extraneous terms of the portal Terms of use, etc.	As per section 1.1.5 (Priority of Documents) of Volume 3

Response to the Pre-Bid Queries

11 65	I	Section 2.11(b), Page 27	If any such change causes an increase or decrease in the cost of, or the time required for the Bidder's performance of any part of the work under the Contract, whether changed or not changed by the order, an equitable adjustment shall be made in the Contract Value or time schedule, or both, as decided by the committee and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause must be asserted within thirty (30) days from the date of the Bidder's receipt of the DoP's changed order	Request that any change be made effective upon execution of a Change order.	As per RFP

Response to the Pre-Bid Queries

11 66	I	Section 2.23(c), Page 34	It is clarified that the Bidder shall be the principal employer for all claims arising from the liabilities statutory or otherwise, concerning the sub-contractors. The Bidder undertakes to indemnify the DoP or its nominated agencies against any claims arising from the approved list of services that are subcontracted, as stated above.	We understand the liability and indemnity here refers to those employment-related claims that are solely within SI's control and responsibility as the employer. Request to modify as follows:	As per RFP

Response to the Pre-Bid Queries

11 67				The Bidder undertakes to indemnify <u>by defending</u> the DoP ~~or its nominated agencies~~ against any <u>employment-related</u> claims ~~arising from the approved list of services that are subcontracted, as stated above~~ <u>that are solely within SI's control and responsibility as the employer</u>	As per RFP

Response to the Pre-Bid Queries

11 68		Section 5.2.1.2.7, Page 66	5.2.1.2.7 Quality Control, Testing, Inspection & Audit		As per RFP

Response to the Pre-Bid Queries

11 69			5.2.1.2.9 Right to Visit		As per RFP

Response to the Pre-Bid Queries

11 70		Section 5.2.1.2.9, Page 69			As per RFP

Response to the Pre-Bid Queries

11 71	I	Section 4.6(a), Page 53	Any information disclosed or obtained from Bidder during the proposal shall remain strictly confidential except in the situations where disclosure is: a. necessary in the process of assessing tenders, or where DoP discloses all or part to any of its advisers and consultants or where DoP publishes in its business papers, or any such publication as may be required and permitted by law;	Please clarify for what purposes will the information be required to be published by DOP in business papers? We would request to modify as follows: Any information disclosed or obtained from Bidder during the proposal shall remain strictly confidential except in the situations where disclosure is: a. necessary in the process of assessing tenders, or where DoP discloses all or part to any of its advisers and consultants or where DoP publishes in its business papers, or any such publication as may be required and permitted by law;	As per RFP

Response to the Pre-Bid Queries

11 72					As per RFP

Response to the Pre-Bid Queries

11 73					As per RFP

Response to the Pre-Bid Queries

11 74					As per RFP

Response to the Pre-Bid Queries

11 75	I	Section 5.1(d)(12), Page 56	D Proposal Checklist 12 N/A Disclosure of Court Cases	Request to remove this requirement. It may not be possible to provide the details of any and all actions that may have been instituted against the Bidder, as Bidder being a large organization may be involved in a variety of ongoing claims, demands, suits, investigations, and proceedings that arise from time to time in the ordinary course of its business. We would be happy to confirm that, to the best of its knowledge as on date, there are no such pending proceedings against Bidder which if determined against Bidder, would adversely affect Bidder's ability to perform the services under the RFP	As per RFP

Response to the Pre-Bid Queries

11 76					As per RFP

Response to the Pre-Bid Queries

11 77		Section 5.7, Form A.7, page 66			As per RFP

Response to the Pre-Bid Queries

11 78					As per RFP

Response to the Pre-Bid Queries

11 79	I	Section 5.3, Form A.3, Page 62	We agree to abide by the conditions outlined in this RFP.	We understand that our agreement to the terms of the RFP shall be read with our proposal if awarded to us.	As per RFP

Response to the Pre-Bid Queries

11 80	I	Section 5.4, Form A.4, page 62	c) is having an unblemished record and is not declared ineligible/blacklisted for corrupt & fraudulent practices either indefinitely or for a particular period by any State/ Central Government/ PSU/ UT as on date of RFP submission.	The reference to 'unblemished' is very broad. Request to limit this declaration to not being declared ineligible/blacklisted.	As per RFP

Response to the Pre-Bid Queries

11 81	I	Section 5.6, Form A.6, Page 65	I/We also confirm that there are no potential elements (timeframe for service delivery, resource, financial or other) that would adversely impact our ability to complete the requirements as given in the RFP.	This statement does not relate to subject matter of this undertaking. This statement is from the perspective of performance of the Services, which is already a part of terms of the RFP. Therefore, this will not be applicable here. Also, request to delete indemnification as that is also the subject matter of the agreement should contract be awarded.	As per RFP

Response to the Pre-Bid Queries

11 82			We undertake and agree to indemnify and hold Department of Posts harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees and fees of professionals, reasonably) by Department of Posts and/or its representatives, if any such conflict arises later		As per RFP

Response to the Pre-Bid Queries

11 83	I	Section 5.11, Form A.11, Page 76	We hereby confirm that the assumptions mentioned in our Approach & Methodology document submitted as part of the bid proposal will not become the basis for Change Request.	Note that every project will be subject to certain baseline assumptions and methodology. DOP is free to determine if those are as per DOP requirement and the RFP, but if we are awarded the project, then it is not reasonable to state that the agreed assumptions if not met will not require change request. Please delete this clause or modify to state that only if it is deviating from the scope of the RFP, will such assumptions not be the basis for Change request.	As per RFP

Response to the Pre-Bid Queries

11 84	I	Section 5.17, Form A.17, Sec 6 Page 93,	In the case of Subcontracting, the Principal Contractor shall take responsibility for the adoption of the Integrity Pact by the Subcontractor	Request to remove this requirement. Note that integrity pact is a requirement as per GFRs and not a requirement between private entities. We will anyways be liable for the acts of the subcontracts if they lead to violation of the integrity pact that we will sign	As per RFP

Response to the Pre-Bid Queries

11 85	I	Section 5.21, Form A.21, Section IV, page 102	IV. The Recipient acknowledges that during the course of the provision of Services by the Recipient, there shall be an exchange of information, discussions, deliberations, negotiations, etc. amongst the Parties and in performance of their obligations mentioned herein, there will be a significant flow of ideas, information, strategy, technical data/ information from the DoP to the Recipient.	Request to clarify that for any information to be subject to the obligations herein, such information should be either marked or identified or be reasonably be understood to be confidential or sensitive in a manner that its disclosure will be prejudicial to the safety or interests of DoP or the Government of India, as Bidder will not be in a position to judge that for DOP's information. Bidder also seeks to confirm that we will not be provided with any trade secret or personal information.	As per RFP

Response to the Pre-Bid Queries

11 86		Section 5.21, Form A.21, sec 1.1, 1.1(d), Page 102, 103	1.1 "Confidential Information" shall mean all confidential and proprietary information (whether in written, oral, electronic or other format) of DoP which includes but is not limited to:		As per RFP

Response to the Pre-Bid Queries

11 87			d. Any other information provided by DoP to the Recipient or procured by the Recipient from DoP shall be treated as Confidential Information under this clause irrespective of the fact whether the same is designated or earmarked as "Confidential"/ "Restricted" etc. or not by DoP; or even if the same is unclassified.		As per RFP

Response to the Pre-Bid Queries

11 88		Section 5.21, Form A.21, Section 2.2, Page 104	2.2 The Recipient further agrees not to divulge any Confidential Information or not to do any act or divulge any information of any nature whatsoever which shall be prejudicial to the safety or interests of DoP or the Government of India including but not limited to those mentioned herein below:		As per RFP

Response to the Pre-Bid Queries

11 89		Section 5.21, Form A.21, sec 1.1(c), Page 103	c. all other information and material of DoP relating to the method of development/deployment, construction, manufacturing, operation, size, specification, quantity, use and service of equipment and components supplied to or used by DoP, intellectual property including, but not limited to reports, process data, test data, performance data, inventions, trade secrets, systems software, object codes, source codes, copyrighted matters, methods, drawings, computation, calculations, computer program narration, flow charts, and all documentation therefore and all the components which might form part of confidential information and might be disclosed.		As per RFP

Response to the Pre-Bid Queries

11 90		Section 5.21, Form A.21, sec 1.1(e), Page 103	e. Confidential Information may also include the Personal and Sensitive Personal Data of DoP's/ other DoP clients, licensors, alliances, contractors and advisors		As per RFP

Response to the Pre-Bid Queries

11 91	I	Section 5.21, Form A.21, Section V, Page 102	V. Recipient hereby agrees and undertakes that any sub-contracting of the services (governed by this agreement) shall only with prior and express written permission of the DoP and that the Recipient shall execute a separate Confidentiality and Non-Disclosure Agreement with the firm/ all the employees involved in the subcontracted delivery of Services under this Agreement.	We understand that Bidder executing NDA on substantially similar terms with its subcontractor and employees shall suffice.	As per RFP

Response to the Pre-Bid Queries

11 92	I	Section 5.21, Form A.21, sec 2.1(e), Page 104	the non-disclosure obligation of the Recipient under this Agreement shall apply during and after the termination of the Agreement unless and until released in writing by DoP after the expiry of the Master Service Agreement, the Recipient agrees that all conditions and obligations imposed under this Agreement apply during the time that the Recipient has access to Confidential Information and at all times thereafter.	We request that confidentiality obligations survive for a reasonable period (3-5 years) after initial disclosure, rather than indefinitely	As per RFP

Response to the Pre-Bid Queries

11 93	I	Section 5.21, Form A.21, sec 3.7, Page 106	3.7. The Recipient shall restrict its discussions or negotiations with any third party during the term of this Agreement except with prior written permission of DoP.	Request to delete or modify this requirement, as this puts a restriction on Bidder to interact with any third parties even if it may not have any impact on our performance or may not lead to disclosure of DOP CI, or may not be conflict of interest.	As per RFP

Response to the Pre-Bid Queries

11 94	I	Section 5.21, Form A.21, sec 5.1, Page 107	5.1 Interpretation: The interpretation of DoP concerning the provisions of this Agreement shall be accepted by the Recipient and if dissatisfied with the interpretation, the Recipient can appeal to the DoP. Any legal remedy available to the Recipient under the laws of India shall only be resorted to after all in-house mechanisms of redressal at DoP have been exhausted	Request that any interpretation related dispute be resolved as per mutual dispute resolution process.	As per RFP

Response to the Pre-Bid Queries

11 95	I	Section 5.21, Form A.21, sec 5.3, Page 107	5.3 Indemnification: The Recipient agrees to indemnify and hold DoP harmless for any cost, damage, losses, penalty and/or liability or claims incurred by or made against DoP due to any breach, non-observance, failure or any other act leading to breach or omissions on part of the Recipient in the performance of this Agreement.	Request to delete this clause as part of the Format NDA as this is anyways part of the RFP and shall apply if we are awarded the contract.	As per RFP

Response to the Pre-Bid Queries

11 96				Alternatively, we understand if this applies, it refers to misuse or misappropriation of the Confidential Information	As per RFP

Response to the Pre-Bid Queries

11 97	I	Section 5, Page 15	Implement robust security measures in line with RBI, CERT-In, and other regulatory body guidelines including DPDP.	Bidder requests following clarification:	As per RFP

Response to the Pre-Bid Queries

11 98		Section 5.1.2.2, Page 25		Bidder will comply with all applicable laws that are applicable to it as an IT Service Provider. However, if DOP wants the Bidder to implement measures as per applicable laws/regulations or policies that are applicable to DOP, DOP shall specify the same as part of the scope and specifications along with related changes to the Bidder. In case there is an additional cost attached to such compliance, the parties should agree to the cost as per the change request.	As per RFP

Response to the Pre-Bid Queries

11 99			This transition shall be carried out in alignment with business continuity principles, regulatory compliance, and operational stability		As per RFP

Response to the Pre-Bid Queries

12 00		Section 5.1.4(ii), Page 33, 37			As per RFP

Response to the Pre-Bid Queries

12 01			e. The SI shall perform all the changes/modifications/updates /enhancements and customisations in the system that are required to comply with any statutory/regulatory requirement or any industry-wide changes. The SI shall be responsible for managing, customisation, scripting, integrating development and patch deployment for Core Banking, Delivery Channels and allied applications.		As per RFP

Response to the Pre-Bid Queries

12 02		Section 5.1.4.1, Page 40	g. Monitor, maintain, support (including OEM Support) and customise the existing interfaces, modules/ sub-modules, reports, etc. Perform customisation/ changes, including but not limited to Core Banking, Mobile Banking and Internet Banking Applications as per directives from DoP/RBI/NPCI/MoF/GOI from time to time related to Banking operations performed at designated Post Offices,		As per RFP

Response to the Pre-Bid Queries

12 03			including existing and upcoming integrations with CTS Platform, NPCI, etc., for clearing related activities.		As per RFP

Response to the Pre-Bid Queries

12 04		Section 5.1.5.1, Section C(4), Page 46			As per RFP

Response to the Pre-Bid Queries

12 05			Any interface required as per Regulatory and statutory requirements (RBI, SEBI, IBA, FIU, MoF, DoP, UIDAI, Government of India, etc) from time to time shall be provided by SI at no additional cost to DoP. The SI shall also be responsible for maintaining these interfaces throughout the contract period.		As per RFP

Response to the Pre-Bid Queries

12 06		Section 5.2.1.2.3, Page 62	Ensure compliance with all applicable regulatory, security, and audit requirements during license renewal, transition, or procurement, including adherence to OEM guidelines and industry standards		As per RFP

Response to the Pre-Bid Queries

12 07					As per RFP

Response to the Pre-Bid Queries

12 08			5. Maintaining strict adherence to regulatory and security standards applicable to infrastructure operations and reporting.		As per RFP

Response to the Pre-Bid Queries

12 09			The SI should comply with DoP's policies and guidelines in key areas relevant to the RFP. Some of the key areas are as under:		As per RFP

Response to the Pre-Bid Queries

12 10					As per RFP

Response to the Pre-Bid Queries

12			In this phase, the SI shall assume lead responsibility for managing the application and infrastructure components in accordance with the defined scope of work, while the outgoing vendor(s) shall remain in a shadow role to provide support.		As per RFP
11					

Response to the Pre-Bid Queries

12			a. The SI shall be fully accountable for the delivery of all operational and project-related activities, including bug-fixing, incident resolution, etc.		As per RFP
12					

Response to the Pre-Bid Queries

12 13			b. The SI may seek clarifications from the outgoing vendor(s) during this phase on a need basis. However, accountability for service continuity, SLA adherence, and deliverable quality shall rest entirely with the SI.		As per RFP

Response to the Pre-Bid Queries

12 14			c. The SI shall ensure alignment of all workstreams with the functional and strategic objectives of the Department.		As per RFP

Response to the Pre-Bid Queries

12 15	I	Section 5.1.4(i), Page 33	The detailed BOQ of existing licenses are mentioned in Annexure C of this RFP. If any additional licenses are required to meet the solution requirements of this RFP, the SI shall bring them and include them in its proposal. DoP will not pay for any additional licenses that are needed but not included by the SI in its proposal. These licenses shall be made available by SI during the contract duration to DoP at no additional cost. All licenses must be in the name of DoP.	We understand that Bidder's winning proposal shall form the basis of the final list of BOQ and scope considered for the price proposed by the Bidder	As per RFP

Response to the Pre-Bid Queries

12 16			The POSB IT Systems shall continue to operate from the current infrastructure during this period. The SI shall ensure uninterrupted business continuity, performance, security, and regulatory compliance during this time.		As per RFP

Response to the Pre-Bid Queries

12 17			6. The lease should not affect the hosting services. In case of disruption of services that arise due to any change in facility ownership or disruption due to the lease of the facility, below shall apply:		As per RFP

Response to the Pre-Bid Queries

12 18			a. DoP shall have the right to terminate the contract due to service disruption.		As per RFP

Response to the Pre-Bid Queries

12 19			b. All costs, including any relocation, damage during transportation, cost of insurance, cost of reactivation of services, cost of new/additional equipment required to reactivate the services, etc., shall be borne by SI.		As per RFP

Response to the Pre-Bid Queries

12 20	I	Section 5.2.1.1.1 (5), Page 52	c. All consequential costs, including loss to business and any other such cost, shall be borne by the SI. Without any prejudice, such cost shall be determined by DoP and shall be final.	Request to delete. Neither party is liable for any consequential costs or losses.	As per RFP

Response to the Pre-Bid Queries

12 21	I	Section 5.2.1.2.11, Page 70	5.2.1.2.11 E-Waste Management 2022 During the whole contract period: • The SI shall facilitate DoP in compliance with the E-Waste (Management) Rules, 2022, including all subsequent amendments and notifications issued by the Government of India. • The System Integrator shall maintain all necessary documentation, records, and reports for e-waste management activities and provide periodic updates to the Department and relevant regulatory authorities as required. • The System Integrator shall assist the Department in implementing all obligations under the Rules, including but not limited to: ○ Collection, segregation, storage, transportation, dismantling, refurbishment, recycling, and environmentally sound disposal of e-waste generated from the Department's operations. ○ Filing of timely quarterly and annual returns related to e-waste management as stipulated in the Rules (if any).	Unclear on the requirement of this clause. If such laws apply to Bidder, we will comply. However, if these are flowing from anything that applies to DOP, we will implement the same as part of the scope as specified by DOP, at mutually agreed cost (if there is cost implications due to such implementation). However, DOP shall remain responsible to assess the applicability and requirements of the laws that apply to DOP	As per RFP

Response to the Pre-Bid Queries

12 22			5.2.1.2.11 E-Waste Management 2022		As per RFP

Response to the Pre-Bid Queries

12 23			During the whole contract period:		As per RFP

Response to the Pre-Bid Queries

12 24			• The SI shall facilitate DoP in compliance with the E-Waste (Management) Rules, 2022, including all subsequent amendments and notifications issued by the Government of India.		As per RFP

Response to the Pre-Bid Queries

12 25			• The System Integrator shall maintain all necessary documentation, records, and reports for e-waste management activities and provide periodic updates to the Department and relevant regulatory authorities as required.		As per RFP

Response to the Pre-Bid Queries

12 26			• The System Integrator shall assist the Department in implementing all obligations under the Rules, including but not limited to:		As per RFP

Response to the Pre-Bid Queries

12 27			O Collection, segregation, storage, transportation, dismantling, refurbishment, recycling, and environmentally sound disposal of e-waste generated from the Department's operations.		As per RFP

Response to the Pre-Bid Queries

12 28			O Filing of timely quarterly and annual returns related to e-waste management as stipulated in the Rules (if any).		As per RFP

Response to the Pre-Bid Queries

12 29			2. Insurance shall be valid for the entire movement duration.		As per RFP

Response to the Pre-Bid Queries

12 30			3. DoP will provide the equipment value for insurance purposes and reimburse the premium on actuals.		As per RFP

Response to the Pre-Bid Queries

12 31			4. The SI shall be responsible for coordinating this activity and ensuring that valid insurance documentation is submitted to DoP before the commencement of asset movement.		As per RFP

Response to the Pre-Bid Queries

12 32	I	Section 5.2.4.1 (1), Page 86	Throughout the procurement lifecycle, including vendor negotiations, contract agreements, and service level agreements, the SI must ensure DoP has complete visibility and control. DoP reserves the right to approve or reject any proposed design or provisioning decision made by the SI, ensuring alignment with POSB's strategic objectives and budget constraints.	Note that procurement process is internal to the Bidder and is also confidential. We will not be able to provide full visibility and control to DOP. Having said that Bidder is responsible and liable for the acts of the subcontractors.	As per RFP

Response to the Pre-Bid Queries

12 33	I, II	Section 5.2.4.1 (4), Page 86, 87 of Vol I	4. The SI is required to ensure that every element of hardware items and software (inclusive of the OS and any other software provided under this contract) falls within the coverage of a comprehensive warranty/AMC/ATS, excluding consumables. Should there be any disparity between POSB's requirements and the OEM warranty/AMC/ATS, the SI is obligated to bridge the gap without imposing any additional cost on POSB.	Any hardware assets, software assets and product licenses from OEMs will be transferred directly from the OEM to DOP and are provided solely as per applicable OEM terms (including warranty, licensing, guarantee etc)	As per RFP

Response to the Pre-Bid Queries

12 34			7. The SI is required to guarantee that the hardware provided to DoP, including all components and attachments, is entirely new, of genuine make, and devoid of any manufacturing defects.		As per RFP

Response to the Pre-Bid Queries

12 35		Section 10.1, Pages 192-193 of Vol II			As per RFP

Response to the Pre-Bid Queries

12 36			• All licenses shall be in the name of DoP and must be perpetual wherever applicable.		As per RFP

Response to the Pre-Bid Queries

12 37			• The SI shall ensure compliance with OEM terms and avoid any legal or commercial risk to DoP.		As per RFP

Response to the Pre-Bid Queries

12 38			• All license management, compliance, and audit activities shall be properly documented and made available to DoP on demand.		As per RFP

Response to the Pre-Bid Queries

12 39			• All licenses shall comply with applicable Government of India procurement policies and shall be fully auditable for license compliance		As per RFP

Response to the Pre-Bid Queries

12 40	II	Section 5.2.4.1 (12), Page 87	12. The SI is required to ensure that the goods supplied under the contract have extensive insurance coverage, safeguarding against loss or damage throughout transportation, storage, implementation, and maintenance phases.	Note that SI shall be able to procure insurance for the goods (itself or through OEM) until the time the title is transferred to DOP.	As per RFP

Response to the Pre-Bid Queries

12 41	II	Section 5.2.4.1 (21), Page 88, Section 5.2.4.5, (2), Page 92, Section 5.2.4.8.2, Page 98(6)(7),	21. ... ensure that the proposed security framework for the network conforms to the guidelines set by the Reserve Bank of India (RBI).	Bidder requests following clarification:	As per RFP

Response to the Pre-Bid Queries

12 42		Section 5.2.4.8.3,(d)(1) Page99,		Bidder will comply with all applicable laws that are applicable to it as an IT Service Provider. However, if DOP wants the Bidder to implement measures as per applicable laws/regulations or policies that are applicable to DOP, DOP shall specify the same as part of the scope and specifications along with related changes to the Bidder. In case there is an additional cost attached to such compliance, the parties should agree to the cost as per the change request.	As per RFP

Response to the Pre-Bid Queries

12 43		Section 5.2.5, Page 105	2.... adhere to all security policies provided by DoP.		As per RFP

Response to the Pre-Bid Queries

12 44		Section 5.2.5.1, Page 106,			As per RFP

Response to the Pre-Bid Queries

12 45		Section, 5.2.5.3(1)(2), Page 108	6. ...adhere to applicable standards and policies on Open Application Programming Interfaces (APIs) and Policy on Adoption of Open-Source Software published by the Government of India authorities, such as CERT-IN, MeitY, etc.		As per RFP

Response to the Pre-Bid Queries

12 46			7. ... ensure that the applications comply with DoP Information security standards/policies/procedures, Information Technology Act and other national & international regulatory and best practices standards (ISO, NIST, PCI-DSS, etc.) at all stages of SDLC. And they should pass any related audit (internal or external) without any risk or findings.		As per RFP

Response to the Pre-Bid Queries

12 47		Section 5.2.5.5 (3), Page 110			As per RFP

Response to the Pre-Bid Queries

12 48			d) API Security		As per RFP

Response to the Pre-Bid Queries

12 49		Section 5.2.5.6 (2), Page 111	... in accordance with industry acceptable standards (e.g., OWASP, ISO 27001, etc.) and adhere to applicable legal, statutory, or regulatory compliance obligations of the DoP.		As per RFP

Response to the Pre-Bid Queries

12 50		Section 5.2.5.8(6), Page 115			As per RFP

Response to the Pre-Bid Queries

12 51		Section 12.1(12), Page 206	• ... ensure periodic updates and enhancements to maintain compliance with evolving regulatory requirements and industry standards and shall support DoP during internal and external audits by providing all necessary documentation, reports, and evidentiary artefacts.		As per RFP

Response to the Pre-Bid Queries

12 52		Annexure D, Page240			As per RFP

Response to the Pre-Bid Queries

12 53			• Adherence to the IT Act 2000/2008/2010 and subsequent amendments, including maker-checker functionalities for manual interventions.		As per RFP

Response to the Pre-Bid Queries

12 54		Annexure E (3), Page 248			As per RFP

Response to the Pre-Bid Queries

12 55		Annexure E (4), Page 249	. Compliance and Security Standards		As per RFP

Response to the Pre-Bid Queries

12 56			• Adherence to national cybersecurity standards and protocols for UPI, card safety, internet banking, and mobile banking.		As per RFP

Response to the Pre-Bid Queries

12 57					As per RFP

Response to the Pre-Bid Queries

12 58			• Ensuring compliance with data protection regulations.		As per RFP

Response to the Pre-Bid Queries

12 59					As per RFP

Response to the Pre-Bid Queries

12 60			3. Security and Compliance		As per RFP

Response to the Pre-Bid Queries

12 61			• Adherence to UIDAI, NPCI & other Govt Ministries/Bodies standards.		As per RFP

Response to the Pre-Bid Queries

12 62			• Compliance with AePS transaction limits, data privacy regulations and cybersecurity frameworks.		As per RFP

Response to the Pre-Bid Queries

12 63			• Full compliance with Indian cyber laws, Aadhaar Act provisions, and NPCI guidelines.		As per RFP

Response to the Pre-Bid Queries

12 64					As per RFP

Response to the Pre-Bid Queries

12 65			2. Security and Compliance		As per RFP

Response to the Pre-Bid Queries

12 66			• Adherence to regional, local, and industry API security standards (e.g., RBI, ISO 27001, PCI DSS, where applicable)		As per RFP

Response to the Pre-Bid Queries

12 67					As per RFP

Response to the Pre-Bid Queries

12 68			6. Regulatory Compliance:		As per RFP

Response to the Pre-Bid Queries

12 69			• Ensure complete adherence to relevant regulatory guidelines, including those issued by the Reserve Bank of India (RBI), CERT-In (Indian Computer Emergency Response Team), and other applicable Government bodies.		As per RFP

Response to the Pre-Bid Queries

12 70			• Maintain audit trails, data privacy protections, and compliance reporting as mandated.		As per RFP

Response to the Pre-Bid Queries

12 71					As per RFP

Response to the Pre-Bid Queries

12 72			12. The SI shall comply with all POSB-specific operational requirements, as well as any statutory, regulatory, or audit guidelines applicable during the reverse transition period, and shall provide all necessary assistance to ensure compliance continuity.		As per RFP

Response to the Pre-Bid Queries

12 73					As per RFP

Response to the Pre-Bid Queries

12 74			... be responsible for providing security patches/upgrades on an ongoing basis to comply with the regulatory requirements and security standards for uninterrupted services of the application. All the regulatory/statutory guidelines released by regulators related to risk, compliance must be complied with, implemented and supported during the entire contract period.		As per RFP

Response to the Pre-Bid Queries

12 75					As per RFP

Response to the Pre-Bid Queries

12 76			3. Mandatory Compliances		As per RFP

Response to the Pre-Bid Queries

12 77			... need to comply with all the present and future provisions of the DoP's Information Security Policy/ NPCI Guidelines/ RBI Guidelines, Respective Govt. Agencies and provide such regulatory requirements at no additional cost to DoP during the contract period. The Solution may be audited by PMLA/ any other Regulatory Authority, and any observation pointed out by these bodies must be complied with by the vendor within the timelines stipulated by the regulatory agencies, without any additional cost to DoP.		As per RFP

Response to the Pre-Bid Queries

12 78					As per RFP

Response to the Pre-Bid Queries

12 79			The offered solution shall be subjected to DoP's audit (VAPT, EAPT, IS Audit, etc.) through off-site and on-site scrutiny at any time/periodically during the contract period. The auditors may be internal/ external. The system should have an Audit Log for all Admin and user operations and should be capable of keeping an Audit trail as per DoP policy. The vendor should provide a solution and implementation for all the audit points raised by DoP's internal/ external team during the contract period, within the stipulated timelines, without any extra cost.		As per RFP

Response to the Pre-Bid Queries

12 80			Alignment with watchlist guidelines and regulatory requirements under:		As per RFP

Response to the Pre-Bid Queries

12 81			▪ a) WMD Act, 2005		As per RFP

Response to the Pre-Bid Queries

12 82			▪ b) UAPA, 1967		As per RFP

Response to the Pre-Bid Queries

12 83			▪ c) UNSCR Mandates		As per RFP

Response to the Pre-Bid Queries

12 84			▪ d) Internal Watchlist and PEP (Politically Exposed Person)		As per RFP

Response to the Pre-Bid Queries

12 85			• The solution must be fully compliant with the Prevention of Money Laundering Act (PMLA), 2002, including all amendments notified from time to time.		As per RFP

Response to the Pre-Bid Queries

12 86	II	Section 5.5, Page 126	5.5 Escrow Management	Please clarify the expectations from Bidder with respect to the existing escrow agreement. We are not a party to the same, hence Bidder expects no responsibility with respect to the same.	An existing escrow arrangement is currently in place. Post completion of the transition phase, the selected bidder shall ensure continuity and compliance with the escrow requirements, either through extension of the existing arrangement or establishment of an appropriate new agreement, as applicable.

Response to the Pre-Bid Queries

12 87			The Department has already entered an escrow arrangement with an existing Service Provider for Finacle Core Banking Solution, which shall remain valid and operational until its scheduled expiry in the year 2027 ("Existing Escrow Agreement").		An existing escrow arrangement is currently in place. Post completion of the transition phase, the selected bidder shall ensure continuity and compliance with the escrow requirements, either through extension of the existing arrangement or establishment of an appropriate new agreement, as applicable.

Response to the Pre-Bid Queries

12 88	II	Section 6.6, Page 134	• In the event of a Service Failure, penalties shall be imposed on the SI, in accordance with the penalty calculation framework specified herein.	Request to clarify that SLA penalty shall apply solely if the default is attributable to the Bidder.	SLA penalty shall apply if the default is attributable to the SI.

Response to the Pre-Bid Queries

12 89			• The SI shall be exempted from any delays or slippages on SLA parameters arising out of the following reasons:		SLA penalty shall apply if the default is attributable to the SI.

Response to the Pre-Bid Queries

12 90			O The non-compliance with the SLA arising solely from events classified as Force Majeure or reasons beyond the reasonable control of the SI, subject to timely notification and approval by DoP as per the Force Majeure clause detailed in the RFP.	Also request to specify a maximum cumulative cap on penalty .	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

12 91	II	Section 6.8.4, Notes, Page 173	4. In case of default on any of the service level metrics, the SI shall submit a performance improvement plan along with the root cause analysis for DoP's approval.	We understands this applies where such default is attributable to the Bidder	In case of default on any of the service level metrics, the SI shall submit a performance improvement plan along with the root cause analysis for DoP's approval. However, SLA for service failure shall not be applicable if it is not attributed to the SI.

Response to the Pre-Bid Queries

12 92		Section 6.10.2, Page 175	6.10.2 Remedial Clause		As per RFP

Response to the Pre-Bid Queries

12 93			In case of any deficiencies or failures during the DR drills, the SI shall promptly initiate corrective actions and re-conduct the DR drill at no additional cost to DoP within a time mutually agreed upon.		As per RFP

Response to the Pre-Bid Queries

12 94	II	Section 7(6), Page 178	6. DoP retains the right to request discontinuation of subcontracting of activities at any time during the contract period, and such activities will have to be performed by the SI directly or by a subcontracting agency acceptable to DoP.	Note that while we shall make good faith efforts to have such contract with the DOP chosen subcontracting agency, however, the same shall be subject to Bidder's ethics and subcontracting policies and subject to successful negotiation of contract with such subcontractor. Failure of the same shall not result in imposition of liabilities or penalties/LDs etc. on the Bidder since the subcontractor is chosen by DOP	As per RFP

Response to the Pre-Bid Queries

12 95	II	Section 11, Page 195, 196	Milestone -based payments shall be released upon successful completion of each activity/milestone and submission of requisite documentation, including but not limited to acceptance certificates, completion reports, OEM warranties (where applicable), and invoice(s) duly certified by the Department.	We understand verified here refers to the invoice which has been raised as per the payment milestone and completion criteria/acceptance criteria agreed.	As per RFP

Response to the Pre-Bid Queries

12 96			• Payment release after acceptance is within 60 working days upon verified invoice submission.		As per RFP

Response to the Pre-Bid Queries

12 97	III	Section 1.1.1, Page 5	Applicable Law(s)	We understand that "Applicable Law" and Bidder's obligation to comply with laws, in the context of the Bidder shall mean only those laws as are applicable to it in the ordinary course of its business as an information technology services provider.	As per RFP

Response to the Pre-Bid Queries

12 98			means laws of India and shall include any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project.		As per RFP

Response to the Pre-Bid Queries

12 99		Section 1.6.1(k), Page 17	k) It has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may harm its ability to perform its obligations under this Agreement;		As per RFP

Response to the Pre-Bid Queries

13 00			o) The System Integrator ("SI") represents and warrants that it is, and shall at all times during the term of this Agreement remain, in full compliance with all applicable laws, statutes, rules, regulations, and ordinances, including but not limited to the Workmen Compensation Act, applicable Labour Laws, the Digital Personal Data Protection Act, 2023 ("DPDP Act"), and any other laws, rules, or regulations applicable to the performance of its obligations under this Agreement, each as amended from time to time		As per RFP

Response to the Pre-Bid Queries

13 01					As per RFP

Response to the Pre-Bid Queries

13 02		Section 1.6.1(o), Page 17	The SI shall comply with the provision of all laws including the Digital Personal Data Protection Act, 2023, labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the DoP shall be applicable in the performance of this Agreement and the SI shall abide by these laws.		As per RFP

Response to the Pre-Bid Queries

13 03			The SI shall also adhere to all security requirement/regulations of the DoP during the execution of the work.		As per RFP

Response to the Pre-Bid Queries

13 04			e) ensure that the Assets that are under the control of the SI, are kept suitably housed and in conformity with Applicable Law and terms agreed with DoP;		As per RFP

Response to the Pre-Bid Queries

13 05			not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to Applicable Law and as per terms agreed with DoP.		As per RFP

Response to the Pre-Bid Queries

13 06		Section 1.22.9(a), Page 48	1.11.3 Security and Safety		As per RFP

Response to the Pre-Bid Queries

13 07		Section 1.9(e), (g), Page 20	a) The SI shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Act, Digital Personal Data Protection Act, 2023 or any other Applicable Law (as amended from time to time), Information Security Management System (ISMS) and Cyber Crisis Management Plan (CCMP) of DoP, guidelines issued by CERT-IN from time to time and follow the industry standards related to safety and security (including those as specified by DoP from time to time), insofar as it applies to the provision of the Services or Deliverables under this Agreement.		As per RFP

Response to the Pre-Bid Queries

13 08		Section 1.11.3(a), Page21	b) The SI shall also comply with DoP or the Government of India security standards and policies in force from time to time at each location of which DoP or its nominated agencies make SI aware in writing in so far as the same apply to the provision of the Deliverables and the Services.		As per RFP

Response to the Pre-Bid Queries

13 09	III	Section 1.1.1, Page 6	Confidential Information	Request to clarify that for any information to be subject to the obligations herein, such information should be either marked or identified or be reasonably be understood to be confidential or sensitive in a manner that its disclosure will be prejudicial to the safety or interests of DoP or the Government of India, as Bidder will not be in a position to judge that for DOP's information.	"Confidential Information" or "CI" means any information that: (a) is expressly marked or designated as "Confidential" at the time of disclosure; or (b) if disclosed orally or in any other non-written form, is identified as confidential at the time of disclosure and is subsequently confirmed in writing as confidential within a reasonable period after such disclosure.

Response to the Pre-Bid Queries

13 10			means all information including Department of Post's Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, methodologies, technologies, intellectual property, Personal Data, Sensitive Personal Data, data, trade secrets, research and development, design rights, flow charts, diagrams, quality manuals, checklists, guidelines, know-how, plans, budgets, methods and procedures of operation, source code materials, specifications, programs, software packages, clients and suppliers, partners, principals, employees, consultants and authorized agents and any information which is of a manifestly confidential nature and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement);	Bidder also seeks to confirm that we will not be provided with any trade secret or personal information.	As per RFP

Response to the Pre-Bid Queries

13 11	III	Section 1.1.1, Page 8	Intellectual Property Rights or IPR	Request to remove 'Trade Secret' from the definition of IPR	As per RFP

Response to the Pre-Bid Queries

13 12			means any patent, designs and copyrights, trademark, trade name, trade secret, permit, service marks, brands, proprietary information, knowledge, technology, licenses, , inventions, utility models, databases, computer programs, software, know-how or other form of intellectual property right, title, benefits, interest, moral rights, rights in databases and Bespoke Software / Pre-existing work including its up-gradation systems and compilation rights (whether registered, registrable, applied for, or unregistered, and including renewals, extensions, continuations, and rights of action (past, present, or future)).		As per RFP

Response to the Pre-Bid Queries

13 13	III	Section 1.1.1, Page 9	Service Specifications	We understand that specifications shall refer to those which agreed and specified as part of scope in the Agreement as read with the proposal.	As per RFP

Response to the Pre-Bid Queries

13 14			means and includes detailed description, statements to technical data, performance characteristics, and standards (Indian as well as International) as applicable and as specified in the Agreement as well as those specifications relating to Industry standards and codes applicable to the performance of the Services and Scope of Work, work performance quality and the specifications affecting the Services and Deliverables or any additional specification required to be produced by the SI to meet its obligations under this Agreement.		As per RFP

Response to the Pre-Bid Queries

13 15	III	Section 1.1.1, Page 9	Required Consents	Request to clarify the usage of the term 'Required Consent'. The definition indicates that it refers to consent wrt any item that DOP makes available to SI.	As per RFP

Response to the Pre-Bid Queries

13 16			means the consents, waivers, clearances and licenses to use DoP's Intellectual Property Rights, rights and other authorizations as may be required to be obtained for the software and other items that DoP or its nominated agencies are required to make available to SI pursuant to this Agreement.	In which case, any obligations in Section 1.6.1 and 1.8 wrt Required Consent should reside with DOP and not Bidder.	As per RFP

Response to the Pre-Bid Queries

13 17		Section 1.6.1(n), Page 17	n) No representation or warranty by SI contained herein or in any other document furnished by it to DoP or its nominated agencies in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading		As per RFP

Response to the Pre-Bid Queries

13 18		Section 1.8(a), Page 19	The SI shall procure, maintain and observe all relevant and regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Required Consents") necessary for the SI to provide the Services. The costs of such Approvals shall be borne by SI		As per RFP

Response to the Pre-Bid Queries

13 19	III	Section 1.1.4(b)(c), Page 10	b) as between the provisions of this Agreement and the Schedules/Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the Agreement or the Schedules/Annexures; and	We understand that the agreement shall be mutually executed between the parties. Further, request that in case of conflict between RFP and Agreement read with Proposal, the terms of the mutually executed agreement read with proposal shall prevail.	As per RFP

Response to the Pre-Bid Queries

13 20			c) as between the provisions of the Agreement and any other volume of RFP and the Proposal, the Agreement shall prevail		As per RFP

Response to the Pre-Bid Queries

13 21	III	Section 1.2.3, Page 11	Without prejudice to the generality of clause 1.2.2 above, the SI is required to provide such services and support as DoP may deem proper and necessary, during the term of the Agreement, including all such processes and activities which are consistent with the Proposal, the RFP and this Agreement and are deemed necessary by DoP, in order to meet its business requirements (hereinafter 'Scope of Work' including the scope of work specified in Vol 2 of the RFP and clarification thereof, and Annexures thereof).	Request to clarify that scope shall be as set forth in the proposal.	As per RFP

Response to the Pre-Bid Queries

13 22	III	Section 1.3, Page 11	Term') extendable to a further period of 2 years, on an year to year basis, subject to a maximum of 2 years ("Extended Term") at the sole discretion of DoP, on the same terms and conditions.	We understand that this provision is an ability for DOP to seek extension. However, any extension shall be effective when executed by both parties as an amendment/CR	As per RFP

Response to the Pre-Bid Queries

13 23	III	Section 1.4.2(c), Page 12	c) Furnishing of such other documents , including the copy of sub-contracts, Non-Disclosure Agreement and any other documents as DoP may specify prior to the signing of this Agreement.	Request to delete this. Note that our subcontracts are confidential agreements and have sensitive and confidential information. Further, there may be multiple engagements we have with our subcontractors and hence, it is not possible for us to provide a copy of the subcontracts.	As per RFP

Response to the Pre-Bid Queries

13 24		Section 1.22.3(b)(c), Page 44	b. As provided in clause 1.22.3 (a) above, the SI shall immediately upon execution of the contract(s) to be entered into with such delegate/sub-contractor provide a copy of the same (without commercials) to the DoP within 15 days from the date of signing the Agreement and shall not review, amend, modify or terminate the terms of such contracts without the prior written consent of the DoP.		As per RFP

Response to the Pre-Bid Queries

13 25			c. Prior to executing any contract or entering into any contract or understanding with a sub-contractor, the SI shall ensure that each sub-contractor appointed by the SI executes a performance Undertaking and non-disclosure agreements as may be required. A copy of the detailed executed agreement with prices blanked shall be submitted to the DoP within 15 days from the date of signing the Agreement.		As per RFP

Response to the Pre-Bid Queries

13 26	III	Section 1.5(c), Page 13	The DoP reserves the right to amend any of the terms and conditions concerning the Agreement / Service Specifications and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the Scope of Work. If the suggested amendments or new directions require the SI to provide more resources, outside the agreed scope of work, the DoP shall bear mutually agreed additional expenses for the same.	Request that any change be made effective upon execution of a written PCR/amendment	As per RFP

Response to the Pre-Bid Queries

13 27	III	Section 1.5(e), Page 14	The Goods or services supplied under this Agreement shall confirm to the Standards mentioned in the technical specifications given in the RFP, and, when no applicable standard is mentioned, the standards issued by the concerned regulatory/controlling authority and incase no standards issued by regulatory body are available, the latest standards available in the concerned industry will be used as mutually agreed upon by the Parties.	Bidder understands that services shall be required to comply with the specifications expressly agreed. If there are standards issued by regulatory authorities which applies to DOP, DOP shall provide such requirement as part of specifications to the Bidder.	As per RFP

Response to the Pre-Bid Queries

13 28				OEM will be selected by bidder basis the specifications provided by the buyer, however, the warranty for such hardware and software of the OEM, shall be provided on standard OEM terms and conditions.	As per RFP

Response to the Pre-Bid Queries

13 29	III	Section 1.5.5, Page 15	If the SI fails to achieve the Timelines or the Service Levels due to reasons attributable to the SI, the SI shall be liable to pay liquidated damages as per Volume 2 of the RFP	We understand that LD is associated with delays, and Service level credits are separately mentioned in relation to the SLAs, and shall not be applied for delays for which LD applies.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

13 30	III	Section 1.5.5, Page 16	SI shall not be relieved from any obligations by payment of such liquidated damages and to perform the Services or from liability for continued default.	We understand that once the SI has paid liquidated damages for a specific delay or service level failure, the SI shall not be subject to further liquidated damages/liability for the same delay or failure. Payment of liquidated damages for a delay shall constitute DoP's sole and exclusive remedy for that specific delay, without prejudice to DoP's rights for any new or subsequent defaults, subject to the adjusted timeline to accommodate the delay for which LD have been paid.	As per RFP

Response to the Pre-Bid Queries

13 31				Request to add the following:	As per RFP

Response to the Pre-Bid Queries

13 32				<i>For the avoidance of doubt, payment of liquidated damages for a specific delay or service level failure shall constitute the sole remedy for that particular default, and the SI shall not be liable for additional penalties or liquidated damages arising from the same underlying delay or failure</i>	As per RFP

Response to the Pre-Bid Queries

13 33	III	Section 1.6.1, page 16	The SI represents and warrants to DoP, as of the date hereof, which represents and warranties shall survive the term and termination hereof, the following:	Request that any warranty with respect to the obligations to be performed within the duration of contract not survive the term and termination of the contract.	As per RFP

Response to the Pre-Bid Queries

13 34			e) In providing the Services, it shall use best endeavors not to cause any unnecessary disruption to DoP's normal business operations;		As per RFP

Response to the Pre-Bid Queries

13 35	III	Section 1.6.1(m), page 17	That SI shall ensure that all goods, software, systems, materials, processes, or products supplied, developed, or used by the SI in the performance of this Agreement are properly licensed or authorized and do not infringe or violate any third-party intellectual property rights, including but not limited to copyrights, patents, trademarks, trade secrets, or other proprietary rights. The SI shall obtain, at its own cost, all necessary permissions, approvals, and licenses for such use and shall ensure that all such items are free from any claims, titles, encumbrances, or liens. The SI shall indemnify and hold harmless the DoP from and against any and all losses, damages, or claims arising out of or in connection with any such infringement or alleged infringement;	Request to delete this or refer to Section 1.14.2 which already addresses IPR Indemnity and provides for detailed process as well.	As per RFP

Response to the Pre-Bid Queries

13 36	III	Section 1.9(b)(c)(d), Page 19, 20	b) keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) as at the date the SI takes control of and/or first uses the Assets and during the entire Term of the Agreement.	We understand that this refers to those Assets which are under the SI's direct physical custody and operational control until the title and risk is transferred to DOP	As per RFP

Response to the Pre-Bid Queries

13 37			c) ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and which are provided to the SI will be followed by the SI and any person who will be responsible for the use of the Assets;	The SI shall not be liable for deterioration, damage, or non-compliance arising from DoP's use, misuse, or modifications of Assets	As per RFP

Response to the Pre-Bid Queries

13 38			d) take such steps as may be properly recommended by the manufacturer of the Assets and notified to the SI or as may, in the reasonable opinion of the SI, be necessary to use the Assets in a safe manner;		As per RFP

Response to the Pre-Bid Queries

13 39					As per RFP

Response to the Pre-Bid Queries

13 40			c. In the event of the DoP noticing at any time that any amount has been disbursed wrongly to the SI or any other amount is due from the SI to the DoP, the DoP may without prejudice to its rights to recover such amounts by other means, after notifying the SI to deduct such amount from any payment falling due to the SI. The details of such recovery, if any, will be intimated to the SI. The SI shall receive the payment of the undisputed amount under the subsequent invoice for any amount that has been omitted in the previous invoice by mistake on the part of the DoP or the SI.		As per RFP

Response to the Pre-Bid Queries

13 41	III	Section 1.12.3(c), Page 24	c. The SI agrees to reimburse and hold the DoP or its nominated agencies harmless from and against any claims, losses, expenses (including third-party claims, attorney fees, court fees) etc. arising out of deficiency (including penalties and interest) in payment of taxes that are SI's or its subcontractor's responsibility	We understand that the indemnity here refers to SI's obligation to reimburse DOP any government-imposed fines or penalties imposed on DOP solely due to any violation of taxation law applicable to SI in its capacity as an IT services provider. Further, the indemnification process and conditions specified in Section 1.14.3 shall apply to any indemnity mentioned in this Agreement.	As per RFP

Response to the Pre-Bid Queries

13 42	III	Section 1.13.1(i), Page 25	The failure on the part of the SI to perform any of its obligations or comply with any of the terms of this Agreement shall constitute an Event of Default on the part of the SI.	Bidder understands that termination for cause may only be invoked where such Event of Default result in a material breach of the Contract which is not remedied by the SI within reasonable period of time.	As per RFP

Response to the Pre-Bid Queries

13 43		Section 1.13.3, Page 27	The DoP may terminate this Agreement in full, by giving the SI a prior and written notice of up to 30 days indicating its intention to terminate the Agreement under the following circumstances:		As per RFP

Response to the Pre-Bid Queries

13 44		Section 1.13.1(i)(c), Page 25	c. The SI or its team has failed to conform with any of the service specifications as set out in the RFP or this Agreement or has failed to adhere to any amended direction, modification or clarification as issued by the DoP during the term of this Agreement and which the DoP deems proper and necessary for the execution of the scope of work under this Agreement;	Bidder understands that scope shall be as specified in the proposal any modification shall be agreed by executing a PCR	As per RFP

Response to the Pre-Bid Queries

13 45	III	Section 1.13.2(i), Page 26	Where an Event of Default subsists or remains uncured, the DoP shall be entitled to:	Request to delete this clause. We are ok that any DOP may invoke termination for material breach of the contract, however, any recovery of damages or penalties or any other imposition of remediation actions, such as re-determination of consideration, suspension, offset etc. arising from such material breach should be addressed as per dispute resolution	As per RFP

Response to the Pre-Bid Queries

13 46			Impose any such obligations and conditions and issue any clarifications as may be necessary to, inter alia, ensure a smooth continuation and business continuity of the Services and the project which the SI shall be obliged to comply with, which may include unilateral re-determination of the consideration payable to the SI under this Agreement. The SI shall in addition take all available steps to minimize loss resulting from such event of default/breach		As per RFP

Response to the Pre-Bid Queries

13 47		Section 1.13.2(ii), Page 26	ii. Suspend all payments to the SI under the Agreement by written notice of suspension to the SI provided that such notice of suspension shall (a) specify the nature of failure, and (b) request the SI to remedy such failure within a specified period from the date of receipt of such notice of suspension by the SI.		As per RFP

Response to the Pre-Bid Queries

13 48		Section 1.13.2(iv), Page 27	iv. Retain such amounts from the payment due and payable by the DoP to the SI as may be required to offset any losses caused to the DoP as a result of such event of default and the SI shall compensate the DoP for any such loss, damages or other costs, incurred by the DoP in this regard. Nothing herein shall affect the continued obligation of the subcontractor/ other members of its team to perform all their obligations and responsibilities under this Agreement in an identical manner as were being performed before the occurrence of default.		As per RFP

Response to the Pre-Bid Queries

13 49		Section 1.13.2(v), Page 27	Nothing herein shall restrict the right of DoP to Invoke the Performance Bank Guarantee and other Guarantees furnished hereunder, enforce indemnity provisions, recover such other costs/losses and other amounts from the SI that may have resulted from such default and pursue such other rights and/or remedies that may be available to the DoP under law.		As per RFP

Response to the Pre-Bid Queries

13 50		Section 1.13.5(iii), Page28	Without prejudice to any other rights, the DoP may retain such amounts from the payment due and payable by the DoP to the SI as may be required to offset any losses caused to the DoP as a result of any act/omissions of the SI. In case of any loss or damage due to default on the part of the SI in performing any of its obligations concerning executing the scope of work under this Agreement, the SI shall compensate the DoP for any such loss, damages or other costs, incurred by the DoP		As per RFP

Response to the Pre-Bid Queries

13 51		Section 1.13.5(iv), Page28	iv. Nothing herein shall restrict the right of the DoP to invoke the Performance Bank Guarantee and other Guarantees furnished hereunder and pursue such other rights and/or remedies that may be available to the DoP under law.		As per RFP

Response to the Pre-Bid Queries

13 52			The DoP may, by written notice of 60 (sixty) days sent to the SI, terminate the Agreement, in whole at any time for its convenience. The notice of termination shall specify that termination is for the DoP's convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective.		As per RFP

Response to the Pre-Bid Queries

13 53			ii. If the termination of this Agreement is due to the expiry of the Term of this Agreement / a decision not to grant any (further) extension by the DoP, or where the termination is before the expiry of the stipulated term due to the occurrence of any Event of Default on the part of the SI, the SI herein shall be obliged to provide all such assistance to the successor SI or any other person as may be required and as the DoP may specify including training, where the successor(s) is a representative/personnel of the DoP to enable the successor to adequately provide the Services hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the Term/earlier termination hereof. Without prejudice to the foregoing, upon termination (or upon expiry of the Term) of this Agreement, the SI will comply with the Exit Management Schedule set out in Schedule III of this Agreement (and as revised from time to time).		As per RFP

Response to the Pre-Bid Queries

13 54			Where the SI's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against the SI, any failure by the SI to pay any of its dues to its creditors, the institution of any winding up proceedings against the SI or the happening of any such events that are adverse to the commercial viability of the SI, the DoP shall reserve the right to take any steps as may be necessary, to ensure the effective transition of the project to a successor SI, and to ensure business continuity provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the DoP.		As per RFP

Response to the Pre-Bid Queries

13 55	III	Section 1.13.5, Page29	The SI shall give prior/advance notice (at least 3 months) about occurrence of the such developments	Note that for any such corporate development, it is not possible for the entity to provide prior advance notice. Request to delete or specify that we will provide notice promptly without delay as per the corporate directions.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

13 56	III	NA	NA	There is no right for SI to terminate the contract for DOP's material breach or non-payment. Request to add: The SI may, without prejudice to any other rights or remedies, terminate this Agreement by written notice to the Department of Posts if the Department of Posts materially breaches any of its obligations under this Agreement and fails to cure such breach within a reasonable period of time, including for non-payment by the Department of Posts of any amount due under this Agreement when due.	As per RFP

Response to the Pre-Bid Queries

13 57				The SI may, without prejudice to any other rights or remedies, terminate this Agreement by written notice to the Department of Posts if the Department of Posts materially breaches any of its obligations under this Agreement and fails to cure such breach within a reasonable period of time, including for non-payment by the Department of Posts of any amount due under this Agreement when due.	As per RFP

Response to the Pre-Bid Queries

13 58	III	Section 1.14.1, Page 29	Subject to Clause 1.14.3 below, SI (the "Indemnifying Party") undertakes to indemnify DoP (the "Indemnified Party"), its officers, employees, agents, and representatives, from and against all claims (including third party claims), losses, liabilities, compensation, expenses (including reasonable attorneys' fees), fines, penalties, taxes, interest or damages etc. (Collectively "Loss") on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or willful default, lack of due care or breach of terms under this Agreement. The Indemnifying Party shall also indemnify Indemnified Party from and against all direct monetary losses, damages etc. arising out of any defect, fault, deficiency in the applications, software licenses, hardware and other components of the Project provided and/or maintained by the Indemnifying Party or any of its sub-contractors etc and breach of its confidential obligation and Data Protection obligation. Further, Indemnifying Party shall protect and fully indemnify and keep indemnified the Indemnified Party from all claims, damages	Request to modify as follows: Subject to Clause 1.14.3 below, SI (the "Indemnifying Party") undertakes to indemnify DoP (the "Indemnified Party"), its officers, employees, agents, and representatives, <u>by defending Indemnified Party</u> from and against ~~all claims (including by~~ third party ~~claims~~), losses, liabilities, compensation, expenses (including reasonable attorneys' fees), fines, penalties, taxes, interest or damages, <u>to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI etc.</u> (Collectively "Loss") on account of bodily injury, death or	As per RFP

Response to the Pre-Bid Queries

			or compensation for breach of any provisions of the Digital Personal Data Protection Act, 2023, and/or any other applicable data protection or privacy laws, as amended from time to time.	damage to tangible personal property arising in favor of any person, corporation or other entity (~~including the Indemnified Party~~) <u>proximately</u> attributable to the Indemnifying Party's negligence or willful default, lack of due care ~~or breach of terms under this Agreement~~. The Indemnifying Party shall also indemnify <u>by defending</u> Indemnified Party from and against <u>all third party claims for</u> direct monetary losses, damages etc. <u>to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI and</u> arising out of any defect, fault, deficiency in the applications, software licenses, hardware and ~~other components of~~	

Response to the Pre-Bid Queries

				the Project provided and/or maintained by the Indemnifying Party or any of its sub-contractors etc and <u>SI's misuse or misappropriation of DOP's data in breach of its confidential obligation and Data Protection obligation</u>	

Response to the Pre-Bid Queries

13 59			Further, Indemnifying Party shall protect and fully indemnify and keep indemnified the Indemnified Party from all claims, damages or compensation for breach of any provisions of the Digital Personal Data Protection Act, 2023, and/or any other applicable data protection or privacy laws, as amended from time to time.		As per RFP

Response to the Pre-Bid Queries

13 60				Subject to Clause 1.14.3 below, SI (the "Indemnifying Party") undertakes to indemnify DoP (the "Indemnified Party"), its officers, employees, agents, and representatives, <u>by defending Indemnified Party</u> from and against ~~all~~ claims ~~(including by third party claims)~~, losses, liabilities, compensation, expenses (including reasonable attorneys' fees), fines, penalties, taxes, interest or damages, <u>to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI</u> ~~etc.~~ (Collectively "Loss") on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity ~~(including the Indemnified Party)~~ <u>proximately</u> attributable to the Indemnifying Party's negligence or willful default, lack of due care ~~or breach of terms under this Agreement~~. The Indemnifying Party shall also indemnify <u>by defending</u> Indemnified Party from and against ~~all third party claims~~ <u>for direct monetary losses, damages etc. to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI and arising out of any defect, fault,</u>	As per RFP

Response to the Pre-Bid Queries

				deficiency in the applications, software licenses, hardware and other components of the Project provided and/or maintained by the Indemnifying Party or any of its sub-contractors etc and SI's misuse or misappropriation of DOP's data in breach of its confidential obligation and Data Protection obligation	

Response to the Pre-Bid Queries

13 61				Further, Indemnifying Party shall protect and fully indemnify and keep indemnified the Indemnified Party <u>by defending from all third party claims, damages or compensation, to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI to the extent arising from</u>~~for~~ breach of ~~any provisions of the Digital Personal Data Protection Act, 2023, and/or any other applicable~~ data protection or privacy laws, as amended from time to time, <u>as applicable to SI in its capacity as an IT service provider in connection with the performance of the Agreement with recovery limited solely to government-imposed fines or penalties</u>	As per RFP

Response to the Pre-Bid Queries

13 62	III	Section 1.14.2, Page 30	SI (Indemnifying Party) shall Indemnify, hold harmless, defend third-party claims against DoP (Indemnified Party) its directors, employees, agents and representatives from and against any costs, loss, damages, expense, claims, litigations, suits, actions, judgments, and or otherwise including but not limited to those from third parties or liabilities of any kind howsoever suffered, arising out of or incurred to infringement of Intellectual Property Rights including but not limited to patent, trademark, copy-rights or industrial drawings and designs arising from use of the Services/Deliverables or any part thereof and/or otherwise	Request to modify as follows: SI (Indemnifying Party) shall ~~Indemnify, hold harmless,~~ defend third-party claims against DoP (Indemnified Party) its directors, employees, agents and representatives from and against any costs, loss, damages, expense, claims, litigations, suits, actions, judgments, and or otherwise ~~including but not limited to those from third parties or liabilities of any kind howsoever suffered, to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI to the extent~~ arising out of or incurred to infringement of <u>registered</u> Intellectual Property Rights including but not limited to patent, trademark,	As per RFP

Response to the Pre-Bid Queries

				copy-rights or industrial drawings and designs arising from use of the Services/Deliverables or any part thereof and/or otherwise	

Response to the Pre-Bid Queries

13 63				SI (Indemnifying Party) shall ~~Indemnify, hold harmless,~~ defend third-party claims against DoP (Indemnified Party) its directors, employees, agents and representatives from and against any costs, loss, damages, expense, claims, litigations, suits, actions, judgments, and or otherwise ~~including but not limited to those from third parties or liabilities of any kind~~ <u>howsoever suffered, to the extent any of the foregoing are awarded by a court of competent jurisdiction or are included in a settlement approved by SI to the extent arising out of or incurred to infringement of registered</u> Intellectual Property Rights including but not limited to patent, trademark, copy-rights or industrial drawings and designs arising from use of the Services/Deliverables or any part thereof ~~and/or otherwise~~	As per RFP

Response to the Pre-Bid Queries

13 64	III	Section 1.14.2, Page 30	Further , the SI shall compensate DoP for the reasonable and duly documented replacement costs incurred by DoP for procuring equivalent Deliverables/Services from an alternate source. Under no circumstances shall DoP be liable to bear any expense, charge, fee, or cost of any nature whatsoever arising out of or in connection with such non-performance or replacement	Request to delete. SI is anyways indemnifying DOP and is also agreeing to replace or modify the affected services or deliverables and further agreeing to reimburse if we fail to do so..	As per RFP

Response to the Pre-Bid Queries

13 65			The provisions of this clause shall remain in effect and continue to be binding notwithstanding the termination or expiration of this Agreement		As per RFP

Response to the Pre-Bid Queries

13 66	III	Section 1.14.3, Page 31	iii. Notwithstanding anything contained herein, the SI and the DoP agree and covenant that a notice by the DoP to the SI concerning the claim as aforesaid shall amount to express acceptance and consent by the SI to indemnify the DoP for all losses concerning such claim. Upon notice by the SI, the DoP shall reasonably cooperate with the SI at the sole costs of the SI, only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the DoP. The DoP shall have the right, at its option, to participate in the defence of such claim;	Request to modify as follows:	As per RFP

Response to the Pre-Bid Queries

13 67				iii. Notwithstanding anything contained herein, the SI and the DoP agree and covenant that a notice by the DoP to the SI concerning the claim as aforesaid <u>for which SI has obligation to indemnify</u> shall amount to express acceptance and consent by the SI to indemnify the DoP <u>in accordance with the terms herein for all losses concerning such claim</u>. Upon notice by the SI, the DoP shall reasonably cooperate with the SI at the sole costs of the SI, ~~only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the DoP.~~ The DoP shall have the right, at its option, to participate in the defence of such claim <u>at its own cost</u>;	As per RFP

Response to the Pre-Bid Queries

13 68	III	Section 1.14.3, Page 31	If the SI does not assume control of the defence of such claims (as mentioned above), the entire defence, negotiation or settlement of such claim by the DoP shall be deemed to have been consented to by and shall be binding upon, SI as fully as though the SI alone had assumed the defence thereof and a judgement had been entered into by the SI, for such claim in respect of the settlement or judgement and the SI shall remain liable for and bound by the outcome of such proceedings or settlement.	We understand this refers to instances where SI refuses to take over the defence for claims for which SI has the obligation to indemnify.	As per RFP

Response to the Pre-Bid Queries

13 69	III	Section 1.14.4, Page 31	If the SI fails to perform its obligations (or any part thereof) under this Agreement or if the Agreement is terminated by the DoP due to breach of any obligations of the SI under this Agreement, DoP reserves the right to procure same or equivalent services/Deliverables from alternative sources at the SI's risk and responsibility. Any incremental cost borne by the DoP in procuring such services/ Deliverables shall be borne by the SI. Any such incremental cost incurred in the procurement of such services/ Deliverables from alternative source will be recovered from the undisputed pending due and payable payments / Performance Bank Guarantee provided by the SI under this Agreement and if the value of the services/Deliverables under risk purchase exceeds the amount of Performance Bank Guarantee, the same may be recovered, if necessary, by due legal process limited to 1.5 times the amount that was	Request that any such amounts payable be as agreed between the parties and within the liability cap of the agreement.	As per RFP

Response to the Pre-Bid Queries

13 70			payable to SI for non-delivered services/ deliverables.		As per RFP

Response to the Pre-Bid Queries

13 71			Notwithstanding anything to the contrary contained elsewhere in this Agreement, the rights and remedies of DoP under this clause, including recovery of incremental or replacement costs, shall prevail over any limitation of liability, indemnity cap, or any other clause restricting the SI's liability.		As per RFP

Response to the Pre-Bid Queries

13 72	III	Section 1.14.5 i Page32	i The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement	Since work includes implementation and maintenance phases which are largely recurring services, the cap be specified as amounts payable in the previous 12 months.	As per RFP

Response to the Pre-Bid Queries

13 73	III	Section 1.14.5 iii Page32	iii. Notwithstanding anything contained in the foregoing, the liability cap and exclusion for the SI given under this Clause shall not apply to the claims that are subject indemnification obligations set out in this Clause and breach of Clauses 1.11.3 (Security and Safety), 1.16 (Confidentiality) damages arising from the gross negligence or willful misconduct or fraud of SI, its employees and subcontractor, loss or unauthorized disclosure by SI, its personnel or contractors, of data of DoP or those of its customers, Non compliance of Regulatory or Statutory guidelines applicable to bank, provided such guidelines were brought to the notice of Service Provide and breach of Intellectual Property Rights of a third party.	Request to revise as follows:	As per RFP

Response to the Pre-Bid Queries

13 74				Notwithstanding anything contained in the foregoing, the liability cap and exclusion for the SI given under this Clause shall not apply to (i) the claims that are subject indemnification obligations set out in ~~this~~ Clause 1.14.2 for IPR infringement claims brought by third parties against DOP and breach of Clauses 1.11.3 (Security and Safety), 1.16 (Confidentiality) (ii) damages arising from the gross negligence or willful misconduct or fraud of SI, its employees and subcontractor, ~~loss or unauthorized disclosure~~ (iii) misuse or misappropriation by SI, its personnel or contractors, of data of DoP or those of its customers in breach of confidentiality obligations, (iv) government imposed fines or penalties incurred by DOP due to non compliance by SI of Regulatory or Statutory guidelines applicable to SI as an IT service provider (v) charges owed by DOP under the Agreement, as well as DOP's misappropriation of SIs intellectual property bank, provided such guidelines were brought to the notice of Service Provider and breach of Intellectual Property Rights of a third party.	As per RFP

Response to the Pre-Bid Queries

13 75	III	Section 1.14.6, Pages 33	1.14.6 Step-In-rights	Bidder understands that Step-in will only be exercised in instances of material failure by SI of a critical service.	As per RFP

Response to the Pre-Bid Queries

13 76			In the event of the SI's failure to perform its obligations or breach of the Agreement, the DoP reserves the right to step in and procure equivalent services or deliverables from alternate sources at the SI's risk and cost. Any additional expenses incurred shall be recoverable from pending dues, the Performance Bank Guarantee, or through legal process.		As per RFP

Response to the Pre-Bid Queries

13 77		DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding 15 days) for rectification. If the SI fails to remedy the default within the said period, DoP may exercise its step-in rights without further notice. Upon invocation of step-in, the SI shall provide DoP or its designated agency full access to project sites, systems, data, documentation, software, and any other resources reasonably required for continued delivery of services. The SI shall extend all cooperation and technical assistance to ensure smooth transition and continuity of operations. DoP shall have the right to use, for the duration of the step-in period, all project assets, equipment, tools, and licences (including third-party software licences, to the extent transferable or sublicensable) necessary for performance of services.	DOP's right to step-in shall be exercised only after providing a written notice to step-in, and SI retains control over unaffected services.	As per RFP

Response to the Pre-Bid Queries

13 78			Invocation of step-in rights shall not relieve the SI of its obligations, liabilities, or warranties under this Agreement, nor be construed as a waiver of any rights or remedies available to DoP.	Request to specify a maximum step-in period.	As per RFP

Response to the Pre-Bid Queries

13 79			During the step-in period, the SI shall continue to be responsible for ensuring data integrity, confidentiality, and compliance with all applicable information security and regulatory requirements until the Department confirms formal transition of such responsibilities.		As per RFP

Response to the Pre-Bid Queries

13 80		If the Department's step-in rights remain in effect for a continuous period exceeding sixty (60) days, or if in the Department's reasonable opinion, the SI is unable to resume satisfactory performance of the affected Services within such period, the Department shall have the right to terminate the Statement of Work (SOW) for which the step-in was invoked, without any liability or penalty. Upon such termination, the Department may permanently retain control of all project materials, data, systems, and deliverables related to the affected SOW and may engage any third party to continue or complete the Services at the risk and cost of the SI. Such termination of an SOW under this clause shall not prejudice the Department's rights to claim damages, invoke the Performance Bank Guarantee, or recover any losses incurred due to the SI's failure.	Request to add the following clarifications:	As per RFP

Response to the Pre-Bid Queries

13 81				As DOP assumes control and full responsibility (operational, financial, legal, and regulatory) for the stepped-in services during the period of control, SI should not be liable wrt such services which are under DOP control.	As per RFP

Response to the Pre-Bid Queries

13 82				DOP should continue to pay SI for all contracted services during the step-in period. The Client must also bear all costs of engaging and managing its substitute provider or if SI to bear such costs, they must be mutually agreed.	As per RFP

Response to the Pre-Bid Queries

13 83				Any DOP or substitute exercising step-in rights may only use SI's tools, processes, and data strictly for the purpose of maintaining continuity of services during the step-in period. Any SI confidential information, data, and materials, IP (if necessary and agreed) will only be shared subject to confidentiality obligations and solely for temporary operational use	As per RFP

Response to the Pre-Bid Queries

13 84				SI resumes services once it notifies DOP that the critical service failure has been remedied, in which case DOP must promptly step out and return control, unless it can demonstrate that the failure remains unresolved. DOP to cooperate with respect to any reintegration or stepping back in of the SI.	As per RFP

Response to the Pre-Bid Queries

13 85				Service credits, liquidated damages, or other contractual remedies shall not apply concurrently during the step-in period.	As per RFP

Response to the Pre-Bid Queries

13 86	III	Section 1.15.3, Page34	For the avoidance of doubt, it is expressly clarified that the failure on the part of the SI under this Agreement or the SLA to implement any disaster contingency planning and back-up and other data safeguards following the terms of this Agreement or the SLA against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event.	Bidder understands that these instances will not be deemed Force Majeure provided that these were not themselves prevented due to Force Majeure.	As per RFP

Response to the Pre-Bid Queries

13 87	III	Section 1.16.1, Page 36	iii. The DoP or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action against the SI regarding any forbidden disclosure. The DoP reserves the right to adopt legal proceedings, civil or criminal, against the SI concerning a dispute arising out of a breach of obligation by the SI under this clause.	We understand the right to take punitive action or adopt proceedings here refers to the right to seek legal remedies as available under applicable law and as per the dispute resolution process mentioned herein.	As per RFP

Response to the Pre-Bid Queries

13 88	III	Section 1.16.1, Page 36	The SI's personnel shall follow the DoP's Information Security policy and Cyber Crisis Management Plan or any other related policy or guideline issued from time to time.	Request to remove this requirement from Confidentiality clause. We are ok to comply with these policies to as applicable to the scope of work and are notified to us as part of specifications.	As per RFP

Response to the Pre-Bid Queries

13 89	III	Section 1.16.1, Page 37	The obligations under this Clause shall survive the expiry, cancellation, or termination of this Agreement and shall continue until such Confidential Information lawfully enters the public domain without any breach of this Agreement.	We request that confidentiality obligations survive for a reasonable period (3-5 years) after initial disclosure, rather than indefinitely	As per RFP

Response to the Pre-Bid Queries

13 90	III	Section 1.16.1, Page 37	It is understood that it would be impractical for the DoP to monitor all information made available to the SI under such circumstances or to provide notice to the SI of the confidentiality of all such information. Therefore, the SI agrees that any technical, business, or other information of the DoP that the SI's personnel, sub-contractors, or agents acquire while on the DoP's premises, or through access to the DoP's computer systems or databases while on or off the DoP's premises, shall be deemed Confidential Information	Request to clarify that such information should be either marked or identified or be reasonably be understood to be confidential	Confidential Information" or "CI" means any information that: (a) is expressly marked or designated as "Confidential" at the time of disclosure; or(b) if disclosed orally or in any other non-written form, is identified as confidential at the time of disclosure and is subsequently confirmed in writing as confidential within a reasonable period after such disclosure.

Response to the Pre-Bid Queries

13 91	III	Section 1.17, Page 37	1.17 Audit	Bidder understands that for any audit or inspection or request for information, the principles, terms and process of audit as specified in Volume III, Section 1.27(2), Page 60 shall be followed	As per RFP

Response to the Pre-Bid Queries

13 92			, Access and Reporting		As per RFP

Response to the Pre-Bid Queries

13 93			The DoP reserves the right to inspect and monitor/assess the progress of the Project at any time during the course of the Agreement, after providing due notice to the SI. The DoP may demand and upon such demand being made, the DoP shall be provided with any document, data, material or any other information which it may require, to enable it to assess the progress of the Project, systems, records, and personnel.	Any outcome of the audit shall be mutually agreed, basis which any rectification may be agreed to be implemented.	As per RFP

Response to the Pre-Bid Queries

13 94			ii. The DoP shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by the SI of its obligations/functions following the standards committed to or required by the DoP and the SI undertakes to cooperate with and provide to the DoP/ any other agency appointed by the DoP, all documents and other details as may be required by them for this purpose. Any deviations or contraventions, identified as a result of such audit/assessment, would need to be rectified by the SI failing which the DoP may, without prejudice to any other rights that it may have issued a notice of default. The cost of acquisition of deliverables by the SI is out of the purview of audit/inspections.		As per RFP

Response to the Pre-Bid Queries

13 95			iii. Without prejudice to the foregoing, the SI shall allow access to the DoP or its nominated agencies to all information which is in the possession or control of the SI and which relates to the provision of the Services/Deliverables as set out in the Audit, Access and Reporting Schedule and which is reasonably required by the DoP to comply with the terms of the Audit, Access and Reporting Schedule set out as Schedule V of this Agreement.		As per RFP

Response to the Pre-Bid Queries

13 96	III	Section 1.18, Page 37	a) Pre-existing work: All intellectual property rights existing before the Effective Date of this Agreement shall belong to the Party that owned such rights immediately before the Effective Date.	Bidder understands pre-existing work includes work created independently of the project as well as prior to the effective date, and any derivative over the same	As per RFP

Response to the Pre-Bid Queries

13 97			Subject to the foregoing, the DoP will also have rights to use and copy all processes,	We request this to be clarified as follows:	As per RFP

Response to the Pre-Bid Queries

13 98			specifications, reports and other document drawings, manuals, deliverables, including but not limited to processes, specifications, reports, drawings, manuals, configuration scripts, system architecture documents, integration code, DR automation scripts, and any other materials created or delivered as part of the Services under this Agreement and other documents, the entire services provided by SI as part of the Scope of Works under this Agreement on non-exclusive, transferable, (including the right to sublicense to DoP's contractors, affiliates, or successor service providers) perpetual, royalty-free license to use, copy, maintain and modify for DoP's internal business purposes		As per RFP

Response to the Pre-Bid Queries

13 99				DoP will own the final service deliverables developed by SI and SI will retain an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, sublicense, distribute, and prepare derivative works of such deliverables. Rights in OEM goods/products supplied shall be as per the standard terms provided by the OEM to DOP.	As per RFP

Response to the Pre-Bid Queries

14 00			For the avoidance of doubt, it is clarified that no additional payment shall be made to SI for the right and non-exclusive, non-transferable, perpetual, royalty-free license to use basis grant of the aforesaid license right to DoP, including the right to use, maintain and modify the deliverables and any background IP embedded therein		As per RFP

Response to the Pre-Bid Queries

14 01				Further, pre-existing IP does not include any SI's commercial offerings, which will be provided as OEM product under its standard terms and conditions.	As per RFP

Response to the Pre-Bid Queries

14 02	III	Section 1.18, Page 38	This will also include any developments/customization done on COTS for the DoP. Any solution/framework that does not meet the definition of COTS shall be treated as bespoke development	Rights in OEM goods/products supplied shall be as per the standard terms provided by the OEM to DOP.	As per RFP

Response to the Pre-Bid Queries

14 03	III	Section 1.18, Page 39	The SI shall process such data only as instructed by DoP and shall comply with all applicable data-protection laws (including the Digital Personal Data Protection Act, 2023) and regulatory guidelines issued by RBI and CERT. If any DoP data is required to leave India, including through use of cloud infrastructure or third-party service providers, the SI shall ensure full compliance with applicable cross-border data-transfer restrictions and obtain DoP's prior written approval before initiating such transfers. The SI shall also ensure that any such transfers provide an equivalent level of data protection as required under applicable law	Bidder understands that no personal information will be required to be shared with Bidder for the performance of services under this RFP. To the extent such information is required, both parties to comply with their respective obligations under the applicable data protection laws and SI shall work as per the instructions provided by DOP (as a data fiduciary/data controller) and sign an appropriate data protection agreement.	As per RFP

Response to the Pre-Bid Queries

14 04				DOP will determine and agree with the SI on any technical and organizational measures that SI needs to implement for DOP to be in compliance with the applicable privacy laws. Any additional cost for such implementations (if any) above and beyond the agreed efforts to be addressed in accordance with a Change request.	As per RFP

Response to the Pre-Bid Queries

14 05				Bidder requests following clarification:	As per RFP

Response to the Pre-Bid Queries

14 06				Bidder will comply with all applicable laws that are applicable to it as an IT Service Provider. However, if DOP wants the Bidder to implement measures as per applicable laws/regulations or policies that are applicable to DOP, DOP shall specify the same as part of the scope and specifications along with related changes to the Bidder. In case there is an additional cost attached to such compliance, the parties should agree to the cost as per the change request	As per RFP

Response to the Pre-Bid Queries

14 07	III	Section 1.18, Page 39	Assets : Upon delivery and receipt of full payment, all customized, developed, or procured assets shall become the exclusive property of the DoP. Any applicable manufacturer or OEM warranties shall be duly assigned to the DoP at that time.	OEM products are procured in client's name. The warranty for OEM hardware and software, shall be provided on standard OEM terms and conditions.	As per RFP

Response to the Pre-Bid Queries

14 08	III	Section 1.19.1, Page 39, 40	1.19.1 Standard :	Bidder is willing to provide industry standard warranties with respect to service performance. OEM will be selected by bidder basis the specifications provided by the buyer, however, the warranty for such hardware and software of the OEM, shall be provided on standard OEM terms and conditions	As per RFP

Response to the Pre-Bid Queries

14 09			i. The SI warrants that the Project, including all the systems(s), materials and goods supplied pursuant to this Agreement, shall be free from any defect or deficiency in the material and goods supplied pursuant to this Agreement, shall be free from any defect or deficiency in the material, design, engineering, and workmanship that prevent the system and/ or any of its systems from fulfilling the technical requirements or that limit in a material fashion the performance, reliability, or extensibility of the system and/or any of its sub-system(s). Commercial warranty provisions of products supplied under the Agreement shall apply to the extent they do not conflict with the provisions of this Agreement.		As per RFP

Response to the Pre-Bid Queries

14 10			ii. The SI also warrants that the products, materials and other goods supplied under the Agreement are new, unused and incorporate all recent improvements in design that materially affect the system's or subsystem's ability to fulfill the technical requirements specified in the RFP.		As per RFP

Response to the Pre-Bid Queries

14 11			If during the warranty period any defect or deficiency is found in the material, design and performance/workmanship of the Project and other Services provided by the SI, the SI shall promptly, in consultation and agreement with DoP, and at the SI's sole cost repair, replace, or otherwise make good (as the SI shall, at its discretion, determine) such default, defect or deficiency as well as any damage to the system caused by such default, defect or deficiency. Any defective component, excluding hard disks, that has been replaced by the SI shall remain the property of the SI.		As per RFP

Response to the Pre-Bid Queries

14 12	III	Section 1.19.2, Page 41	1.19.2 Implied Warranty: The warranties provided herein are in lieu of all other warranties, both express and implied, to the extent permitted by applicable law. Notwithstanding the foregoing, the Supplier does not disclaim (a) any warranty that the Deliverables will conform to the specifications, documentation, or agreed service levels, or (b) any warranty that cannot lawfully be excluded. The warranties set out in this clause are in addition to and not in substitution for any other warranties, representations, conditions, or remedies available to the DoP under this Agreement or applicable law.	The last sentence is contradictory to the intent of this implied warranty:	As per RFP

Response to the Pre-Bid Queries

14 13				1.19.2 Implied Warranty: The warranties provided herein are in lieu of all other warranties, both express and implied, to the extent permitted by applicable law. Notwithstanding the foregoing, the Supplier does not disclaim (a) any warranty that the Deliverables will conform to the specifications, documentation, or agreed service levels, or (b) any warranty that cannot lawfully be excluded. ~~The warranties set out in this clause are in addition to and not in substitution for any other warranties, representations, conditions, or remedies available to the DoP under this Agreement or applicable law.~~	As per RFP

Response to the Pre-Bid Queries

14 14	III	Section 1.20.1, Page 41	1.20.1 Obligation to Maintain Insurance	Request to modify as follows:	As per RFP

Response to the Pre-Bid Queries

14 15			(i) In connection with the provision of the Services, the SI must have and maintain, and shall cause any sub-contractor to take out and maintain, at his (or subcontractors, as the case may be) cost but on terms and conditions approved by DoP, valid and enforceable insurance for the Agreement Term against the risks, and for the coverages including but not limited to:		As per RFP

Response to the Pre-Bid Queries

14 16			a. either professional indemnity or errors and omissions	1.20.1 Obligation to Maintain Insurance	As per RFP

Response to the Pre-Bid Queries

14 17			b. product liability	(i) In connection with the provision of the Services, the SI must have and maintain, ~~and shall cause any sub-contractor to take out and maintain,~~ at his (or subcontractors, ~~as the case may be~~) cost but on terms and conditions approved by ~~DoP~~ , valid and enforceable insurance for the Agreement Term against the risks, and for the coverages including but not limited to:	As per RFP

Response to the Pre-Bid Queries

14 18			c. workers' compensation as required by law and	a. either professional indemnity or errors and omissions	As per RFP

Response to the Pre-Bid Queries

14 19			d. any additional types, if any, as may be required depending on the Services provided in this Agreement; and	b. product liability	As per RFP

Response to the Pre-Bid Queries

14 20			(ii) The above insurance policies shall be of appropriate values so as to cover risks of SI under this Agreement.	c. workers' compensation as required by law and	As per RFP

Response to the Pre-Bid Queries

14 21				d. any additional types, if any, as may be required by applicable laws of India ~~depending on the Services provided in this Agreement;~~ and	As per RFP

Response to the Pre-Bid Queries

14 22				(ii) The above insurance policies shall be of <u>the types and limits customary for businesses of similar size and in accordance with industry practice</u> ~~appropriate values so as to cover risks of SI under this Agreement.~~	As per RFP

Response to the Pre-Bid Queries

14 23	III	Section 1.20.1, Page 41	(iii) The SI shall not use these documents for purposes unrelated to this Agreement without the prior written approval of the DoP.	Request to clarify the intent of this clause.	As per RFP

Response to the Pre-Bid Queries

14 24	III	Section 1.21, Page 42	1.21 Escrow Management	We understand that this will be limited to any deliverable created by SI specifically for DOP. Any source code with respect to OEM shall be governed by the OEM terms and conditions.	As per RFP

Response to the Pre-Bid Queries

14 25			i. The SI shall, within a period not exceeding six (6) weeks from the date of issuance of the Letter of Award under the RFP, or within such period as may be reasonably specified by the DoP in writing, commence the required activities, deposit the Source Code of the existing functionalities/applications (as instructed in Volume II of the RFP) with Escrow Agent based on the appropriate standard agreement or on such other terms as the DoP, the SI and the Escrow Agent shall agree. For new implementations or enhancements, the SI shall deposit the Source Code (as instructed in Volume II of the RFP) along with the corresponding flow diagrams build scripts, configuration files, and technical documentation/write-up for the software within thirty (30) days of implementation.		As per RFP

Response to the Pre-Bid Queries

14 26			ii. The SI shall ensure that the deposited version of the Source Code is the current version of the POSB Solution and that the deposited version is kept up-to-date as the POSB Solution is modified or upgraded. The SI shall pay the initial storage fees renewal, and maintenance fee under the escrow agreement and the DoP shall only pay the release fees in the event of an actual release from escrow. The escrow agent and the escrow arrangement shall be geographically located in India.		As per RFP

Response to the Pre-Bid Queries

14 27			iii. DoP shall have the right, either directly or through a third-party auditor/escrow agent, to periodically verify and/or test the completeness, accuracy, and usability of the Source Code and other materials deposited in escrow. Such verification may include compilation, build, and test of the deposited Source Code to ensure that it is sufficient and functional for DoP to use, maintain, and modify the Solution in accordance with this Agreement. The SI shall fully cooperate in such verification process and provide any necessary		As per RFP

Response to the Pre-Bid Queries

14 28	III	Section 1.22.2, Page 43	During the Term and 12 months thereafter, neither Party will solicit for employment or knowingly hire an employee of the other Party with whom such Party has contact pursuant to Project engagements under this Agreement. This restriction shall not apply to employees of either Party responding to advertisements in job fairs or news media	We understand that this applies to an employee directly involved in the performance of the contract, and the term shall apply for the duration such person is so involved and for 12 month thereafter.	As per RFP

Response to the Pre-Bid Queries

14 29			circulated to the general public.	Further, the acts that are restricted are the acts of targeted solicitation to hire such employee.	As per RFP

Response to the Pre-Bid Queries

14 30	III	Section 1.22.3, Page 44	The terms of the contracts proposed to be entered into with the sub-contractors shall require the prior written approval of the DoP and shall be in conformity with the terms of the Agreement.		As per RFP

Response to the Pre-Bid Queries

14 31			The SI shall ensure that all subcontractors engaged sign an agreement that is aligned in duration with this Agreement and remain available for the entire duration of this Agreement, unless otherwise approved in writing by the DoP.		As per RFP

Response to the Pre-Bid Queries

14 32	III	Section 1.22.3, Page 44	The SI indemnifies and shall keep indemnified the DoP against any losses, damages, claims or such other implications arising from or out of the acts and omissions of such sub-contractor.	We understand that this refers to indemnity only where and to the extent the acts of subcontractors trigger SI's indemnity obligations mentioned elsewhere in the agreement.	As per RFP

Response to the Pre-Bid Queries

14 33	III	Section 1.22.3, Page 45	f. All rights of use of any process, service or facility developed or any other task performed by the subcontractor for the SI for the purposes of this Agreement, under a subcontract/agreement would lie exclusively with the DoP and shall vests absolutely and irrevocably in DoP in perpetuity free from all liens, encumbrances and other third party rights and the SI shall, wherever required take all steps that may be necessary to ensure the use of such rights by the DoP. Ownership and all rights of use of all deliverables / documents/ reports etc. supplied by the SI and/or by authorized subcontractor for the SI for the purposes of this Agreement, under a subcontract/agreement would lie exclusively with the DoP from the time of their creation in perpetuity free from all liens, encumbrances and other third party rights and the SI shall, wherever required take all steps that may be necessary to ensure the ownership and use of such rights by the DoP. DoP shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed by the subcontractor solely during execution of this Agreement. The SI will provide the undertakings given by the subcontractor within 30 days from the date of appointment	OEM products are provided in the name of the client as per their standard terms and conditions.	As per RFP

Response to the Pre-Bid Queries

			of subcontractor to disclose all such Intellectual Property Rights arising in performance of the Services to the DoP and shall execute all such agreements/documents and file all relevant applications, effect transfers, and obtain all permits and approvals that may be necessary in this regard to effectively transfer perfect and protect and preserve the Intellectual Property Rights of the DoP.		

Response to the Pre-Bid Queries

14 34			g. SI shall ensure that the deliverables delivered by the sub-contractors are genuine and in the case of software, are duly licensed ones. The SI will indemnify and defend the DoP against any claim that any third-party products delivered under this Agreement are either not genuine or are not a proper licensed one	We understand that by subcontractor here you are referring to the manpower.	As per RFP

Response to the Pre-Bid Queries

14 35				Bidder understands that the IPR and ownership of the preexisting IPR of the Bidder and any derivative over the same, would lie with the Bidder	As per RFP

Response to the Pre-Bid Queries

14 36				We request this to be clarified as follows:	As per RFP

Response to the Pre-Bid Queries

14 37				DoP will own the final service deliverables developed by SI and SI will retain an irrevocable, nonexclusive, worldwide, paid-up license to use, execute, reproduce, display, perform, sublicense, distribute, and prepare derivative works of such deliverables. Each Party shall retain all rights in the materials it brings in. Rights in OEM goods/products supplied shall be as per the terms provided by the OEM to DOP.	As per RFP

Response to the Pre-Bid Queries

14 38	III	Section 1.22.3, Page 45	Further, in case the SI terminates any contract/arrangement or agreement with a sub-contractor for any reason whatsoever, the SI shall ensure the smooth continuation of Services by providing forthwith a suitable replacement which is acceptable to the DoP at no additional charge and ensures no degradation or interruption of the Services or extension of timelines.	We understand this only applies where such termination is not requested by DOP, in which case, parties to mutually agree on the impact.	As per RFP

Response to the Pre-Bid Queries

14 39	III	Section 1.22.4, Page46	c. DoP may assign or novate all or any part of this Agreement and Schedules/Annexures, and the SI shall be a party to such novation, to any third party contracted to provide outsourced services to DoP or any of its nominees.	We understand that any such assignment shall be subject to assessment of credibility of the assignee	As per RFP

Response to the Pre-Bid Queries

14 40	III	Section 1.22.8(g), Page 47	If it is discovered at any time that the person, so signing has no authority to do so, DoP reserves its right, without prejudice to any other right or remedy, to terminate the Agreement for default in terms of the Agreement and avail any or all the remedies thereunder and hold such person personally and/ or the SI liable to the DoP for all costs and damages arising from such remedies.	Request to remove personal liability as any person executing the contract or acting hereunder is acting on behalf of SI. If they do not have authority, SI shall be liable and not the person.	As per RFP

Response to the Pre-Bid Queries

14 41	III	Section 1.22.9(b), Page 48	b. In cases where Services are to be performed by SI at the premises of DoP or beneficiary of Services designated by the DoP, the SI shall comply with the provisions of the Labour Codes including Code on Wages, 2019 The Industrial Relations Code 2020, Code on the Social Security 2020, and the Occupational Safety, Health and Working Conditions 2020, and Draft Rules made thereunder, as modified from time to time, wherever applicable and shall also indemnify the DoP from and against any claims under the aforesaid Labour Codes and the Rules	We understand here it refers to SI's compliance with applicable labor laws, that apply to it as an employer, and indemnification refers to defending DOP from employment-related claims that are solely within SI's control and responsibility as the employer.	As per RFP

Response to the Pre-Bid Queries

14 42	III	Section 1.22.9(d), Page 48	During the tenure of this Agreement, the SI shall comply with all Applicable Laws and shall obtain and maintain all statutory and other approvals required for the performance of the Services under this Agreement and nothing shall be done by the SI in contravention of any Applicable Law or any amendment thereof and the SI shall keep the DoP indemnified in this regard.	We understand that the indemnity here refers to SI's obligation to indemnify DOP for any government-imposed fines or penalties imposed on DOP solely due to any violation of law applicable to SI in its capacity as an IT services provider.	As per RFP

Response to the Pre-Bid Queries

14 43				Further, the indemnification process and conditions specified in Section 1.14.3 shall apply to any indemnity mentioned in this Agreement.	As per RFP

Response to the Pre-Bid Queries

14 44	III	Section 1.22.9(e)(ii)(b) Page 49	(b) provide the DoP with a copy of information in its possession or power in the form that the DoP requires within (five) days or such other period as DoP may specify.	We understand that RTI here refers to any information or document which is owned by DOP. This doesn't extend to any confidential, sensitive, proprietary, privileged or other non-public information of the SI.	As per RFP

Response to the Pre-Bid Queries

14 45			iii. DoP shall be responsible for determining at its absolute discretion whether the commercially, sensitive, confidential and other information is exempt from disclosure, to be disclosed in accordance with the provision of RTIA.		As per RFP

Response to the Pre-Bid Queries

14 46	III	Section 1.22.12, Pages 50	b. Without prejudice to the generality of sub-clause 1.21.12 (a) above, on matters not covered by this Agreement, the provisions of RFP shall apply.	We understand that Agreement shall be mutually agreed between the parties. Hence, for any matter, Agreement (along with its annexures) should be solely relied upon.	As per RFP

Response to the Pre-Bid Queries

14 47	III	Section 1.22.14, Pages 50-53	Dispute Resolution –	Instead of institutional arbitration, request to allow parties flexibility by specifying that any dispute not resolved as per the dispute resolution mechanism amicably, shall be finally settled in accordance with The Arbitration and Conciliation Act, 1996 then in effect. There shall be one arbitrator if the amount in dispute is less than or equal to Indian Rupee five crores and three arbitrators if the amount is more	As per RFP

Response to the Pre-Bid Queries

14 48		invoking resolution of disputes through arbitration in accordance with the provisions of the India International Arbitration Centre (Conduct of Arbitration) Rules and administered by the India International Arbitration Centre (IIAC"). and can submit any dispute or difference whatsoever arising between the parties to this Agreement out of or relating to the construction, meaning, scope, operation or effect of this agreement or the validity of the breach thereof arbitration by an Arbitral Panel which shall be comprised with three arbitrators wherein each Party shall appoint one appointed/nominated by each Party, from IIAC's Panel of Arbitrators, subject to approval by the Chairperson and the two such appointed arbitrators shall appoint a third arbitrator who shall act as the presiding arbitrator. If the two nominated arbitrators cannot agree on the third arbitrator within the period specified (or agreed) timeline, the Chairperson of IIAC will appoint the third arbitrator. Constitution of Arbitral Panel shall be in accordance with and in full satisfaction of the qualifications to be prescribed for such arbitrator, including but not limited to the qualifications so as to technical experience, nationality and legal experience, by the DoP and the SI, at the time of appointment with arbitration	As per RFP

Response to the Pre-Bid Queries

			proceedings shall be conducted in English language. The arbitration proceedings with seat and venue will be held at New Delhi, India.		

Response to the Pre-Bid Queries

14 49			h. The provisions of the The India International Arbitration Centre (Conduct of Arbitration) Rules and administered by the India International Arbitration Centre "IIAC" will be applicable on the Arbitration Proceedings and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the "IIAC", or of any modifications, rules or re-enactments thereof		As per RFP

Response to the Pre-Bid Queries

14 50	III	Section 1.25.2, Page 57	(v) The outgoing SI will pass on to DoP and/or to the Replacement SI, the subsisting rights in any leased properties/ licensed products on terms not less favorable to DoP/ Replacement SI, than that enjoyed by the outgoing SI.	Note that any assignment shall be subject to the terms of the agreement with third parties. For any transfer, Bidder may provide reasonable connect with the third party for DOP to engage in direct relationship with them.	As per RFP

Response to the Pre-Bid Queries

14 51	III	Section 1.25.2, Page 57	The SI will promptly on the commencement of the exit management period supply to the DoP or its nominated agency the following:	Bidder understands that handover will be required for the deliverables which are created by the bidder for the buyer under the contract. Any confidential information, proprietary or privileged information will not be required to be handed over.	As per RFP

Response to the Pre-Bid Queries

14 52		Section 1.25.2, Page 57	ii) All risk in and title to the Assets to be transferred / to be purchased by the DoP under this clause shall be transferred to DoP, on the last day of the exit management period.	With respect to transfer of assets, license, etc. Bidder understands that since all licenses and hardware etc will be taken in the name of DOP, transfer from Bidder to DOP is not relevant.	As per RFP

Response to the Pre-Bid Queries

14 53				With respect to subcontracts, Bidder is unable to disclose confidential details of its contracts with subcontractors/vendors but we would like to clarify that buyer may enter into direct contracts with them as per mutually agreed terms between buyer and the vendor/subcontractor.	As per RFP

Response to the Pre-Bid Queries

14 54		Section 1.25.3, Page 58	1.25.3 Transfer of certain agreements		As per RFP

Response to the Pre-Bid Queries

14 55			On request by the DoP or its nominated agency, the SI shall effect such assignments, transfers, novation, licenses and sub-licenses to DoP or its Replacement SI in relation to any equipment lease, maintenance or service provision agreement between SI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the DoP or its nominated agency or its Replacement SI.	Any assignability will be subject to consent/contractual provisions between Bidder and third party.	As per RFP

Response to the Pre-Bid Queries

14 56			b) The SI shall also give the DoP or its nominated agency or its nominated agencies, or any Replacement SI right of reasonable access to the SI's premises and shall procure the DoP or its nominated agency or its nominated agencies and any Replacement SI rights of access to relevant third party premises during the exit management period and for such period of time following termination or expiry of the MSA as is reasonably necessary to migrate the services to DoP, or a Replacement SI.		As per RFP

Response to the Pre-Bid Queries

14 57	Volume II Annexure N	Annexure N : External NGFW	External NGFW	As per standards, the external firewall & Intranet firewall are usually of different technology / make to provide optimalo security to the enterprise network. The Annexure does not specify separate description / requirements for Intranet Firewall. Please clarify	As per RFP

Response to the Pre-Bid Queries

14 58	Volume II	Annexure N : SIEM, UEBA, SOAR, TI, NTA	Threat Intel Management	Will there be any requirement to integrate current (existing) threat feeds into newly provisioned TIP at modernised Data-centers ? Please provide details of present threat-feeds being used by DOP for security monitoring	As per RFP

Response to the Pre-Bid Queries

14 59	II	Section 5.2.4, Page 82, Pt14	Detailed Scope of Work	Bidder request to minimize Scope creep by removing clauses like "Not limited to" and "etc" in the scope section. Also clauses like "The SI must accommodate unforeseen demand surges and provide mechanisms to adapt and scale infrastructure promptly."	As per RFP

Response to the Pre-Bid Queries

14 60	II	Annexure B, C, M, Pg 212	Annexure C – BoQ of Existing Licenses, Annexure M – Tech Stack	Please provide details like software Bill-of-quantity, CSI #, start & end date) for all OEMs/application licenses like Oracle Symantec, etc. This will help the bidder to ask for ATS from the OEMs for the contract duration	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

14 61	I	3. Criteria for Evaluation, Sl. No A1 Page 38 to 40	A1. i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. OR Certificate from the Statutory Auditor/ Authorized Signatory certifying that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase.	Bidder proposes to change as follows : i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. OR Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory certifying that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. In case of NDA with the client, please allow to submit the Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory .	As per RFP

Response to the Pre-Bid Queries

14 62	I	3. Criteria for Evaluation, Sl. No A2 Page 38 to 40	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work along with proof of execution/ Credential Letter from the competent Authority. (Installations from multiple clients/projects are accepted)	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work along with proof of execution/ Credential Letter from the competent Authority. (Installations from multiple clients/projects are accepted) OR Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory certifying that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. In case of NDA with the client, please allow to submit the Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory .	As per RFP

Response to the Pre-Bid Queries

14 63	I	3. Criteria for Evaluation, Sl. No B1 Page 38 to 40	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. OR Certificate from the Statutory Auditor/ Authorized Signatory certifying that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase.	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. OR Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory certifying that the Project has been declared "Go-Live" and is under the Operations & Maintenance phase. In case of NDA with the client, please allow to submit the Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory .	As per RFP

Response to the Pre-Bid Queries

14 64	I	3. Criteria for Evaluation, Sl. No B2 Page 38 to 40	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live". OR Certificate from the Statutory Auditor/ Authorized Signatory certifying that the Project has been declared "Go-Live".	i. Project Citation as per the Form A.5: Format for Project Citation. ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract. iii. Certificate/Letter from the Competent Authority (who has issued the work order) that the Project has been declared "Go-Live". OR Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory certifying that the Project has been declared "Go-Live". In case of NDA with the client, please allow to submit the Certificate from the Statutory Auditor/ Chartered Accountant /Company Secretaty / Authorized Signatory .	As per RFP

Response to the Pre-Bid Queries

14 65	II	Page 13, Figure	Figure I: Solution Architecture IT 2.0	Figure I: Solution Architecture IT 2.0 is for information purpose only and is not part of scope. Please confirm	Solution Architecture Diagram are indicative in nature, Successful bidder need to provide final architecture during the assesment phase.

Response to the Pre-Bid Queries

14 66	II	Page 128	6. Service Level Agreement Penalties	The bidder request to include clause for overall penalty capping.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 67	II	Page 24	5.1.1 Details of existing vendors Figure II: Existing Contract(s) Timeline (Apr 2026 onwards)	During the transition phase, all the existing contracts (software, hardware, manpower vendors/OEMs) should be in active support. Also clarify, post transition , how will the existing contracts be managed.	Refer #360

Response to the Pre-Bid Queries

14 68	II	5.2.4.6 Near DC (NDC) Requirements, Page 92	The SI is required to furnish a thorough cost estimation encompassing the setup, maintenance, and continuous operation of the Near DC site. The breakdown should include costs for hardware, software, connectivity, and any additional resources necessary.	NDC location will have the storage solution for meeting RPO 0 .Is DoP will be using NDC location for serving user traffic in case of DC failure ?Pls clarify	The SI is required to achieve storage based replication between the DC and NDC to ensure zero data loss.

Response to the Pre-Bid Queries

14 69	I	Section 3, Pg 37	A1. Evaluation Criteria: The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Core Banking Services and allied products within the last five (5) years from the date of bid submission, with each such project having a value of at least INR 130 crore in the BFSI sector, either in India or globally	The Bidder must have experience in Software Development / Implementation / Maintenance projects related to Finacle Core Banking Services and allied products within the last five (5) years from the date of bid submission, with each such project having a value of at least INR 130 crore in the BFSI sector, ~~either in India or globally~~ only	As per RFP

Response to the Pre-Bid Queries

14 70	I	Section 3, Pg 37 (A1 and B1)	A1 and B1. Supporting Documents Required : ii. Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and value of the contract.	A1 & B1. Supporting Documents Required : ii. Masked Work order / Purchase Order / Contract Agreement clearly specifying the Scope of Work, Bill of Material and ~~value of the contract~~ a self decalration from authorised signatory / statutory auditor providing project details with contract value	As per RFP

Response to the Pre-Bid Queries

14 71	II	Section 5.1.1, Pg23	a. CBS Software (License/ATS): To be procured and implemented by the SI from September 2027 till the end of the contract. And also any kind of new procurement from IBM / AIX in contention.	a. For compliance to this clause by any bidder except Infosys / EV, kindly revoke the clause Volume I - Page 16 that states - <i>"Either the Principal or its authorized agent may submit a bid for a given item/product under this RFP; however, both shall not submit bids simultaneously for the same item/product."</i>	As per RFP

Response to the Pre-Bid Queries

14 72	I	Pg 16 2.4 Eligible Bidders	Either the Principal or its authorized agent may submit a bid for a given item/product under this RFP; however, both shall not submit bids simultaneously for the same item/product	a. For compliance to this clause by any bidder except Infosys / EV, kindly revoke the clause Volume I - Page 16 that states - <i>"Either the Principal or its authorized agent may submit a bid for a given item/product under this RFP; however, both shall not submit bids simultaneously for the same item/product."</i>	As per RFP

Response to the Pre-Bid Queries

14 73	I	Section 2.23, Pg 34	a. Subcontracting is allowed only for Manpower and Data Centre facility services and the details for the same needs to be disclosed by the Bidder in their technical proposal. The overall value of all the subcontracted work/services shall not exceed more than 20% of the total value of contract.	a. Subcontracting is allowed only for <u>OEM related services</u> , Manpower and Data Centre facility services and the details for the same needs to be disclosed by the Bidder in their technical proposal. ~~The overall value of all the subcontracted work/services shall not exceed more than 20% of the total value of contract.~~	As per RFP

Response to the Pre-Bid Queries

14 74	III	Section 1.3, Pg 12	This Agreement shall come into effect on _____, YYYY (hereinafter the 'Effective Date') and shall be for a duration of 5 (years) from the date of acceptance of letter of award by SI i.e. _____till _____,YYYY ('Initial Term') extendable to a further period of 2 years, on an year to year basis, subject to a maximum of 2 years ("Extended Term") at the sole discretion of DoP, on the same terms and conditions.	This Agreement shall come into effect on _____, YYYY (hereinafter the 'Effective Date') and shall be for a duration of 5 (years) from the date of acceptance of letter of award by SI i.e. _____till _____,YYYY ('Initial Term') extendable to a further period of 2 years, on an year to year basis, subject to a maximum of 2 years ("Extended Term") at the sole discretion of DoP, ~~on the same terms and conditions.~~ as per mutual agreement between SI and DOP at the time of extension.	As per RFP

Response to the Pre-Bid Queries

14 75	III	Pg 15/16 Section 1.5.5	Liquidated damages will be capped at 10% of the Total Contract Value (TCV)	Liquidated damages / <u>SLA Penalty</u> will be capped at 5% of the Total Contract Value (TCV).	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 76	III	Pg 31/32/33 Section 1.14.4 and 1.14.6,	1.14.4 Risk Purchase 1.14.6 Step-In-rights	1.14.4 Risk Purchase: We request Risk Purchase clause to be removed as it is being duplicated with Step in rights. 1.14.6: Step-In-rights: We request the capping of the amount payable by the SI due legal process under Step in rights be limited to 10% of the amount that was payable to SI for non-delivered services/ deliverables.	As per RFP

Response to the Pre-Bid Queries

14 77	III	Pg 39/40 Section 1.19	iv. The warranty period shall commence from the date of Go-live of the Project (as defined in Volume 2 of the RFP) and shall extend for as follows:	iv. The warranty period shall <i>be in block of years</i> commencing from the date of ~~Go-live of the Project~~ <u>delivery of hardware/software product</u> (as defined in Volume 2 of the RFP) <i>followed by AMC/ATS for the entire duration of the contract as per the proposal.</i> ~~and shall extend for as follows:~~ Reason: <i>Warranty / AMC, ATS is only available on annual basis (payable upfront, monthly AMC ATS is not possible)</i>	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 78	I	49	The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately.	The bid price will include all taxes and levies and shall be in Indian Rupees and mentioned separately <i>(excluding GST & other taxes which are controlled by Govt of India).</i>	As per RFP

Response to the Pre-Bid Queries

14 79	iii	1.13.5 pg 32	1-Effects of termination 2-Termination of this Agreement due to Bankruptcy of SI	Both the sections have the same reference number viz 1.13.5 which needs to be corrected	Clause to be referenced as 1.13.5(a) - Termination of this Agreement due to Bankruptcy of SI Provisions of the clause shall remain as per RFP.

Response to the Pre-Bid Queries

14 80	iii	1.14.5, pg35	The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement.	i. The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed ~~one time the total contract value payable under this Agreement~~ the average annual Charges (excluding taxes, reimbursements, and pass through expenses) paid to SI by DoP under the relevant SOW. Notwithstanding anything herein to the contrary, the maximum liability of the SI with respect to any privacy or data breach obligations shall not exceed two (2) times of applicable fees paid during the 12 months period.	As per RFP

Response to the Pre-Bid Queries

14 81	iii	1.20.2, pg48	The SI must, on request by the DoP, provide current relevant confirmation of insurance documentation from its insurance brokers certifying that it has insurance as required by this Clause 1.21. The SI agrees to replace any coverage prior to the date of expiry/cancellation.	The SI must, on request by the DoP, provide current relevant confirmation of insurance documentation from its insurance brokers certifying that it has insurance as required by this Clause 1.24 ~~0~~ . The SI agrees to replace any coverage prior to the date of expiry/cancellation.	Clause to be referenced as 1.20. Provisions of the clause shall remain as per RFP

Response to the Pre-Bid Queries

14 82	ii	11.3, pg 194	Payment Milestones for Track 2	2.2 Commercial bid DCF hosting charges - The payment for DCF hosting charges which are basically charges need to be paid upfront quarterly and are not defined here. Secondly, These charges should not be linked to any milestone achievement. Secondly, whether DoPB wants power charges to be part of rack price or to be carved out separately ?	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 83	ii	11.3, pg 194	Payment Milestones for Track 2	2.1 Implementation of DCF - The Hardware and Software charges to be paid 90% on delivery and 10% upon Go-live. These charges should not be linked to any milestone achievement	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 84	ii	11, pg 194, 11.3, pg 201	Payment terms for AMC, ATS, SW Licenses & HW	Payment terms of Software (Products) are seemingly linked to non Delivery milestones. Also it is not clear if the Hardware (Products) Payment terms are linked to Delivery or not. As the Commercial Template and Scope documents has different T&C mentioned for Software and Hardware payment terms. We need 90% payment for Software (Products) & Hardware (Products) upon delivery and 10% on Go-live. AMC/ATS, O&M Apps & Infra to be in 30 days. Payment beyond 30 days DOP-POSB will be liable to pay interest @ 18% p.a. Beyond 180days, Wipro gets the right to invoke Termination. In the event of termination of this Agreement for default on payment, the DoP shall pay the SI: (a) all fees and expenses for services performed up to the effective date of termination, including work in progress; (b) fees for the applicable notice period, irrespective of whether the DoP requires the SI's services during such period; (c) any termination charges agreed by the Parties or as may have been set out in the applicable SOW; and (d) any unamortized costs for lease, licenses or other materials procured by the SI for the DoP.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

14 85	iii	1.12.2.c, pg 24	Subject to the accomplishment of obligations of the SI and delivery of the Deliverables and the Services to the satisfaction of the DoP, payment shall be made within 60 working days of the receipt of invoice along with supporting documents. Payments will be subject to the deduction of applicable liquidated damages or SLA penalties. The penalties are imposed on the SI as per the SLA specified in Volume 2 of the RFP.	Subject to the accomplishment of obligations of the SI and delivery of the Deliverables and the Services to the satisfaction of the DoP, payment shall be made within ~~60 working~~ 30 days of the receipt of invoice along with supporting documents. Payments will be subject to the deduction of applicable liquidated damages or SLA penalties. The penalties are imposed on the SI as per the SLA specified in Volume 2 of the RFP.	As per RFP

Response to the Pre-Bid Queries

14 86	iii	Pg, 13 1.2.1 Scope of Work	In consideration of the award of the work under the RFP to SI and undisputed payments to be made by DoP to the SI as hereinafter mentioned, the SI hereby covenants with the DoP to provide the Services as detailed under Scope of Work Volume 2 of the RFP along with clarifications thereof, and Annexures thereunder and to remedy defects therein in conformity in all respects with the provisions of the Agreement.	In consideration of the award of the work under the RFP to SI and undisputed payments to be made by DoP to the SI as hereinafter mentioned, the SI hereby covenants with the DoP to provide the Services as detailed under Scope of Work Volume 2 of the RFP along with clarifications thereof, and Annexures thereunder and to remedy defects therein in conformity in all respects with the provisions of the Agreement, <u>provided that the SI shall only be required to provide those Services that are expressly described in a mutually executed Scope of Work.</u>	As per RFP

Response to the Pre-Bid Queries

14 87	iii	Pg, 13 1.3 Term and Duration of the Agreement	This Agreement shall come into effect on _____, YYYY (hereinafter the 'Effective Date') and shall be for a duration of 5 (years) from the date of acceptance of letter of award by SI i.e. _____ till _____, YYYY ('Initial Term') extendable to a further period of 2 years, on an year to year basis, subject to a maximum of 2 years ("Extended Term") at the sole discretion of DoP, on the same terms and conditions. The price agreed under this Agreement shall serve as the ceiling rate for any extension period for the same scope of Services. In case of any material change in scope, the Parties shall mutually agree on revised _____ commercials commensurate with such change. The Agreement shall continue till the date of the completion of the operation and maintenance to the DoP, unless terminated earlier (as per Clause 1.13), in which case the Agreement will get terminated on fulfillment of all obligations mentioned as per Clause 1.13 and Schedule III (i.e. Exit Management Schedule).	This Agreement shall come into effect on _____, YYYY (hereinafter the 'Effective Date') and shall be for a duration of 5 (years) from the date of acceptance of letter of award by SI i.e. _____ till _____, YYYY ('Initial Term') extendable to a further period of 2 years, on an year to year basis, subject to a maximum of 2 years ("Extended Term")- <u>which will be mutually agreed between the Parties in writing at the sole discretion of DoP, on the same terms and conditions.</u> The price agreed under this Agreement shall <u>remain valid for the Term of the Agreement</u> ~~serve as the ceiling rate for any extension period for the same scope of Services.~~ In case of any material change in scope, the Parties shall mutually agree on revised commercials commensurate with such change. The Agreement shall continue till the date of the completion of the operation and maintenance to the DoP, unless terminated earlier (as per Clause 1.13), in which case the Agreement will get terminated on fulfillment of all obligations mentioned as per Clause 1.13 and Schedule III (i.e. Exit Management Schedule).	As per RFP

Response to the Pre-Bid Queries

14 88	iii	Pg, 17 1.5.5 Liquidated Damages and Service Levels	Time is the essence of the Agreement, and the delivery dates are binding on the SI. The SI shall accomplish the Scope of Work under this Agreement as per the Timelines and as per the Service Levels mentioned in Volume 2 of the RFP. If the SI fails to achieve the Timelines or the Service Levels due to reasons attributable to the SI, the SI shall be liable to pay liquidated damages as per Volume 2 of the RFP. Payment of liquidated damages shall not be the sole and exclusive remedies available to the DoP and the SI shall not be relieved from any obligations by payment of such liquidated damages and to perform the Services or from liability for continued default. Liquidated damages will be capped at 10% of the Total Contract Value (TCV). It is clarified that taxes will be excluded from the TCV while calculating the Liquidated Damages. The right to claim any liquidated damages shall be without prejudice and in addition to other rights and remedies available to DoP under the contract and law.	Time is the essence of the Agreement, and the delivery dates are binding on the SI. The SI shall accomplish the Scope of Work under this Agreement as per the Timelines and as per the Service Levels mentioned in Volume 2 of the RFP. If the SI fails to achieve the Timelines or the Service Levels due to reasons attributable to the SI, the SI shall be liable to pay liquidated damages as per Volume 2 of the RFP. Payment of liquidated damages shall ~~not~~ be the sole and exclusive remedies available to the DoP and the SI shall ~~not~~ be relieved from any obligations by payment of such liquidated damages and to perform the Services or from liability for continued default. Liquidated damages will be capped at 10% of the Total Contract Value (TCV). It is clarified that taxes will be excluded from the TCV while calculating the Liquidated Damages. The right to claim any liquidated damages shall be without prejudice ~~and in addition to other rights and remedies available to DoP~~ under the contract and law.	As per RFP

Response to the Pre-Bid Queries

14 89	iii	Pg, 17 1.5.5 Liquidated Damages and Service Levels	If the liquidated damages cross the cap on liquidated damages mentioned in Volume 2 of the RFP, DoP shall have the right to terminate the Agreement for default and consequences for such termination for default as provided in this Agreement and as per applicable law shall follow.	If the liquidated damages cross the cap on liquidated damages mentioned in Volume 2 of the RFP, <u>and such breach is solely attributable to the SI,</u> DoP shall have the right to terminate the Agreement for default, <u>provided that DoP shall first provide SI with a written notice and a cure period of thirty (30) days to remedy the default.</u> ~~and~~ The consequences for such termination for default <u>shall be</u> as provided in this Agreement and as per applicable law ~~shall follow~~ .	As per RFP

Response to the Pre-Bid Queries

14 90	iii	Pg, 18 1.6.1 Representations and Warranties of the SI	The SI represents and warrants to DoP, as of the date hereof, which represents and warranties shall survive the term and termination hereof, the following:	The SI represents and warrants to DoP, as of the date hereof, which represents and warranties shall <u>remain valid for the</u> <u>Term of the</u> <u>Agreements survive the term</u> <u>and termination hereof</u> , the following:	As per RFP

Response to the Pre-Bid Queries

14 91	iii	1.6.1 Representations and Warranties of the SI	a) That SI shall ensure that all goods, software, systems, materials, processes, or products supplied, developed, or used by the SI in the performance of this Agreement are properly licensed or authorized and do not infringe or violate any third-party intellectual property rights, including but not limited to copyrights, patents, trademarks, trade secrets, or other proprietary rights. The SI shall obtain, at its own cost, all necessary permissions, approvals, and licenses for such use and shall ensure that all such items are free from any claims, titles, encumbrances, or liens. The SI shall indemnify and hold harmless the DoP from and against any and all losses, damages, or claims arising out of or in connection with any such infringement or alleged infringement;	That SI shall ensure that all goods, software, systems, materials, processes, or products supplied, developed, or used by the SI in the performance of this Agreement are properly licensed or authorized and do not infringe or violate any third-party intellectual property rights, including but not limited to copyrights, patents, trademarks, trade secrets, or other proprietary rights. The SI shall obtain, at its own cost, all necessary permissions, approvals, and licenses for such use and shall ensure that all such items are free from any claims, titles, encumbrances, or liens. ~~The SI shall indemnify and hold harmless the DoP from and against any and all losses, damages, or claims arising out of or in connection with any such infringement or alleged infringement~~	As per RFP

Response to the Pre-Bid Queries

14 92	iii	Pg, 19 1.6.1 Representations and Warranties of the SI	Insertion of new clause	Except for the foregoing, SI excludes and disclaims all warranties, conditions, or statements, whether express, implied, or statutory, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, or that deliverables will be error- free.	As per RFP

Response to the Pre-Bid Queries

14 93	iii	Pg, 20 1.6.2 Representations and Warranties of the DoP	f) it has complied with Applicable Laws in all material respects.	f) it has complied with Applicable Laws, <u>rules, or</u> <u>regulations applicable to the</u> <u>performance of its obligations</u> <u>under this Agreement, each</u> <u>as amended from time to time</u> in all material respects.	As per RFP

Response to the Pre-Bid Queries

14 94	iii	Pg, 20 1.7.1 Obligations of the DoP	Insertion of new clause	SI's failure to perform or delay in performing its contractual responsibilities (in whole or in part), to perform any part of the Services (whether in conformance with the Agreement or at all), or to meet any agreed service levels shall be excused if and to the extent SI's non-performance is contributed to by DoP's act or omission to act, delay, wrongful action, failure to provide inputs, or failure to perform its obligations under this Agreement. DoP shall in this regard also be responsible for the acts and omissions of its nominated agencies and other suppliers and advisors. Further, in the event of a default by DoP (or its nominated agencies) contributing to any loss or damage, the liability of SI shall be reduced to the extent related to DoP (or its nominated agencies) act or omission.	As per RFP

Response to the Pre-Bid Queries

14 95	iii	Pg, 21 1.7.2 Obligations of the SI	b) It shall perform the Services as set out in clause 1.2 of this Agreement with standards of professional skill, care, diligence, and in workmanlike manner fully consistent with industry best practices and internationally recognized technical and engineering standards applicable to projects of similar scale, and complexity, and commensurate with industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, and so as to comply with the applicable Service Levels specifications, functional requirements, and quality parameters Set out in the Vol 2 of the RFP.	b) It shall perform the Services as set out in clause 1.2 of this Agreement with standards of professional skill, care, diligence, and in workmanlike manner fully consistent with industry best practices and internationally recognized technical and engineering standards applicable to projects of similar scale, and complexity, and commensurate with industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, and so as to comply with the applicable Service Levels specifications, functional requirements, and quality parameters Set out in the Vol 2 of the RFP.	As per RFP

Response to the Pre-Bid Queries

14 96	iii	Pg, 30 1.13.4 Termination for Convenience	The DoP may, by written notice of 60 (sixty) days sent to the SI, terminate the Agreement, in whole at any time for its convenience. The notice of termination shall specify that termination is for the DoP's convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective.	The DoP may, by written notice of ~~60 (ninety-sixty)~~ days sent to the SI, terminate the Agreement, in whole <u>or in part</u>, at any time for its convenience. The notice of termination shall specify that termination is for the DoP's convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective. <u>The SI may, by written notice of 90 (ninety) days sent to the DoP, terminate the Agreement, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the SI's convenience, the extent to which the performance of work under the Agreement is terminated, and the date upon which such termination becomes effective. In the event of termination of this Agreement for convenience by either Party, the DoP shall pay the SI: (a) all fees and expenses for services performed up to the effective date of termination, including work in progress; (b) fees for the applicable notice period, irrespective of whether the DoP requires the SI's services during such period; (c) any termination charges agreed by the Parties or as may have been set out in the applicable SOW; and (d) any unamortized costs for lease.</u>	As per RFP

Response to the Pre-Bid Queries

				<u>licenses or other materials procured by the SI for the DoP.</u>	

Response to the Pre-Bid Queries

14 97	iii	Pg, 32 1.14.1 General Indemnity	Subject to Clause 1.14.3 below, SI (the "Indemnifying Party") undertakes to indemnify DoP (the "Indemnified Party"), its officers, employees, agents, and representatives, from and against all claims (including third party claims), losses, liabilities, compensation, expenses (including reasonable attorneys' fees), fines, penalties, taxes, interest or damages etc. (Collectively "Loss") on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or willful default, lack of due care or breach of terms under this Agreement. The Indemnifying Party shall also indemnify Indemnified Party from and against all direct monetary losses, damages etc. arising out of any defect, fault, deficiency in the applications, software licenses, hardware and other components of the Project provided and/or maintained by the Indemnifying Party or any of its sub-contractors etc and breach of its confidentiality obligation and Data Protection obligation.	Subject to Clause 1.14.3 below, SI (the "Indemnifying Party") undertakes to indemnify DoP (the "Indemnified Party"), its officers, employees, agents, and representatives, from and against ~~all claims (including all third party claims)~~, losses, liabilities, compensation, expenses (including reasonable attorneys' fees), fines, penalties, taxes, interest or damages etc. (Collectively "Loss") on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (~~excluding~~<u>including</u> the Indemnified Party) attributable to the Indemnifying Party's <u>gross negligence or willful default/misconduct</u>, lack of due care ~~or breach of terms under this Agreement~~. The Indemnifying Party shall also indemnify Indemnified Party from and against all ~~direct monetary~~<u>third party claims arising out of breach of its confidentiality obligation but shall not indemnify for direct</u> losses, damages etc. arising out of any defect, fault, deficiency in the applications, software licenses, hardware and other components of the Project provided and/or maintained by the Indemnifying Party or any of its sub-contractors ~~etc and, or for breach of its~~	As per RFP

Response to the Pre-Bid Queries

				confidential obligation and Data Protection obligation contract or performance failures, except to the extent such indemnity is required for third party claims as set out above.	

Response to the Pre-Bid Queries

14 98	iii	Pg, 32 1.14.1 General Indemnity	Further, Indemnifying Party shall protect and fully indemnify and keep indemnified the Indemnified Party from all claims, damages or compensation for breach of any provisions of the Digital Personal Data Protection Act, 2023, and/or any other applicable data protection or privacy laws, as amended from time to time.	~~Further, Indemnifying Party shall protect and fully indemnify and keep indemnified the Indemnified Party from all claims, damages or compensation for breach of any provisions of the Digital Personal Data Protection Act, 2023, and/or any other applicable data protection or privacy laws, as amended from time to time.~~	As per RFP

Response to the Pre-Bid Queries

14 99	iii	Pg, 32 1.14.2 IPR Indemnity	SI (Indemnifying Party) shall Indemnify, hold harmless, defend third-party claims against DoP (Indemnified Party) its directors, employees, agents and representatives from and against any costs, loss, damages, expense, claims, litigations, suits, actions, judgments, and or otherwise including but not limited to those from third parties or liabilities of any kind howsoever suffered, arising out of or incurred to infringement of Intellectual Property Rights including but not limited to patent, trademark, copy-rights or industrial drawings and designs arising from use of the Services/Deliverables or any part thereof and/or otherwise.	SI (Indemnifying Party) shall Indemnify, hold harmless, defend third-party claims against DoP (Indemnified Party) its directors, employees, agents and representatives from and against any costs, loss, damages, expense, claims, litigations, suits, actions, judgments, and or otherwise including but not limited to those from third parties or liabilities of any kind howsoever suffered, arising out of or incurred to infringement of Intellectual Property Rights including but not limited to ~~patent~~ , trademark, copy-rights or industrial drawings and designs arising from use of the Services/Deliverables or any part thereof and/or otherwise.	As per RFP

Response to the Pre-Bid Queries

15 00	iii	Pg, 33 1.14.2 IPR Indemnity	Insertion of new clause	SI shall not have any liability to DoP under this clause to the extent that any infringement or claim thereof is attributable to: (1) the combination, operation or use of a Developed Material or Services with equipment or software supplied by DoP where the Developed Material or Services would not itself be infringing; (2) compliance with designs, specifications, materials, inputs, or instructions provided by DoP; (3) use of a Developed Material or Services in an application or environment for which it was not designed or contemplated under this Agreement; or (4) modifications of a Developed Material or Services by anyone other than the SI where the unmodified version of the Developed Material or Services would not have been infringing.	As per RFP

Response to the Pre-Bid Queries

15 01	iii	Pg, 33 1.14.2 IPR Indemnity	In the event the System Integrator ("SI") is unable to procure the requisite rights to use, or to replace or modify the affected Services or Deliverables in accordance with the provisions of this Agreement, the SI shall accept the return of such Deliverables/Services and shall reimburse the Department of Posts ("DoP") for all amounts paid by DoP towards such Deliverables/Services.	In the event the System Integrator ("SI") is unable to procure the requisite rights to use, or to replace or modify the affected Services or Deliverables in accordance with the provisions of this Agreement, the SI shall accept the return of such Deliverables/Services and shall <u>pay a pro-rata refund of the charges paid to SI for ~~reimburse the Department of Posts ("DoP") for all amounts paid by DoP towards such infringing~~</u> Deliverables/Services. <u>The foregoing shall be SI's sole obligation and DoP's exclusive remedy in case of any infringement claim.</u>	As per RFP

Response to the Pre-Bid Queries

15 02	iii	Pg, 33 1.14.2 IPR Indemnity	Further, the SI shall compensate DoP for the reasonable and duly documented replacement costs incurred by DoP for procuring equivalent Deliverables/Services from an alternate source. Under no circumstances shall DoP be liable to bear any expense, charge, fee, or cost of any nature whatsoever arising out of or in connection with such non-performance or replacement.	~~Further, the SI shall compensate DoP for the reasonable and duly documented replacement costs incurred by DoP for procuring equivalent Deliverables/Services from an alternate source. Under no circumstances shall DoP be liable to bear any expense, charge, fee, or cost of any nature whatsoever arising out of or in connection with such non-performance or replacement.~~	As per RFP

Response to the Pre-Bid Queries

15 03	iii	Pg, 33 1.14.2 IPR Indemnity	Without prejudice to the foregoing, the SI shall also be liable to pay to DoP such reasonable liquidated damages or service credits, as applicable, for failure to meet the agreed service levels or performance obligations to the extent such failure arises from DoP's inability to use the proposed solution.	~~Without prejudice to the foregoing, the SI shall also be liable to pay to DoP such reasonable liquidated damages or service credits, as applicable, for failure to meet the agreed service levels or performance obligations to the extent such failure arises from DoP's inability to use the proposed solution.~~	As per RFP

Response to the Pre-Bid Queries

15 04	iii	Pg, 33 1.14.3 Conditions for Indemnity	ii. Immediately upon receipt of notification of any claim from the DoP, the SI within a period of 7 days from the date of receipt of such notice from the DoP, notify the DoP whether the SI wish to assume the defence concerning such claim (including settlement or resolution thereof). Thereafter, the SI shall be entitled in consultation with the DoP, and only to the extent such action does not in any manner compromise, prejudice or adversely affect the interests of the DoP, to take such action as mutually agreed upon by SI and the DoP to avoid, dispute, deny, resist, appeal, compromise or consent such claim, within a period of 30 days from the date of receipt of such claim notification;	ii. Immediately upon receipt of notification of any claim from the DoP, the SI within a period of 7 days from the date of receipt of such notice from the DoP, <u>shall</u> notify the DoP whether the SI <u>wishes</u> to assume the defence concerning such claim (including settlement or resolution thereof). Thereafter , ~~the SI shall be entitled in consultation with the DoP, and only to the extent such action does not in any manner compromise, prejudice or adversely affect the interests of the DoP, to take such action as mutually agreed upon by SI and the DoP to avoid, dispute, deny, resist, appeal, compromise or consent such claim, within a period of 30 days from the date of receipt of such claim notification;~~<u>if the SI assumes the defence, the SI shall have sole control over the defence and settlement of the claim.</u>	As per RFP

Response to the Pre-Bid Queries

15 05	iii	Pg, 33 1.14.3 Conditions for Indemnity	iii. Notwithstanding anything contained herein, the SI and the DoP agree and covenant that a notice by the DoP to the SI concerning the claim as aforesaid shall amount to express acceptance and consent by the SI to indemnify the DoP for all losses concerning such claim. Upon notice by the SI, the DoP shall reasonably cooperate with the SI at the sole costs of the SI, only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the DoP. The DoP shall have the right, at its option, to participate in the defence of such claim;	~~iii. Notwithstanding anything contained herein, the SI and the DoP agree and covenant that a notice by the DoP to the SI concerning the claim as aforesaid shall amount to express acceptance and consent by the SI to indemnify the DoP for all losses concerning such claim. Upon notice by the SI, the DoP shall reasonably cooperate with the SI at the sole costs of the SI, only to the extent the same does not in any manner compromise, prejudice or adversely affect the rights of the DoP. The DoP shall have the right, at its option, to participate in the defence of such claim; at its own expense.~~	As per RFP

Response to the Pre-Bid Queries

15 06	iii	Pg, 34 1.14.4 Risk Purchase	If the SI fails to perform its obligations (or any part thereof) under this Agreement or if the Agreement is terminated by the DoP due to breach of any obligations of the SI under this Agreement, DoP reserves the right to procure same or equivalent services/Deliverables from alternative sources at the SI's risk and responsibility. Any incremental cost borne by the DoP in procuring such services/ Deliverables shall be borne by the SI. Any such incremental cost incurred in the procurement of such services/ Deliverables from alternative source will be recovered from the undisputed pending due and payable payments / Performance Bank Guarantee provided by the SI under this Agreement and if the value of the services/Deliverables under risk purchase exceeds the amount of Performance Bank Guarantee, the same may be recovered, if necessary, by due legal process limited to 1.5 times the amount that was payable to SI for non-delivered services/ deliverables.	~~If the SI fails to perform its obligations (or any part thereof) under this Agreement or if the Agreement is terminated by the DoP due to breach of any obligations of the SI under this Agreement, DoP reserves the right to procure same or equivalent services/Deliverables from alternative sources at the SI's risk and responsibility. Any incremental cost borne by the DoP in procuring such services/ Deliverables shall be borne by the SI. Any such incremental cost incurred in the procurement of such services/ Deliverables from alternative source will be recovered from the undisputed pending due and payable payments / Performance Bank Guarantee provided by the SI under this Agreement and if the value of the services/Deliverables under risk purchase exceeds the amount of Performance Bank Guarantee, the same may be recovered, if necessary, by due legal process limited to 1.5 times the amount that was payable to SI for non-delivered services/ deliverables.~~	As per RFP

Response to the Pre-Bid Queries

15 07	iii	1.14.4 Risk Purchase	Notwithstanding anything to the contrary contained elsewhere in this Agreement, the rights and remedies of DoP under this clause, including recovery of incremental or replacement costs, shall prevail over any limitation of liability, indemnity cap, or any other clause restricting the SI's liability.	~~Notwithstanding anything to the contrary contained elsewhere in this Agreement, the rights and remedies of DoP under this clause, including recovery of incremental or replacement costs, shall prevail over any limitation of liability, indemnity cap, or any other clause restricting the SI's liability.~~	As per RFP

Response to the Pre-Bid Queries

15 08	iii	Pg, 34 1.14.5 Limitation of Liability	i. The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement.	i. The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed ~~one time the total contract value payable under this Agreement~~ <u>the average annual Charges (excluding taxes, reimbursements, and pass through expenses) paid to SI by DoP under the relevant SOW.</u> Notwithstanding anything herein to the contrary, <u>the maximum liability of the SI with respect to any privacy or data breach obligations shall not exceed two (2) times of applicable fees paid during the 12 months period.</u>	As per RFP

Response to the Pre-Bid Queries

15 09	iii	Pg, 34 1.14.5 Limitation of Liability	ii. Except as otherwise provided herein, in no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (, lost business, lost profits, or lost savings), even if it has been advised of their possible existence.	ii. Except as otherwise provided herein, in no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (~~including~~ lost business, lost profits, or lost savings), even if it has been advised of their possible existence.	As per RFP

Response to the Pre-Bid Queries

15 10	iii	Pg, 34 1.14.5 Limitation of Liability	iii. Notwithstanding anything contained in the foregoing, the liability cap and exclusion for the SI given under this Clause shall not apply to the claims that are subject indemnification obligations set out in this Clause and breach of Clauses 1.11.3 (Security and Safety), 1.16 (Confidentiality) damages arising from the gross negligence or willful misconduct or fraud of SI, its employees and subcontractor, loss or unauthorized disclosure by SI, its personnel or contractors, of data of DoP or those of its customers, Non compliance of Regulatory or Statutory guidelines applicable to bank, provided such guidelines were brought to the notice of Service Provide and breach of Intellectual Property Rights of a third party.	iii. Notwithstanding anything contained in the foregoing, the liability cap and exclusion for the SI given under this Clause shall not apply to the claims that are subject to indemnification obligations set out in the Clause 1.14.1 and 1.14.2 and ~~breach of Clauses 1.11.3 (Security and Safety), 1.16 (Confidentiality), or to~~ damages arising from the gross negligence or willful misconduct or fraud of SI, its employees and subcontractors, ~~loss or unauthorized disclosure by SI, its personnel or contractors, of data of DoP or those of its customers, Non compliance of Regulatory or Statutory guidelines applicable to bank, provided such~~ guidelines were brought to the notice of Service Provide and breach of Intellectual Property Rights of a third party.	As per RFP

Response to the Pre-Bid Queries

15 11	iii	Pg, 35 1.14.5 Limitation of Liability	Insertion of new clause	iv. <u>SI shall not be liable for any failure or delay by it to perform its obligations under this Agreement or any Statement of Work (including, but not limited to, any failure to achieve a Service Level) and the time by which such obligation shall be performed shall be automatically extended if that breach is caused or contributed to by: (a) any failure or delay of DoP, its nominated agencies or their respective employees in the performance of its obligations pursuant to this Agreement or any Statement of Work; (ii) any negligent or unlawful act or omission of DoP, its nominated agencies or their respective employees; (iii) any breach of contract or negligent act or omission on the part of any third party contractor or advisor employed by DoP or its nominated agencies; (iv) service or resource reductions requested or approved by DoP through the changes to services; (v) the failure of any software, tools or materials supplied to SI by the DoP or its nominated agencies.</u>	As per RFP

Response to the Pre-Bid Queries

15 12	iii	Pg, 35 1.14.6 Step-In-rights	In the event of the SI's failure to perform its obligations or breach of the Agreement, the DoP reserves the right to step in and procure equivalent services or deliverables from alternate sources at the SI's risk and cost. Any additional expenses incurred shall be recoverable from pending dues, the Performance Bank Guarantee, or through legal process.	In the event of the SI's failure to <u>remedy the defect(s)/delays within thirty (30) days from date of receipt of notice of such breach by the DoP and the defect becomes irremediable at SI's end</u> ~~perform its obligations or breach of the Agreement~~ , for a time period not to exceed <u>[thirty (30)] days from the date of DoP's receipt of a notice of breach by SI of such a nature</u> , the DoP reserves the right to step in and procure equivalent services or deliverables from alternate sources <u>and at the SI's risk and cost</u> ~~require SI to reimburse the DoP for any additional costs incurred in procuring such affected services from a third party up to a maximum incremental charges not exceeding 10% of the amount payable if the impacted services were procured from SI. This claim shall be payable if the Parties have failed to reach a resolution as per the governance process as stated in Section 1.22.14. DoP shall be entitled for only this relief. DoP may procure substitute services from third party for a maximum period of 30 days.~~ Any additional ~~expenses incurred shall be recoverable from pending dues, the Performance Bank Guarantee, or through legal process.~~	As per RFP

Response to the Pre-Bid Queries

15 13	iii	Pg, 35 1.14.6 Step-In-rights	DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding 15 days) for rectification. If the SI fails to remedy the default within the said period, DoP may exercise its step-in rights without further notice. Upon invocation of step-in, the SI shall provide DoP or its designated agency full access to project sites, systems, data, documentation, software, and any other resources reasonably required for continued delivery of services. The SI shall extend all cooperation and technical assistance to ensure smooth transition and continuity of operations. DoP shall have the right to use, for the duration of the step-in period, all project assets, equipment, tools, and licences (including third-party software licences, to the extent transferable or sublicensable) necessary for performance of services.	DoP may issue a written notice specifying the default and providing a reasonable period (not exceeding ~~30~~ ⁴⁵ days) for rectification. If the SI fails to remedy the default within the said period, DoP may exercise its step-in rights without further notice. Upon invocation of step-in, the SI shall provide DoP or its designated agency ~~full~~ <u>reasonable</u> access to project sites, systems, data, documentation, software, and any other resources reasonably required for continued delivery of services. ~~The SI shall extend all cooperation and technical assistance to ensure smooth transition and continuity of operations. DoP shall have the right to use, for the duration of the step-in period, all project assets, equipment, tools, and licences (including third party software licences, to the extent transferable or sublicensable) necessary for performance of services.~~	As per RFP

Response to the Pre-Bid Queries

15 14	iii	Pg, 35 1.14.6 Step-In-rights	Invocation of step-in rights shall not relieve the SI of its obligations, liabilities, or warranties under this Agreement, nor be construed as a waiver of any rights or remedies available to DoP.	~~Invocation of step-in rights shall not relieve the SI of its obligations, liabilities, or warranties under this Agreement, nor be construed as a waiver of any rights or remedies available to DoP.~~	As per RFP

Response to the Pre-Bid Queries

15 15	iii	Pg, 35 1.14.6 Step-In-rights	During the step-in period, the SI shall continue to be responsible for ensuring data integrity, confidentiality, and compliance with all applicable information security and regulatory requirements until the Department confirms formal transition of such responsibilities.	~~During the step-in period, the SI shall continue to be responsible for ensuring data integrity, confidentiality, and compliance with all applicable information security and regulatory requirements until the Department confirms formal transition of such responsibilities.~~	As per RFP

Response to the Pre-Bid Queries

15 16	iii	Pg, 35 1.14.6 Step-In-rights	If the Department's step-in rights remain in effect for a continuous period exceeding sixty (60) days, or if in the Department's reasonable opinion, the SI is unable to resume satisfactory performance of the affected Services within such period, the Department shall have the right to terminate the Statement of Work (SOW) for which the step-in was invoked, without any liability or penalty. Upon such termination, the Department may permanently retain control of all project materials, data, systems, and deliverables related to the affected SOW and may engage any third party to continue or complete the Services at the risk and cost of the SI. Such termination of an SOW under this clause shall not prejudice the Department's rights to claim damages, invoke the Performance Bank Guarantee, or recover any losses incurred due to the SI's failure.	If the Department's step-in rights remain in effect for a continuous period exceeding ~~thirtysixty (3060)~~ days, or if in the Department's reasonable opinion, the SI is unable to resume satisfactory performance of the affected Services within such period, the Department shall have the right to terminate the Statement of Work (SOW) for which the step-in was invoked, without any liability or penalty. ~~Upon such termination, the Department may permanently retain control of all project materials, data, systems, and deliverables related to the affected SOW and may engage any third party to continue or complete the Services at the risk and cost of the SI. Such termination of an SOW under this clause shall not prejudice the Department's rights to claim damages, invoke the Performance Bank Guarantee, or recover any losses incurred due to the SI's failure.~~	As per RFP

Response to the Pre-Bid Queries

15 17	iii	1.15.3 Notification Procedure for Force Majeure	iii. DoP may terminate the Contract / Agreement, by giving a written notice of minimum 30 (Thirty) days to SI, if as a result of Force Majeure the SI is unable to perform a material portion of the Service(s) for a period of more than 60 (Sixty) days. Notwithstanding such termination, the SI shall remain responsible for complying with its obligations under the Exit Management provisions of this Agreement.	iii. ~~DoP~~ <u>Either Party</u> may terminate the Contract / Agreement, by giving a written notice of minimum 30 (Thirty) days to ~~SI~~ <u>the other Party</u> , if as a result of Force Majeure the ~~SI~~ <u>affected Party</u> is unable to perform a material portion of ~~the Service(s)~~ <u>its obligations under this Agreement</u> for a period of more than 60 (Sixty) days. Notwithstanding such termination, the SI shall remain responsible for complying with its obligations under the Exit Management provisions of this Agreement.	As per RFP

Response to the Pre-Bid Queries

15 18	iii	Pg, 38 1.16 Confidentiality	i. The DoP or its nominated agencies may allow the SI to utilize highly Confidential Information including confidential public records and the SI shall maintain the highest level of secrecy, confidentiality and privacy concerning such Confidential Information.	~~i. The DoP or its nominated agencies may allow the SI to utilize highly Confidential Information including confidential public records and the SI~~ <u>Each Party ("Recipient") shall keep confidential and not disclose to any third party any Confidential Information (as defined in this Agreement) of the other Party ("Disclosing Party") disclosed in connection with this Agreement, and shall maintain the highest level of secrecy, confidentiality and privacy concerning such Confidential Information.</u>	As per RFP

Response to the Pre-Bid Queries

15 19	iii	Pg, 38 1.16 Confidentiality	iii. The DoP or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action against the SI regarding any forbidden disclosure. The DoP reserves the right to adopt legal proceedings, civil or criminal, against the SI concerning a dispute arising out of a breach of obligation by the SI under this clause.	~~iii. The DoP or its nominated agencies~~ <u>Each Party</u> shall retain all rights to prevent, stop and if required take the necessary ~~punitive~~ action against the ~~SI~~ <u>Other Party</u> regarding any forbidden disclosure. ~~The DoP~~ <u>Each Party</u> reserves the right to adopt legal proceedings, civil or criminal, against the ~~SI~~ <u>Other Party</u> concerning a dispute arising out of a breach of obligation ~~by the SI~~ under this clause.	As per RFP

Response to the Pre-Bid Queries

15 20	iii	Pg, 38 1.16 Confidentiality	v. The SI may only disclose the Confidential Information in the following circumstances:	v. ~~The SI may only disclose the Confidential Information~~ <u>may only be disclosed</u> in the following circumstances:	As per RFP

Response to the Pre-Bid Queries

15 21	iii		a. with the prior written consent of the DoP;	a. with the prior written consent of the ~~DoP~~ <u>Disclosing Party</u> ;	As per RFP

Response to the Pre-Bid Queries

15 22	iii		b. to a member of the SI's Team ("Authorized Person") provided the Authorized Person needs to know the Confidential Information for the accomplishment of the Services and the Authorized Person has executed a confidentiality agreement with the DoP before receiving such information; and	b. to a member of the ~~SI's Team~~ <u>Recipient's team</u> ("Authorized Person") provided the Authorized Person needs to know the Confidential Information for the accomplishment of the Services and the Authorized Person has executed a confidentiality agreement with the ~~DoP~~ <u>Disclosing Party</u> before receiving such information; and	As per RFP

Response to the Pre-Bid Queries

15 23	iii		c. if and to the extent that the SI is compelled legally to disclose the Confidential Information.	c. if and to the extent that the SI is compelled legally to disclose the Confidential Information.	As per RFP

Response to the Pre-Bid Queries

15 24	iii	Pg, 38 1.16 Confidentiality	vi. When the SI is aware of any steps being taken or considered to compel legally the SI or an Authorized Person to disclose the Confidential Information, it shall:	~~vi. When the SI is aware of any steps being taken or considered to compel legally the SI or an Authorized Person, if and to the extent that the Recipient is compelled legally to disclose the Confidential Information, it shall:~~	As per RFP

Response to the Pre-Bid Queries

15 25	iii		a. To the extent legally permitted, defer and limit the disclosure to preserve the confidentiality of the Confidential Information as much as possible;	a. To the extent legally permitted, defer and limit the disclosure to preserve the confidentiality of the Confidential Information as much as possible;	As per RFP

Response to the Pre-Bid Queries

15 26	iii		b. Promptly notify the DoP; and	b. Promptly notify the DoP; and	As per RFP

Response to the Pre-Bid Queries

15 27	iii		c. Do anything reasonable required by the DoP to oppose or restrict that disclosure.	c. Do anything reasonable required by the DoP to oppose or restrict that disclosure.	As per RFP

Response to the Pre-Bid Queries

15 28	iii	Pg, 39 1.16 Confidentiality	vii. The SI shall notify the DoP promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Agreement or with the authority of the DoP.	vii. The ~~SI~~ <u>Recipient</u> shall notify the ~~DoP~~ <u>Disclosing Party</u> promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by this Agreement or with the authority of the ~~DoP~~ <u>Disclosing Party</u> .	As per RFP

Response to the Pre-Bid Queries

15 29	iii	Pg, 39 1.16 Confidentiality	viii. The SI shall not carry any written material, layout, diagrams, floppy diskettes, pen drive, CDs, hard disks, storage tapes or any other media out of the DoP premise without written permission from the DoP. The SI's personnel shall follow the DoP's Information Security policy and Cyber Crisis Management Plan or any other related policy or guideline issued from time to time. The SI acknowledges that the DoP's business data and other DoP proprietary information or materials, whether developed by the DoP or being used by the DoP according to a license agreement with a third party (the foregoing collectively referred to herein as "Proprietary Information") are confidential and proprietary to the DoP shall at all times remain the sole and exclusive property of DoP; and the SI agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by the SI to protect its proprietary information. The SI recognizes that the goodwill of the DoP depends, among other things, upon keeping such proprietary information confidential and that unauthorized disclosure of the same by the SI could damage the DoP, and that because of the SI's duties hereunder, the SI may come into possession of such	viii. The ~~SI~~<u>Recipient</u> shall not carry any written material, layout, diagrams, floppy diskettes, pen drive, CDs, hard disks, storage tapes or any other media out of the ~~DoP~~<u>Disclosing Party's</u> premise without written permission from the ~~DoP~~<u>Disclosing Party</u>. The ~~SI~~<u>Disclosing Party</u> The <u>Recipient's</u> personnel shall follow the ~~DoP~~<u>Disclosing Party's</u> Information Security policy and Cyber Crisis Management Plan or any other related policy or guideline issued from time to time. The ~~SI~~<u>Recipient</u> acknowledges that the ~~DoP~~<u>Disclosing Party's</u> business data and other ~~DoP~~ proprietary information or materials, whether developed by the ~~DoP~~<u>Disclosing Party</u> or being used by the ~~DoP~~<u>Disclosing Party</u> according to a license agreement with a third party (the foregoing collectively referred to herein as "Proprietary Information") are confidential and proprietary to the ~~DoP~~<u>Disclosing Party</u> and shall -at all times remain the sole and exclusive property of ~~DoP~~<u>the Disclosing Party</u>; and the ~~SI~~<u>Recipient</u> agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by the ~~SI~~<u>Recipient</u>	As per RFP

Response to the Pre-Bid Queries

		proprietary information, even though the SI does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this Agreement. The SI shall use such information only to perform the said services. The SI shall, upon termination of this Agreement for any reason, or upon demand by the DoP, whichever is earliest return all information provided to the SI by the DoP, including any copies or reproductions, both hardcopy and electronic or destroy, if incapable of return.	to protect its proprietary information. The ~~SI~~<u>Recipient</u> recognizes that the goodwill of the ~~DoP~~<u>Disclosing Party</u> depends, among other things, upon keeping such proprietary information confidential and that unauthorized disclosure of the same by the ~~SI~~<u>Recipient</u> could damage the ~~DoP~~<u>Disclosing Party</u>, and that because of the ~~SI~~<u>Recipient's</u> duties hereunder, the ~~SI~~<u>Recipient</u> may come into possession of such proprietary information, even though the ~~SI~~<u>Recipient</u> does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this Agreement. The ~~SI~~<u>Recipient</u> shall use such information only to perform the said services. The ~~SI~~<u>Recipient</u> shall, upon termination of this Agreement for any reason, or upon demand by the ~~DoP~~<u>Disclosing Party</u>, whichever is earliest, return all information provided to the ~~SI by the DoP~~<u>Recipient by the Disclosing Party</u>, including any copies or reproductions, both hardcopy and electronic or destroy, if incapable of return.	

Response to the Pre-Bid Queries

15 30	iii	Pg, 39 1.16 Confidentiality	ix. The System Integrator ("SI") shall protect the Confidential Information of DoP with the same degree of care that it uses to protect its own confidential information of a similar nature, but in no event with less than a reasonable standard of care. The obligations under this Clause shall survive the expiry, cancellation, or termination of this Agreement and shall continue until such Confidential Information lawfully enters the public domain without any breach of this Agreement.	ix. ~~The System Integrator ("SI")~~ Each Party shall protect the Confidential Information of ~~DoP~~ the other Party with the same degree of care that it uses to protect its own confidential information of a similar nature, but in no event with less than a reasonable standard of care. The obligations under this Clause shall survive the expiry, cancellation, or termination of this Agreement and shall continue ~~until such Confidential Information lawfully enters the public domain without any breach of this Agreement~~ for a period of three (3) years from the date of disclosure of such Confidential Information, except for Confidential Information that constitutes a trade secret, which shall be protected for so long as it remains a trade secret under applicable law.	As per RFP

Response to the Pre-Bid Queries

15 31	iii	Pg, 40 1.16 Confidentiality	x. Notwithstanding the foregoing, the Parties acknowledge that the nature of the services to be performed under this Contract may require the SI's personnel to be present on the premises of the DoP or to have access to the DoP's computer networks and databases while on or off such premises. It is understood that it would be impractical for the DoP to monitor all information made available to the SI under such circumstances or to provide notice to the SI of the confidentiality of all such information. Therefore, the SI agrees that any technical, business, or other information of the DoP that the SI's personnel, subcontractors, or agents acquire while on the DoP's premises, or through access to the DoP's computer systems or databases while on or off the DoP's premises, shall be deemed Confidential Information	x. Notwithstanding the foregoing, the Parties acknowledge that the nature of the services to be performed under this Contract may require ~~the SI's~~ personnel to be present on the premises of the ~~DoP~~<u>Other Party</u> or to have access to the ~~DoP~~<u>Other Party's</u> computer networks and databases while on or off such premises. It is understood that it would be impractical for ~~the DoP~~<u>either Party</u> to monitor all information made available to the ~~SI~~<u>Other</u> under such circumstances or to provide notice ~~to the SI~~ of the confidentiality of all such information. Therefore, ~~the SI~~<u>the SI</u> ~~agrees that~~ any technical, business, or other information of ~~the DoP~~<u>the Other Party</u> that the ~~SI~~<u>Other Party's</u> personnel, subcontractors, or agents acquire while on the ~~DoP~~<u>Other Party's</u> premises, or through access to the ~~DoP~~<u>Other Party's</u> computer systems or databases while on or off the ~~DoP~~<u>Other Party's</u> premises, shall be deemed Confidential Information.	As per RFP

Response to the Pre-Bid Queries

15 32	iii	Pg, 40 1.16 Confidentiality	Insertion of new clause	xi. <u>Confidential Information shall not include information that: (a) is or becomes part of the public domain through no fault of the Recipient; (b) is lawfully received from a third party without any obligation of confidentiality; (c) was already in the Recipient's possession prior to disclosure by the Disclosing Party; (d) is independently developed by the Recipient without use of or reference to the Disclosing Party's Confidential Information; or (e) is required to be disclosed by law, regulation, or court order, provided that the Recipient gives prompt written notice to the Disclosing Party (where legally permitted) and cooperates with the Disclosing Party to seek a protective order or other appropriate remedy.</u>	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

15 33	iii	Pg. 40 1.17 Audit, Access and Reporting	i. The DoP reserves the right to inspect and monitor/assess the progress of the Project at any time during the course of the Agreement, after providing due notice to the SI. The DoP may demand and upon such demand being made, the DoP shall be provided with any document, data, material or any other information which it may require, to enable it to assess the progress of the Project, systems, records, and personnel.	i. The DoP reserves the right to inspect and monitor/assess the progress of the Project ~~at any time~~ during the course of the Agreement, after providing ~~due~~ <u>a written notice of thirty (30) days</u> to the SI. The DoP may demand and upon such demand being made, the DoP shall be provided with ~~any~~ document, data, material or any other information which it may require, to enable it to assess the progress of the Project, systems, records, and personnel <u>in connection with the supply of the Services only.</u>	As per RFP

Response to the Pre-Bid Queries

15 34	iii	Pg. 40 1.17 Audit, Access and Reporting	ii. The DoP shall also have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by the SI of its obligations/functions following the standards committed to or required by the DoP and the SI undertakes to cooperate with and provide to the DoP/ any other agency appointed by the DoP, all documents and other details as may be required by them for this purpose. Any deviations or contraventions, identified as a result of such audit/assessment, would need to be rectified by the SI failing which the DoP may, without prejudice to any other rights that it may have issued a notice of default. The cost of acquisition of deliverables by the SI is out of the purview of audit/inspections.	ii. The DoP shall also have the right to conduct, either itself or through another agency <u>(who shall not be a competitor of the SI)</u> as it may deem fit, an audit to monitor the performance by the SI of its obligations/functions following the standards committed to or required by the DoP and the SI undertakes to cooperate with and provide to the DoP/ any other agency appointed by the DoP, all documents and other details as may be required by them for this purpose <u>in connection with the supply of the Services.</u> Any deviations or contraventions, identified as a result of such audit/assessment, would need to be rectified by the SI failing which the DoP may, without prejudice to any other rights that it may have issued a notice of default. The cost of acquisition of deliverables by the SI is out of the purview of audit/inspections.	As per RFP

Response to the Pre-Bid Queries

15 35	iii	Pg. 40 1.17 Audit, Access and Reporting	Insertion of new clause	<u>iv. Parties agree that the scope of the audit shall not extend to the SI's internal costs, personal or confidential information of the SI or any of its customers.</u>	As per RFP

Response to the Pre-Bid Queries

15 36	iii	Pg. 40 1.18 Ownership and Intellectual Property Rights	a) Pre-existing work: All intellectual property rights existing before the Effective Date of this Agreement shall belong to the Party that owned such rights immediately before the Effective Date. Subject to the foregoing, the DoP will also have rights to use and copy all processes, specifications, reports and other document drawings, manuals, deliverables, including but not limited to processes, specifications, reports, drawings, manuals, configuration scripts, system architecture documents, integration code, DR automation scripts, and any other materials created or delivered as part of the Services under this Agreement and other documents, the entire services provided by SI as part of the Scope of Works under this Agreement on non-exclusive, transferable, (including the right to sublicense to DoP's contractors, affiliates, or successor service providers) perpetual, royalty-free license to use, copy, maintain and modify for DoP's internal business purposes.	a) Pre-existing work: All intellectual property rights existing before the Effective Date of this Agreement shall belong to the Party that owned such rights immediately before the Effective Date. Subject to the foregoing, the DoP will also have rights to use and copy all processes, specifications, reports and other document drawings, manuals, deliverables, including but not limited to processes, specifications, reports, drawings, manuals, configuration scripts, system architecture documents, integration code, DR automation scripts, and any other materials created or delivered as part of the Services under this Agreement and other documents, the entire services provided by SI as part of the Scope of Works under this Agreement on non-exclusive, transferable, (including the right to sublicense to DoP's contractors, affiliates, or successor service providers) perpetual, royalty-free license to use, copy, maintain and modify for DoP's internal business purposes. <u>Notwithstanding the foregoing, SI retains all rights, title and interest in and to any methodologies, tools, frameworks, software, know-how, techniques, or other materials that are of a</u>	As per RFP

Response to the Pre-Bid Queries

				<u>general abstract character or may be generically re-used ("Service Provider Materials"), including any modifications or enhancements thereto, except to the extent such materials are expressly identified as Deliverables. To the extent any Service Provider Materials are necessarily required for the proper functioning of the Deliverables or are embedded into the Deliverables, SI grants to DoP a perpetual, non-exclusive, non-transferable, royalty-free license to use such Service Provider Materials solely in conjunction with its anticipated use of such Deliverables.</u>	

Response to the Pre-Bid Queries

15 37	iii	Pg. 41 1.18 Ownership and Intellectual Property Rights	For the avoidance of doubt, it is clarified that no additional payment shall be made to SI for the right and non-exclusive, non-transferable, perpetual, royalty-free license to use basis grant of the aforesaid license right to DoP, including the right to use, maintain and modify the deliverables and any background IP embedded therein.	For the avoidance of doubt, it is clarified that no additional payment shall be made to SI for the right and non-exclusive, non-transferable, perpetual, royalty-free license to use basis grant of the aforesaid license right to DoP, including the right to use, maintain and modify the deliverables and any background IP embedded therein, <u>provided that such rights are subject to full payment of the applicable fees for the relevant Deliverables.</u>	As per RFP

Response to the Pre-Bid Queries

15 38	iii	Pg. 41 1.18 Ownership and Intellectual Property Rights	b) Bespoke Development: The DoP shall own and have a right in perpetuity to use and sublicense all newly created Intellectual Property Rights that have solely arisen out of or have been developed solely during the execution of this Agreement, including but not limited to all processes, products, specifications, reports, drawings and other documents which have been newly created and developed by the SI solely during the performance of the Services. The SI undertakes to disclose all such Intellectual Property Rights arising in the performance of the Services to the DoP and execute all such agreements/documents file all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the DoP. The SI shall treat all materials related to bespoke development as Confidential Information under this Agreement. This will also include any developments/customization done on COTS for the DoP. Any solution/framework that does not meet the definition of COTS shall be treated as bespoke development.	b) Bespoke Development: The DoP shall own and have a right in perpetuity to use and sublicense all newly created Intellectual Property Rights that have solely arisen out of or have been developed solely during the execution of this Agreement, including but not limited to all processes, products, specifications, reports, drawings and other documents which have been newly created and developed by the SI solely during the performance of the Services. The SI undertakes to disclose all such Intellectual Property Rights arising in the performance of the Services to the DoP and execute all such agreements/documents file all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the DoP. The SI shall treat all materials related to bespoke development as Confidential Information under this Agreement. This will also include any developments/customization done on COTS for the DoP. Any solution/framework that does not meet the definition of COTS shall be treated as bespoke development. <u>Notwithstanding the foregoing, the transfer of ownership of Intellectual</u>	As per RFP

Response to the Pre-Bid Queries

				Property Rights in Deliverables shall be effective only upon full payment of the applicable fees by DoP for such Deliverables. Until such payment is made, DoP shall have a limited, revocable license to use the Deliverables solely for internal business purposes.	

Response to the Pre-Bid Queries

15 39	iii	Pg. 41 1.18 Ownership and Intellectual Property Rights	c) Third Party Products: If license agreements are necessary or appropriate between the SI and third parties for purposes of enabling/enforcing/implementing the provisions hereinabove, the SI shall enter into such agreements at its own sole cost, expense and risk. Further, the SI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for the delivery of Services by the SI and for use of the Deliverables, applications, services etc. (including, inter alia, licenses for Commercially-Off-The-Shelf software and products) provided by the SI under this Agreement shall be acquired in the name of the DoP and shall be assigned/sublicensed by the DoP to the SI (to the extent legally and contractually permissible) for execution of any of its obligations under the terms of this Agreement. However, after the term of this Agreement, such approvals registrations, licenses, permit rights etc. shall inure to the exclusive benefit of the DoP, subject to OEM terms and renewal fees (if any), without any additional costs to the DoP.	c) Third Party Products: If license agreements are necessary or appropriate between the SI and third parties for purposes of enabling/enforcing/implementing the provisions hereinabove, the SI shall enter into such agreements at its own sole cost, expense and risk. Further, the SI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for the delivery of Services by the SI and for use of the Deliverables, applications, services etc. (including, inter alia, licenses for Commercially-Off-The-Shelf software and products) provided by the SI under this Agreement shall be acquired in the name of the DoP and shall be assigned/sublicensed by the DoP ~~to the SI~~ (to the extent legally and contractually permissible) for execution of any of its obligations under the terms of this Agreement. However, after the term of this Agreement, such approvals registrations, licenses, permit rights etc. shall inure to the exclusive benefit of the DoP, subject to OEM terms and renewal fees (if any), without any additional costs to the DoP. <u>For any third party materials provided by DoP to SI, DoP warrants that it has all rights</u>	As per RFP

Response to the Pre-Bid Queries

				<u>to sublicense or transfer such materials for their intended purpose and shall indemnify SI from any third party claims arising from such use.</u>	

Response to the Pre-Bid Queries

15 40	iii	Pg. 42 1.18 Ownership and Intellectual Property Rights	e) The ownership of all IPR rights in any and all documents, artefacts, etc. (including all training materials) made during the Term for implementation of the Project under this Agreement shall vest in DoP upon creation. The SI retains ownership of its Background IP but grants DoP a perpetual license to use any embedded components necessary for continued operation and maintenance.	e) The ownership of all IPR rights in any and all documents, artefacts, etc. (including all training materials) made during the Term for implementation of the Project under this Agreement shall vest in DoP upon creation. The SI retains ownership of its Background IP but grants DoP a perpetual license to use any embedded components necessary for continued operation and maintenance, <u>subject to full payment for the relevant Deliverables.</u>	As per RFP

Response to the Pre-Bid Queries

15 41	iii	Pg. 42 1.19.1 Standard	i. The SI warrants that the Project, including all the systems(s), materials and goods supplied pursuant to this Agreement, shall be free from any defect or deficiency in the material and goods supplied pursuant to this Agreement, shall be free from any defect or deficiency in the material, design, engineering, and workmanship that prevent the system and/ or any of its systems from fulfilling the technical requirements or that limit in a material fashion the performance, reliability, or extensibility of the system and/or any of its sub-system(s). Commercial warranty provisions of products supplied under the Agreement shall apply to the extent they do not conflict with the provisions of this Agreement.	i. The SI warrants that the Project, including all the systems(s), materials and goods supplied pursuant to this Agreement, shall be free from any ~~defect or deficiency in the material and goods supplied pursuant to this Agreement, shall be free from any material~~ defect or deficiency in the material, design, engineering, and workmanship that prevent the system and/-or any of its systems from fulfilling the technical requirements or that limit in a material fashion the performance, reliability, or extensibility of the system and/or any of its sub-system(s). Commercial warranty provisions of products supplied under the Agreement shall apply to the extent they do not conflict with the provisions of this Agreement.	As per RFP

Response to the Pre-Bid Queries

15 42	iii	Pg. 43 1.19.1 Standard	iv. DoP should approve signoff within 15 working days from the submission of deliverables for Go-Live (as relevant, depending on project requirement) by the SI.	DoP should approve signoff within 15 working days from the submission of deliverables for Go-Live (as relevant, depending on project requirement) by the SI. <u>The standard of review of the deliverables shall be material conformance with the agreed specifications. By the expiration of such review period, DoP will submit a written statement to the SI indicating acceptance of the deliverables or specifying in detail how the submitted deliverables fail to materially conform to the agreed specification, in which case SI shall be afforded a commercially reasonable period of time not less than thirty (30) days to correct any nonconformities, whereupon the review cycle will recommence.</u>	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

15 43	iii	Pg. 43 1.19.1 Standard	iv. In case the DoP fails to respond and provide feedback on the above stated submission, the deliverables will be deemed accepted for the commencement of warranty for the Project.	In case the DoP fails to respond and provide feedback on the above stated submission, the deliverables will be deemed accepted for the commencement of warranty for the Project. <u>Deliverables will also be deemed accepted if DoP uses the deliverable in a production environment, whichever occurs first.</u>	As per RFP

Response to the Pre-Bid Queries

15 44	iii	Pg. 43 1.19.1 Standard	v. If during the warranty period any defect or deficiency is found in the material, design and performance/workmanship of the Project and other Services provided by the SI, the SI shall promptly, in consultation and agreement with DoP, and at the SI's sole cost repair, replace, or otherwise make good (as the SI shall, at its discretion, determine) such default, defect or deficiency as well as any damage to the system caused by such default, defect or deficiency. Any defective component, excluding hard disks, that has been replaced by the SI shall remain the property of the SI.	v. If during the warranty period any <u>material</u> defect or deficiency is found in the material, design and performance/workmanship of the Project and other Services provided by the SI, the SI shall promptly, in consultation and agreement with DoP, and at the SI's sole cost repair, replace, or otherwise make good (as the SI shall, at its discretion, determine) such default, defect or deficiency as well as any damage to the system caused by such default, defect or deficiency. Any defective component, excluding hard disks, that has been replaced by the SI shall remain the property of the SI.	As per RFP

Response to the Pre-Bid Queries

15 45	iii	Pg. 44 1.19.2 Implied Warranty	The warranties provided herein are in lieu of all other warranties, both express and implied, to the extent permitted by applicable law. Notwithstanding the foregoing, the Supplier does not disclaim (a) any warranty that the Deliverables will conform to the specifications, documentation, or agreed service levels, or (b) any warranty that cannot lawfully be excluded. The warranties set out in this clause are in addition to and not in substitution for any other warranties, representations, conditions, or remedies available to the DoP under this Agreement or applicable law.	The warranties provided herein are in lieu of all other warranties, both express and implied. <u>Except for the express warranties set out above, the SI excludes and disclaims all other warranties, conditions or statements, whether express, implied or statutory, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, or that deliverables will be error-free, to the extent permitted by applicable law.</u> Notwithstanding the foregoing, the ~~Supplier~~ <u>SI</u> does not disclaim (a) any warranty that the Deliverables will conform to the specifications, documentation, or agreed service levels, or (b) any warranty that cannot lawfully be excluded. ~~The warranties set out in this clause are in addition to and not in substitution for any other warranties, representations, conditions, or remedies available to the DoP under this Agreement or applicable law.~~	As per RFP

Response to the Pre-Bid Queries

15 46	iii	Pg. 45 1.21 Escrow Management	i. The SI shall, within a period not exceeding six (6) weeks from the date of issuance of the Letter of Award under the RFP, or within such period as may be reasonably specified by the DoP in writing, commence the required activities, deposit the Source Code of the existing functionalities/applications (as instructed in Volume II of the RFP) with Escrow Agent based on the appropriate standard agreement or on such other terms as the DoP, the SI and the Escrow Agent shall agree. For new implementations or enhancements, the SI shall deposit the Source Code (as instructed in Volume II of the RFP) along with the corresponding flow diagrams build scripts, configuration files, and technical documentation/write-up for the software within thirty (30) days of implementation.	~~i. The SI shall, within a period not exceeding six (6) weeks from the date of issuance of the Letter of Award under the RFP, or within such period as may be reasonably specified by the DoP in writing, commence the required activities, deposit the Source Code of the existing functionalities/applications (as instructed in Volume II of the RFP) with Escrow Agent based on the appropriate standard agreement or on such other terms as the DoP, the SI and the Escrow Agent shall agree. For new implementations or enhancements, the SI shall deposit the Source Code (as instructed in Volume II of the RFP) along with the corresponding flow diagrams build scripts, configuration files, and technical documentation/write-up for the software within thirty (30) days of implementation.~~	As per RFP

Response to the Pre-Bid Queries

15 47	iii	Pg. 45 1.21 Escrow Management	ii. The SI shall ensure that the deposited version of the Source Code is the current version of the POSB Solution and that the deposited version is kept up-to-date as the POSB Solution is modified or upgraded. The SI shall pay the initial storage fees renewal, and maintenance fee under the escrow agreement and the DoP shall only pay the release fees in the event of an actual release from escrow. The escrow agent and the escrow arrangement shall be geographically located in India.	~~i. The SI shall ensure that the deposited version of the Source Code is the current version of the POSB Solution and that the deposited version is kept up-to-date as the POSB Solution is modified or upgraded. The SI shall pay the initial storage fees renewal, and maintenance fee under the escrow agreement and the DoP shall only pay the release fees in the event of an actual release from escrow. The escrow agent and the escrow arrangement shall be geographically located in India.~~	As per RFP

Response to the Pre-Bid Queries

15 48	iii	Pg. 45 1.21 Escrow Management	iii. DoP shall have the right, either directly or through a third-party auditor/escrow agent, to periodically verify and/or test the completeness, accuracy, and usability of the Source Code and other materials deposited in escrow. Such verification may include compilation, build, and test of the deposited Source Code to ensure that it is sufficient and functional for DoP to use, maintain, and modify the Solution in accordance with this Agreement. The SI shall fully cooperate in such verification process and provide any necessary documentation, tools, instructions, or assistance. Any deficiencies errors, or missing components identified during such verification shall be rectified and re-deposited by the SI within a mutually agreed timeframe at no additional cost to DoP.	~~i. DoP shall have the right, either directly or through a third-party auditor/escrow agent, to periodically verify and/or test the completeness, accuracy, and usability of the Source Code and other materials deposited in escrow. Such verification may include compilation, build, and test of the deposited Source Code to ensure that it is sufficient and functional for DoP to use, maintain, and modify the Solution in accordance with this Agreement. The SI shall fully cooperate in such verification process and provide any necessary documentation, tools, instructions, or assistance. Any deficiencies errors, or missing components identified during such verification shall be rectified and re-deposited by the SI within a mutually agreed timeframe at no additional cost to DoP.~~	As per RFP

Response to the Pre-Bid Queries

15 49	iii	Pg. 45 1.21 Escrow Management	iv. In circumstances where the DoP obtains the release of the Source Code from escrow, the SI hereby grants to the DoP a perpetual, assignable, royalty-free, irrevocable, worldwide and exclusive license to use copy, modify, enhance and support the Source Code version of the POSB Solution to the extent necessary for the receipt of the Services or any Replacement Services or the DoP's normal business undertakings. Such license shall remain in effect and continue to be enforceable notwithstanding the expiration or termination of this Agreement, regardless of the reason.	~~i. In circumstances where the DoP obtains the release of the Source Code from escrow, the SI hereby grants to the DoP a perpetual, assignable, royalty-free, irrevocable, worldwide and exclusive license to use copy, modify, enhance and support the Source Code version of the POSB Solution to the extent necessary for the receipt of the Services or any Replacement Services or the DoP's normal business undertakings. Such license shall remain in effect and continue to be enforceable notwithstanding the expiration or termination of this Agreement, regardless of the reason.~~	As per RFP

Response to the Pre-Bid Queries

15 50	iii	Pg. 46 1.21 Escrow Management	v. In the event of (a) bankruptcy liquidation, or winding-up of the SI; (b) SI's material breach or persistent failure to perform its obligations under this Agreement; (c) SI's cessation or suspension of business operations; or (d) DoP's determination that the SI is unable or unwilling to continue the Project or maintain the POSB Solution , the DoP shall have the right to get the Source Code released from the escrow agent upon payment of the release fees. Upon such release, DoP shall be entitled to exercise all rights granted under sub-clause (iv) above, and the SI shall provide all reasonable transition assistance to enable DoP or its nominated third party to use and maintain the Solution without interruption.	~~i. In the event of (a) bankruptcy liquidation, or winding-up of the SI; (b) SI's material breach or persistent failure to perform its obligations under this Agreement; (c) SI's cessation or suspension of business operations; or (d) DoP's determination that the SI is unable or unwilling to continue the Project or maintain the POSB Solution , the DoP shall have the right to get the Source Code released from the escrow agent upon payment of the release fees. Upon such release, DoP shall be entitled to exercise all rights granted under sub-clause (iv) above, and the SI shall provide all reasonable transition assistance to enable DoP or its nominated third party to use and maintain the Solution without interruption.~~	As per RFP

Response to the Pre-Bid Queries

15 51	iii	Pg. 47 1.22.3 Subcontractors	a. Subject to the final discretion and prior written consent of the DoP, the SI may seek the appointment of a sub-contractor for the specific tasks mentioned in the RFP and thereby disclose the list of services it is subcontracting before execution of this Agreement. The terms of the contracts proposed to be entered into with the sub-contractors shall require the prior written approval of the DoP and shall be in conformity with the terms of the Agreement. Where the DoP deems necessary, it may refuse to consent to the delegation/sub-contracting of any part of scope of work. The SI shall ensure that all subcontractors engaged sign an agreement that is aligned in duration with this Agreement and remain available for the entire duration of this Agreement, unless otherwise approved in writing by the DoP.	a. Subject to the final discretion and prior written consent of the DoP, the SI may seek the appointment of a sub-contractor for the specific tasks mentioned in the RFP and thereby disclose the list of services it is subcontracting before execution of this Agreement. ~~The terms of the contracts proposed to be entered into with the sub-contractors shall require the prior written approval of the DoP and shall be in conformity with the terms of the Agreement.~~ Where the DoP deems necessary, it may refuse to consent to the delegation/sub-contracting of any part of scope of work. The SI shall ensure that all subcontractors engaged sign an agreement that is aligned in duration with this Agreement and remain available for the entire duration of this Agreement, unless otherwise approved in writing by the DoP.	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

15 52	iii	Pg. 49 1.22.4 Assignment	a. All terms and provisions of this Agreement shall be binding on and shall inure to the benefit of DoP and their respective successors and permitted assigns.	a. All terms and provisions of this Agreement shall be binding on and shall inure to the benefit of ~~DoP~~ <u>the Parties</u> and their respective successors and permitted assigns.	As per RFP

Response to the Pre-Bid Queries

15 53	iii	Pg. 49 1.22.4 Assignment	b. Except as otherwise expressly provided in this Agreement, and until the previous consent in writing of DoP is obtained, the SI shall not be permitted to assign its rights and obligations under this Agreement to any third party.	b. Except as otherwise expressly provided in this Agreement, ~~and until the previous consent in writing of DoP is obtained, the SI shall~~ neither Party may <u>assign or novate this Agreement or any of its rights or obligations hereunder, in whole or in part, without the prior written consent of the other Party, such consent not to be permitted to assign its rights and obligations under this Agreement to any third party</u> ~~unreasonably withheld or delayed.~~ Notwithstanding the foregoing, either Party may assign this Agreement to an Affiliate or in connection with a merger, acquisition, or sale of all or substantially all of its assets or business, provided that prior written notice is given to the other Party.	As per RFP

Response to the Pre-Bid Queries

15 54	iii	Pg. 49 1.22.4 Assignment	c. DoP may assign or novate all or any part of this Agreement and Schedules/Annexures, and the SI shall be a party to such novation, to any third party contracted to provide outsourced services to DoP or any of its nominees.	c. ~~DoP may assign or novate all or any part of this Agreement and Schedules/Annexures, and the SI shall be a party to such novation, to any third party contracted to provide outsourced services to DoP or any of its nominees.~~ Any assignment or novation in contravention of this clause shall be void and of no effect. <u>If the SI assigns this Agreement or any part thereof without such permission, DoP shall be entitled to treat it as a material breach of Agreement and avail any or all remedies as provided in this Agreement or at law or in equity, including the right to recover all losses, costs, damages, or expenses incurred as a result of such unauthorized act, and terminate the Agreement, in whole or in part, without any liability to the DoP.</u>	As per RFP

Response to the Pre-Bid Queries

15 55	iii	Pg. 49 1.22.4 Assignment	If the SI assigns this Agreement or any part thereof without such permission, DoP shall be entitled, and it shall be lawful on his part, to treat it as material breach of Agreement and avail any or all remedies as provided in this Agreement or at law or in equity, including the right to recover all losses, costs, damages, or expenses incurred as a result of such unauthorized act. And terminate the Agreement, in whole or in part, without any liability to the DoP	~~If the SI assigns this Agreement or any part thereof without such permission, DoP shall be entitled, and it shall be lawful on his part, to treat it as material breach of Agreement and avail any or all remedies as provided in this Agreement or at law or in equity, including the right to recover all losses, costs, damages, or expenses incurred as a result of such unauthorized act. And terminate the Agreement, in whole or in part, without any liability to the DoP~~	As per RFP

Response to the Pre-Bid Queries

15 56	iii	Pg. 49 1.22.5 Trademarks, Publicity	Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that the SI may, upon completion, use the Project as a reference for credential purposes. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that the SI may include the DoP or its client lists for reference to third parties subject to the prior written consent of the DoP. Such approval shall apply to each specific case and relate only to that case.	Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that the SI may, upon completion, use the Project as a reference for credential purposes. <u>Notwithstanding the foregoing, SI shall have the permission to use DoP's name and logo in identifying DoP as a client of SI, including in SI's client lists and marketing materials, provided that such use is in a manner that is not disparaging or misleading.</u> Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the SLA or the business of the Parties without prior reference to and approval in writing from the other Party, such approval not to be unreasonably withheld or delayed provided however that the SI may include the DoP or its client lists for reference to third parties subject to the prior written consent of the DoP. Such approval shall apply to each specific case and relate only to that case.	As per RFP

Response to the Pre-Bid Queries

15 57	iii	Pg. 52 1.22.9 Compliance with Applicable Law	a. The SI shall comply with the provision of all laws including the Digital Personal Data Protection Act, 2023, labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the DoP shall be applicable in the performance of this Agreement and the SI shall abide by these laws. The SI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. The SI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations. The SI shall also adhere to all security requirement/regulations of the DoP during the execution of the work.	a. The SI shall comply with the provision of ~~all~~ laws including ~~the Digital Personal Data Protection Act, 2023,~~ labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory agencies and by the DoP shall be applicable in the performance of this Agreement and the SI shall abide by these laws. The SI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. The SI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations. The SI shall also adhere to all security requirement/regulations of the DoP during the execution of the work.	As per RFP

Response to the Pre-Bid Queries

15 58	iii	Pg. 52 1.22.9 Compliance with Applicable Law	c. Each Party to this Agreement accepts that its individual conduct shall (to the extent applicable to its business like the SI as an information technology service provider) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be provided at no additional cost to the DoP.	c. Each Party to this Agreement accepts that its individual conduct shall (to the extent applicable to its business like the SI as an information technology service provider) at all times comply with all laws, rules and regulations of government and other bodies having jurisdiction over the area in which the Services are undertaken provided that changes in such laws, rules and regulations which result in a change to the Services shall be provided at ~~no~~ <u>no additional cost to the mutually agreed between DoP and SI in writing by executing an amendment.</u>	As per RFP

Response to the Pre-Bid Queries

15 59	iii	Pg. 52 1.22.9 Compliance with Applicable Law	d. During the tenure of this Agreement, the SI shall comply with all Applicable Laws and shall obtain and maintain all statutory and other approvals required for the performance of the Services under this Agreement and nothing shall be done by the SI in contravention of any Applicable Law or any amendment thereof and the SI shall keep the DoP indemnified in this regard.	d. During the tenure of this Agreement, the SI shall comply with all Applicable Laws and shall obtain and maintain all statutory and other approvals required for the performance of the Services under this Agreement and nothing shall be done by the SI in contravention of any Applicable Law or any amendment thereof ~~and the SI shall keep the DoP indemnified in this regard.~~	As per RFP

Response to the Pre-Bid Queries

15 60	iii	Pg. 53 1.22.2 Entire Agreement	a. This Agreement with all Schedules & Annexures appended thereto, and the contents and specifications of the RFP constitute the entire agreement between the Parties with respect to their subject matter, and as to all other representations, understandings or agreements which are not fully expressed herein, provided that nothing in this Clause shall be interpreted so as to exclude any liability in respect of fraud, misrepresentation and corrupt practice.	a. This Agreement, <u>together</u> with all Schedules ~~& and~~ Annexures appended ~~thereto, and the contents and specifications of the RFP constitute~~ <u>hereto, constitutes</u> the entire agreement between the Parties with respect to ~~their~~ <u>its</u> subject matter, and ~~as to all other~~ <u>supersedes all prior agreements,</u> representations, understandings or ~~agreements which are not fully expressed herein,~~ <u>provided that nothing arrangements,</u> whether written or oral, relating to such subject matter. Nothing in this Clause shall be interpreted so as to exclude any liability in respect of fraud, misrepresentation ~~and~~ <u>or</u> corrupt practice.	As per RFP

Response to the Pre-Bid Queries

15 61	iii	Pg. 53 1.22.2 Entire Agreement	b. Without prejudice to the generality of sub-clause 1.21.12 (a) above, on matters not covered by this Agreement, the provisions of RFP shall apply.	~~b. Without prejudice to the generality of sub-clause 1.21.12 (a) above, on matters not covered by this Agreement, the provisions of RFP shall apply.~~ <u>For the avoidance of doubt, in the event of any conflict between the provisions of this Agreement (including its Schedules and Annexures) and the RFP, the provisions of this Agreement shall prevail. The provisions of the RFP shall only apply to the extent expressly incorporated into this Agreement.</u>	As per RFP

Response to the Pre-Bid Queries

15 62	II	NA	NA	Is the upgrade to Finacle 10.2.25 mandatory within a fixed timeline , or mutually agreed post-award?	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

15 63	II	NA	NA	Please confirm the exact list of Finacle modules in scope (CASA, Loans, TD, GL, Govt Business, etc.).	As per RFP

Response to the Pre-Bid Queries

15 64	II	NA	NA	Is there any non finacle - UI/workflows that would be considered in the scope	As per RFP

Response to the Pre-Bid Queries

15 65	II	NA	NA	Please share Approximate count of: Custom menus Custom reports (Jrxml/mrt) Custom batch jobs Custom Integrations	As per RFP

Response to the Pre-Bid Queries

15 66	II	NA	NA	Are source codes and design documents for all customizations available?	Data is available for the current vendor via bugzilla and previous SI has shared FDMS dump for the old ones.

Response to the Pre-Bid Queries

15 67	II	NA	NA	Are there any bank-developed customizations unsupported by OEM, if not supported by current team at POSB?	No such customizations.

Response to the Pre-Bid Queries

15 68	II	NA	NA	Is there any regression automation tool used by bank for functional testing of Finacle CBS, Internet banking and Mobile banking and interfaces?	No.

Response to the Pre-Bid Queries

15 69	II	NA	NA	Please share current average EOD and EOM timeline/duration for CBS EOD.	Both are around 7-8 hours(3 steps at branch level and 3 steps at DC).

Response to the Pre-Bid Queries

15 70	II	NA	NA	Are there any known batch failures or spillovers in last 3 months?	No

Response to the Pre-Bid Queries

15 71	II	NA	NA	Is batch optimization considered as part of BAU. Has the same (NBR, sequencing etc) of batches revisited regularly?	Yes, batches are reviewed regularly.

Response to the Pre-Bid Queries

15 72	II	NA	NA	Are there known performance pain areas (modules, reports, channels)?	As per RFP

Response to the Pre-Bid Queries

15 73	II		NA	NA	Who owns SIT, UAT, and regression testing – Bank or SI?	Currently handled by DOP Team.

Response to the Pre-Bid Queries

15 74	II	NA	NA	Will business users support UAT , or is SI expected to manage end-to-end?	Currently handled by DOP Team. SI to manage end-to-end.

Response to the Pre-Bid Queries

15 75	II	NA	NA	How many non- production environments are currently available ? Eg) UAT /Dev/ Pre production/Reports/ MIS servers etc	UAT/SIT/Training/MIS.

Response to the Pre-Bid Queries

15 76	II	NA	NA	Are test environments always in sync with production?	No

Response to the Pre-Bid Queries

15 77	II	NA	NA	Are VAPT findings for Finacle applications expected to be closed by SI?	Yes.

Response to the Pre-Bid Queries

15 78	II	NA	NA	Will the incumbent SI be contractually obligated to provide KT?	Yes.

Response to the Pre-Bid Queries

15 79	II	NA	NA	Is reverse KT and shadow run mandatory for all modules?	Yes.

Response to the Pre-Bid Queries

15 80	II	NA	NA	Is a minimum exit support period defined beyond contract end?	As per RFP

Response to the Pre-Bid Queries

15 81	II	NA	NA	Please share tickte volumetric dump of the total number of L1, L2 and L3 tickets in the last 2 Quarters	Refer sheet "Additional details on applications"

Response to the Pre-Bid Queries

15 82	II	NA	NA	Please share the number of changes wrt the AMS scope (Finacle, IB, MB, KYC etc) per week/per month in the last 3 months.	Changes are raised on a need basis. Based on recent trends, the average volume is approximately 30 requests per month, covering minor/major enhancements, issue fixes, and reporting changes.

Response to the Pre-Bid Queries

15 83	II	NA	NA	Please share the number of incidents encountered by the bank in the last 3 Quarters	As per RFP

Response to the Pre-Bid Queries

15 84	II	NA	NA	Please share the details on the number of people doing L1, L2 and L3 tasks for the AMS support scope as per RFP	As per RFP

Response to the Pre-Bid Queries

15 85	II	5.2.5	-	For the new applications development of below solutions - could you confirm if there are any solutions currently used in landscape that could be continued or each of these will be a new solution to be introduced. - cKYC, AEPS, IMPS, vKYC, API Gateway, Middleware	These solutions are not implemented at the moment. Bidder to propose implementation strategy as part of the proposal.

Response to the Pre-Bid Queries

15 86	II	5.2.5.12	The Selected SI shall deliver a feature-parity revamp of Internet Banking that retains existing functionalities and provides a redesigned UI/UX with improved usability.	Kindly confirm if the base solution for this revamp will be Finacle Internet Banking solution which needs to be enhanced.	Bidder to propose

Response to the Pre-Bid Queries

15 87	NA		Facility	Please share the preferred new DC, NDR location, Will it be DC, NDR Mumbai and new DR in Mysore?	As per RFP

Response to the Pre-Bid Queries

15 88	NA		The SI shall ensure deployment of dedicated experienced manpower	Please confirm the No. of data centre non IT infrastructure resource (Manpower) required at each. Is 24x7 availability of resource required?	Bidder to propose

Response to the Pre-Bid Queries

15 89	NA		General	Please share the current automation and the use cases which are available today	Details will be shared with the selected bidder.

Response to the Pre-Bid Queries

15 90	NA	NA	General	Please share the list of AI use cases currently deployed.	Details will be shared with the selected bidder.

Response to the Pre-Bid Queries

15 91	NA		NA	Automation	What are the automation use cases in effect currently? What is the efficiency of the resolution of tickets?	Details will be shared with the selected bidder.

Response to the Pre-Bid Queries

15 92	NA	NA	General	What are tools deployed for a.) Server monitoring (windows, unix) b.) DB monitoring c.) Storage monitoring d.) Application monitoring e.) Network monitoring	No external tools are in use other than the current vendor developed tools/scripts by respective domain experts.

Response to the Pre-Bid Queries

15 93	NA	NA	General	Are there any real user monitoring or synthetic transactions in place for application monitoring? If yes, how many applications are been monitored? What are tools used for the same? If no, can it be proposed?	No tools. Bidder to propose.

Response to the Pre-Bid Queries

15 94	NA	NA	General	Is there an existing PowerBI license in place?	As per RFP

Response to the Pre-Bid Queries

15 95	NA	NA	General	Please share ticket dump for last 6 -12 months (#service requests # problems, # changes)/ Please bifurcate manual vs automated tickets	Refer sheet "Additional details on applications"

Response to the Pre-Bid Queries

15 96	NA	NA	General	Please let us know the Centralized CMDB tool deployed for tracking all DC elements(On-premise and Cloud) and end user asset information?	No tools for asset reporting.

Response to the Pre-Bid Queries

15 97	NA	NA	General	Do you have a barcode solution/process for asset tagging?	No.

Response to the Pre-Bid Queries

15 98	NA	NA	General	What is the accuracy level/maturity on software license report?	No tools to evaluate.

Response to the Pre-Bid Queries

15 99	NA		NA	General	what are the tools currently deployed for remote desktop management?	No specific tools.

Response to the Pre-Bid Queries

16 00	NA		NA	General	What are the tools deployed for patching and software distribution for	No Tools.

Response to the Pre-Bid Queries

16 01	NA	NA	General	Do you have batch jobs configured, if yes, which tool is used	No tools used for batch jobs.

Response to the Pre-Bid Queries

16 02	NA	NA	General	Please share the expected Y.O.Y growth of batch jobs	Bidder to propose as per the solution.

Response to the Pre-Bid Queries

16 03	NA		NA	General	Please share the breakup of hourly, daily, weekly and monthly batch job volumes	As per RFP

Response to the Pre-Bid Queries

16 04	NA	NA	General	Please share total volume of Batch jobs currently running	As per RFP

Response to the Pre-Bid Queries

16 05	II	5.2.2 Shifting of IT Infrastructure components from the existing DCF to the new DCFPage-69	The SI shall be responsible for executing the end-to-end lift-and-shift of IT infrastructure from the existing DC (Mumbai) DR (Mysuru) to the new co-hosting facility locations.	does POSB has any preferential city/Location for DC/NDC & DR sites ? Will they continue to be in Mumbai and Mysuru?	As per RFP

Response to the Pre-Bid Queries

16 06	II	5.2.2.12 Special Considerations Page-77	Rack space provisioning must accommodate both current and future expansion, ensuring contiguous allocation for additional racks.	Does Bidder have to consider all new Racks at the new DC and DR or existing Racks can be reused ? Is there any specific make of Racks which we need to consider ?	Racks for the new DC and DR under this RFP shall be newly provisioned by the bidder. Existing racks are not proposed to be reused. Racks must comply with the technical specifications and standards defined in the RFP.

Response to the Pre-Bid Queries

16 07	II	5.2.3.1 Underlying ICT Infrastructure Layer Page-78	POSB IT systems shall have a common infrastructure layer catering to the network, compute, storage, security, and operating system requirement built on a Software Defined Platform to be used by all applications.	Bidder Request to share current Logical and Physical Network architecture for DC and DR sites , This is required to understand the current landscape and planning for future site maintaing same zoning .	Confidential Information, to be shared with the Selected Bidder. Interested bidders may request for physical visits to the existing DC and DR upon request. Such requests should be submitted via email to pmu-fsdivision@indiapost.gov.in within three (3) days from the release of the corrigendum.

Response to the Pre-Bid Queries

16 08	II	5.2.3.1 Underlying ICT Infrastructure Layer Page-78	To address the infrastructure requirement of POSB IT systems, the infrastructure architecture would be based on service-oriented network architecture in which functionalities can be added to the infrastructure as and when required.	is POSB expecting dedicated Network Service Layer/Zone for Services like LB , FW, WAF etc ? Please elaborate further	As per RFP

Response to the Pre-Bid Queries

16 09	II	2.Bandwidth Connectivity:Page-210	Branch Connectivity	1) What is the SDWAN solution at Branch end - pls clarify the OEM ? 2) Request to share logical and Physical WAN architecture 3) Are any branches on Traditional WAN (non SDWAN). If yes, 4) how are they connected to DC/DR - eg MPLS,IPSEC etc	SDWAN is not in scope of the RFP. Details of the Networking solution are provide in the RFP. Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

16 10	II	5.2.2 Shifting of IT Infrastructure components from the existing DCF to the new DCF : RACI Point 6 Page-71	OEM engagement for transition support, shutdown, restart & beta testing	Is the OEM engagement mandatory? Also clarify which technologies/devices this is applicable for – whether Network, Server, Storage etc	As per RFP

Response to the Pre-Bid Queries

16 11	II	5.2.4.3 Integration Page-89	The SI is required to deploy engineers <u>from the OEM</u> for the installation and maintenance of the proposed hardware and software at DC, DR, and NDC	Pls amend this clause – implementation & maintenance can be done by the System Integrator Engineers with OEM support. OEM can do the Design and a Pilot implementation and SI can implement the balance subsequently	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

16 12	Annexure-L	Core-Router	Each Router should have minimum number of ports to accommodate the termination of MPLS links from all the locations and the DRC. There must be provision for at least 50% free ports for future expansion.	Please mention Minimum port required along with Type of Port (1G Copper/Fiber , 10G , 40G etc)	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 13	Annexure-L	Spine Switches	Min of 34 non-blocking interfaces populated with multimode 40/100G Transceivers from day 1. Switch should have console port for local management & out of band management interface for remote management.	Bidder request to change the compliance as " Min of ~~34~~ 32 non-blocking interfaces populated with multimode 40/100G Transceivers from day 1. Switch should have console port for local management & out of band management interface for remote management."	Refer #641

Response to the Pre-Bid Queries

16 14	Annexure-L	Spine Switches	Device should be based on simple and intelligent shared-memory buffered architecture that simplifies the system buffer management and queuing implementation. Both the SAN switch and the Spine/Leaf switches should be from the same OEM	Bidder request to change the clause as "Device should be based on simple and intelligent shared/ dedicated -memory buffered architecture that simplifies the system buffer management and queuing implementation. Both the SAN switch and the Spine/Leaf switches should be from the same OEM	Refer #642

Response to the Pre-Bid Queries

16 15	Annexure-L	Spine Switches	Switch should support minimum 10 Tbps of switching throughput. Switch should support a minimum of 12 TBps Bandwidth	the statements are contradictory , mentioning two different Value , Bidder request to rectify the same	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 16	Annexure-L	Spine Switches	The switch should have capability to support 400G without any additional software or module from day 1	Bidder Request to make changes to clause as "The switch should have capability to support ~~400G~~ 100G without any additional software or module from day 1	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 17	Annexure-L	Core-Router	Load balancing feature to be present in routers and must work mainly for internet terminated links. Internet and MPLS both will be terminated in router and the same must work seamlessly in different routing planes without affecting security and maintaining IT security compliance.	From Security perspective terminating both Internet & MPLS links on the same Router is not a recommended practice & separate Routers should be proposed. Request you to consider the same & amend this point	Refer #259

Response to the Pre-Bid Queries

16 18	Annexure-L	Core-Router	Load balancing feature to be present in routers and must work mainly for internet terminated links. Internet and MPLS both will be terminated in router and the same must work seamlessly in different routing planes without affecting security and maintaining IT security compliance.	we should also have separate dedicated Routers for DC to DR replication as well as DC to NDC connectivity. We request you to consider this & provide relevant specifications of these Routers	Refer #259

Response to the Pre-Bid Queries

16 19	Annexure-L	Core-Router ,WAN Routers	Generic	Pls elaborate on the functionality of Core Routers versus WAN Routers	As per RFP

Response to the Pre-Bid Queries

16 20	Generic		Generic	Wrt DC Software Defined Network, there is an SDN Controller responsible for managing the Switches. Request you to publish the specifications for the same	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 21	Generic		Generic	Request you to provide the existing WAN bandwidth details at DC & DR (Internet, MPLS & replication) . What is the YoY scalability anticipated because the bidder has to design for the highest throughput in its lifetime ?	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 22	Annexure-L	Software LB & Server LB		Pls elaborate on the functionality & Purpose of Software LB and Server LB	As per RFP

Response to the Pre-Bid Queries

16 23	Annexure-L & Annexure N	Software LB & Server LB		There is Specification for SLB and waf being asked under Annexure I & N , Please suggest which specification to be consider for SLB	As per RFP

Response to the Pre-Bid Queries

16 24	ii	5.3 Page 121	Quality Control & Testing	Do you have test assets (automation frameworks/ scripts/ utilities) which are reusable?	Bidder to propose

Response to the Pre-Bid Queries

16 25	ii	5.3 Page 121	Quality Control & Testing	Do we have test case suite for Performance testing ? How much is automated ? Is there any baseline metrics captured?	Bidder to propose

Response to the Pre-Bid Queries

16 26	ii	5.3 Page 121	Quality Control & Testing	What is the expected level of automation coverage (e.g., % of regression suite automated)?	Bidder to propose

Response to the Pre-Bid Queries

16 27	ii	5.3 Page 121	Quality Control & Testing	Are there any third-party systems or interfaces for which test stubs or simulators will be provided, or is the SI expected to develop these?	SI to develop these.

Response to the Pre-Bid Queries

16 28	ii	5.3 Page 121	Quality Control & Testing	1. Is there a preferred defect management tool or process?	Bidder to propose

Response to the Pre-Bid Queries

16 29	ii	5.3 Page 121	Quality Control & Testing	Are there any existing test strategy documents or standards that the SI must align with, or is the SI expected to define the complete test strategy?	Bidder to propose

Response to the Pre-Bid Queries

16 30	ii	5.3 Page 121	Quality Control & Testing	Do you allow use of open-source tools for test automation ?	Bidder to propose

Response to the Pre-Bid Queries

16 31	Annexure N	External NGFW	Firewall	Could you please re confirm the Minimum TCP Connections (500 Million)	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 32	Annexure N	Internal NGFW	Internal NGFW	Could you please share the Sizing for Internal Firewall	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 33	Annexure N	External NGFW	Firewall	Could you please re confirm total Number of VPN Users and Concurrent users	Bidders may refer to Corrigendum Annexure N for updated details of the requirements.

Response to the Pre-Bid Queries

16 34	II	115/5.2.5.9	EFRM	Do you have a robust fraud risk management policy & guidelines, explicitly depicting the fraud detection methodology, approach, threshold, rules, risk scoring approach etc?	Bidder to propose

Response to the Pre-Bid Queries

16 35	II	Page114 Section 5.2.5.9	EFRM	Which solution is currently in place for Fraud Risk Detection and Management?	None. Only AML is implemented.

Response to the Pre-Bid Queries

16 36	II	Page114 Section 5.2.5.9	EFRM	Is there any preference for a specific EFRM solution or platform?	Bidder to propose

Response to the Pre-Bid Queries

16 37	II	Page114 Section 5.2.5.9	EFRM	Please share details on type of channels, volume of transactions, no. of integrations, user volume, no. of reports, etc expected to be managed through EFRM solution	Bidder to analyze as per given information

Response to the Pre-Bid Queries

16 38	II	115/5.2.5.9	EFRM - Fraud Detection & Analytics	What are the existing NPCI fraud tools in place?	As per RFP

Response to the Pre-Bid Queries

16 39	II	115/5.2.5.9	EFRM - Fraud Detection & Analytics	How many fraud detection rules are expected to be configured & customized, based on the existing fraud mitigation guidelines?	Bidder to propose

Response to the Pre-Bid Queries

16 40	II	115/5.2.5.9	EFRM - Reporting & BI	How many reports pertaining to fraud detection analysis to be generated, based on the current fraud risk management framework?	Approx 50 reports

Response to the Pre-Bid Queries

16 41	II	115/5.2.5.9	EFRM - Integration & Data Management	How many upstream data sources are expected to be integrated for any fraud analytics or profiling work?	The bidder is expected to integrate all relevant upstream systems required for fraud monitoring and profiling, including but not limited to Core Banking, delivery channels, payment systems, customer onboarding/KYC systems, and third-party interfaces. The number of data sources may evolve over the project duration, and the solution shall support onboarding of additional sources.

Response to the Pre-Bid Queries

16 42	II	115/5.2.5.9	EFRM - Integration & Data Management	How many external data bases exist to integrate facilitating to augment the data for quick better decisioning?	Refer AML section for details. Indicative list of integrations has been provided in the RFP.

Response to the Pre-Bid Queries

16 43	II	115/5.2.5.9	EFRM - Integration & Data Management	Are there any third-party intelligence systems exists currently to integrate with fraud detection systems?	As per RFP

Response to the Pre-Bid Queries

16 44	II	115/5.2.5.9	EFRM - Rule Management & Scenario Tuning	How many fraud models exists currently & what kind of analytics tools used in creating the models?	Bidder to propose

Response to the Pre-Bid Queries

16 45	II	115/5.2.5.9	EFRM - Investigations & Case Management	Do you prefer a standalone case management tool to analyse the fraud alerts, or can you continue to use the case management which already exists at your end and consumed for AML?	Bidder to propose

Response to the Pre-Bid Queries

16 46	II	115/5.2.5.9	EFRM - Reporting & BI	Do you prefer a standalone business intelligence tool or convenient to choose the embedded reporting tool within a third-party fraud management tool?	Bidder to propose

Response to the Pre-Bid Queries

16 47	II	115/5.2.5.9	EFRM - Implementation, Training & Support	Do you have an approximate plan to complete the entire EFRM system implementation?, which includes requirements gathering, system design, solution configuration, data migration, system integration, end-to-end testing, along with reporting & dashboards?	As per RFP

Response to the Pre-Bid Queries

16 48	II	115/5.2.5.9	EFRM - Implementation, Training & Support	How many months of support & maintenance is expected and do you require all the levels of support like L1, L2, L3?	Bidder to propose. Solution must meet RFP requirements.

Response to the Pre-Bid Queries

16 49	II	115/5.2.5.9	EFRM - Implementation, Training & Support	How many cycles of UAT is expected? Generally we offer 2 round of UAT which includes fixes and retesting;	Bidder to propose as per best practices, DoP signoff shall be necessary to complete the UAT requirements.

Response to the Pre-Bid Queries

16 50	II	115/5.2.5.9	EFRM - Implementation, Training & Support	PI share more light on the training sessions expected to be conducted by the SI's? How many weeks, and whether the functional, administration and technical trainings?	Training shall cover all new developments and implementations undertaken as part of the scope of work under this RFP, including any configurations, integrations, and customizations carried out during the project duration. Depending upon the functionality, minimum 1 to 4 days of training to be provisioned by the SI. The training plan to be submitted accordingly. Trainings can be conducted in-person/virtually based on criticality of functionality as mutually agreed between DoP and the SI.

Response to the Pre-Bid Queries

16 51	II	115/5.2.5.9	EFRM - Integration & Data Management	Are we expecting to integrate the Risk Based Authentication alerts to the fraud case management tool?	Bidder to propose

Response to the Pre-Bid Queries

16 52	II	21/5.1.1	AML Solution - Software License	From the track plan, the SAS AML solution will be implemented from April to Aug 2026. What kind of roles & responsibilities the platform professional services team will own?	SAS AML product license to be extended for one year by DoP. Selected Bidder to ensure continuity of AML functionality as per FRS till the end of contract through its proposed approach and solution.

Response to the Pre-Bid Queries

16 53	II	21/5.1.1	AML Solution -Manpower	From the existing track plan, SI will overlap with the AML SAS provider for about 5 months and What kind of specific help and support is expected from the SI in this development & implementation?	SAS AML product license to be extended for one year by DoP. Selected Bidder to ensure continuity of AML functionality as per FRS till the end of contract through its proposed approach and solution.

Response to the Pre-Bid Queries

16 54	II	246/Annexure E	AML Solution - Volume of transactions	What would be approximate volume of transactions - Inward remittances - IMTS, MTSS, Money changing services, on a daily, monthly & annual basis?	Daily Trans : 1. CASH - 2698963 2. ATM -25977 3. NEFT - 22431 4. RTGS - 3041 5. EBK - 3486 6. MBK - 939 Monthly : 1. CASH - 56415213 2. ATM - 962869 3. NEFT - 607554 4. RTGS - 76802 5. EBK - 103660 6. MBK - 26181 Above are the existing values.

Response to the Pre-Bid Queries

16 55	II	246/Annexure E	AML Solution -RFI's	Are you expecting the SI to reactivate the unused RFI (81 count)?	Current solution O&M to be done as is. Bidder to propose for future implementation.

Response to the Pre-Bid Queries

16 56	II	246/Annexure E	AML Solution - Alerts	What would be volume of alerts generating out of 24 RFI's?	1. Daily Alerts - 500-700 2. Weekly Alerts - 4000-6000 3. Monthly Alerts -80000-90000

Response to the Pre-Bid Queries

16 57	II	246/Annexure E	AML - current tool	It is written that the current solution is providing 26 different reports to monitor AML breaches? What is the tool used in generating these 26 reports?	Report - MIS -REPORT Tools - SAS Enterprise Guide

Response to the Pre-Bid Queries

16 58	II	247/Annexure E	AML-Reports	It is expected from SI that we need to generate MIS & nearly 50 reports? Do we need to create the report format & wireframe to configure in the system?	Bidder to propose

Response to the Pre-Bid Queries

16 59	II	248/Annexure E	AML - Solution	How many months of support & maintenance is expected and do you require all the levels of support like L1, L2, L3?	Refer #1648

Response to the Pre-Bid Queries

16 60	II	Page245 Annexure E	AML Solution	Does POSB intend to continue with SAS AML solution or do we need to provide alternative potential AML solution options in our response?	Refer #1652

Response to the Pre-Bid Queries

16 61	II	Page245 Annexure E	AML Solution	Is SAS AML being used for KYC, Screening and Transaction Monitoring or are there any other supporting solutions involved?	As per RFP

Response to the Pre-Bid Queries

16 62	II	Page245 Annexure E	AML Solution	Can you please share a view or details on the existing logical framework for AML?	As per RFP

Response to the Pre-Bid Queries

16 63	II	Page106 Section 5.2.5.1	cKYC	How is POSB currently performing cKYC? Any third party solutions are involved?	cKYC is not implemented.

Response to the Pre-Bid Queries

16 64	II	Page106 Section 5.2.5.11	vKYC	How is POSB currently performing vKYC? Any third party solutions are involved?	vKYC is not implemented.

Response to the Pre-Bid Queries

16 65	II	Page117 5.2.5.10	Middleware	Please share the current integration architecture diagram and interface inventory for all systems.	As per RFP

Response to the Pre-Bid Queries

16 66	II	Page117 5.2.5.10	Middleware	Please share details of the ESB/middleware and message brokers currently in use (vendor/version). Also, please confirm whether IBM MQ is part of your existing integration landscape.	There is no Middleware implemented for POSB.

Response to the Pre-Bid Queries

16 67	II	Page117 5.2.5.10	Middleware	How do you integrate with Finacle today (Finacle Integrator APIs, OFS, REST, MQ/JMS etc.)?	Finacle integrator (XML only) or Via C24 (ISO 8583)

Response to the Pre-Bid Queries

16 68	II	Page117 5.2.5.10	Middleware	Please share the list of new integration interfaces to be developed under the new scope.	As per RFP

Response to the Pre-Bid Queries

16 69	II	Page117 5.2.5.10	Middleware	How many existing integration interfaces must be migrated to the new middleware platform? Please provide the probable interface list (REST/SOAP/MQ/SFTP/File).	The details of existing interfaces will be shared with the selected bidder during the transition phase. Bidders are expected to factor migration of all in-scope integrations to the proposed middleware platform, supporting standard integration mechanisms, file-based interfaces, and other prevalent protocols, as applicable.

Response to the Pre-Bid Queries

16 70	II	Page110 5.2.5.6	Middleware	How many backend services/APIs must be exposed as API Proxies or API Products in the APIM layer?	Bidder to propose as per RFP requirements

Response to the Pre-Bid Queries

16 71	II	Page110 5.2.5.6	Middleware	What is the expected peak TPS and average daily volumes for both new and migrated APIs?	Refer#6

Response to the Pre-Bid Queries

16 72	II	Page110 5.2.5.6	Middleware	For the new API Management platform, please confirm required capabilities such as API publishing, Developer portal, Monetization (if applicable) etc.	Bidder to propose as per RFP requirements

Response to the Pre-Bid Queries

16 73	II	Page117 5.2.5.10	Middleware	Will the current middleware layer continue to run during the migration? If yes, please confirm the preferred cutover strategy (phased, big bang, dual run) and any constraints.	There is no Middleware implemented for POSB currently. Bidder to propose cutover strategy.

Response to the Pre-Bid Queries

16 74	II	Page265 Annexure M	Middleware	As Kafka/event-driven integration is referenced in the scope, kindly confirm: (a) Is Kafka already deployed in the current landscape? (b) If yes, please share topology, versions, event volumes and DR model. (c) If no, do you expect the new middleware platform to provide Kafka based event streaming capabilities?	Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

16 75	II	5.1.1	Takeover & Transition	As per the RFP various vendor contracts are set to expire at different times, Please confirm mentioned tracks need to be consider in our scope even the expiry date of the existing bender still not reached?	As per RFP

Response to the Pre-Bid Queries

16 76	II	5.1.3	Upgrade of Finacle CBS and Alert Solution	We assume that infrastructure for finacle new version is available with POSB to accommodate the requirement . Please confirm	Bidder to analyze as per given information

Response to the Pre-Bid Queries

16 77	II	5.1.3	Upgrade of Finacle CBS and Alert Solution	Please share the current environment wise infra sizing for the finacle & associated application deployed	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

16 78	II	5.1.3 (Pg 39)	extraction and provisioning of data from POSB IT systems and POSB Data Lake	Please share the POSB Data Lake details and sizing of the POSB data to be extracted and transfer from POSB IT system	Data lake house/warehouse setup is not in scope. Bidder shall integrate with DoP implemented central data lakehouse.

Response to the Pre-Bid Queries

16 79	II	5.1.5.1(Pg43)	A. Core Responsibilities	Please share the patching tool currently deployed	Bugzilla

Response to the Pre-Bid Queries

16 80	II	Pg 212-	Annexure A – Existing Infrastructure (As-Is Compute, Storage & Backup Solution)	Please share the instance wise count of each flavour (Physical / virtual), for Windows, Linux, Unix etc.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

16 81	BOQ_93745 7		Bill of Quantity	As per the list shared in RFP most of the infra (Storages & Servers) are commonly utilised by POSB , PLI & ECMS- Please suggest how to take this forward separation between the entities for infra prospective.	Selected bidder shall be responsible for the O&M of shared infra till the go-live of new DCF. Bidder to assess and propose HW components for separation.

Response to the Pre-Bid Queries

16 82	II	Pg 226	Annexure B – Common Infra and Security solutions maintained by HPE	Please share the details of Hardware configuration, serial number, software details etc maintained by HPE if SI has to takeover this.	As per RFP

Response to the Pre-Bid Queries

16 83	II	5.2.1.1	Facility Requirements	Please share the preferred DR location we assumed the DC & NDC will be in Mumbai.	Bidder to propose. DR should be in different seismic zone.

Response to the Pre-Bid Queries

16 84	II	5.2.1.1.13	The SI shall ensure deployment of dedicated experienced manpower	Please confirm the No. of data centre non IT infrastructure resource (Manpower) required at each facility. Is 24x7 availability of resource required?	Bidder to propose

Response to the Pre-Bid Queries

16 85	II	5.2.2	Shifting of IT Infrastructure components from the existing DCF to the new DCF	We understand from RFP that the installation & Upgrade of the solution happened at existing DC. Post implementation the migration to new DC will be initiated. Please confirm is our understanding correct?	Bidder to propose

Response to the Pre-Bid Queries

16 86	II	5.2.2	Shifting of IT Infrastructure components from the existing DCF to the new DCF	Please share the list of the infrastructure to be shifted before or in parallel to upgradation of existing solution at current Data Center	Bidder to analyze

Response to the Pre-Bid Queries

16 87	II	General	Backup and associated infra	Please suggest the proposition for new Backup solution & associated backup devices or existing to be averaged.	Bidder to propose

Response to the Pre-Bid Queries

16 88	II	Pg 83 point#19	The SI is required to ensure that each server, as mentioned earlier, remains physically independent, unless specified otherwise. For this purpose, any type of partitioning within the same machine will not qualify as a separate server.	Please elaborate, as per our understanding this statement shows there will be only physical instances no any virtual instance to be factored - please suggest	Virtualization may be used as part of the solution architecture, provided that performance, availability, and sizing requirements are fully met and each required server instance is provisioned with dedicated resources.

Response to the Pre-Bid Queries

16 89	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 2	2.Router should have a physical separation between control and data planes processor. Router should support inline hardware accelerated encryption for high-throughput IPSec	As per the clause 16 in specification of core Router external appliance is allowed for firewall Functionality , Request to kindly allow to have IPSEC functionality offloaded to external device . This will remove ambiguity in design and will also insure high scale along with maximum participation while insuring maximum return on investment with next generation architecture	Refer #258

Response to the Pre-Bid Queries

16 90	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 3	3. Load balancing feature to be present in routers and must work mainly for internet terminated links. Internet and MPLS both will be terminated in router and the same must work seamlessly in different routing planes without affecting security and maintaining IT security compliance.	we understand that Load balancing / Load Sharing on the internet side can be achieved by BGP learned routes or through Policy based Routing , Kindly confirm	Refer #259

Response to the Pre-Bid Queries

16 91	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 9	9. The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should be able to create GRE tunnel.	L2TP is a legacy unencrypted protocol , IPSEC is already asked in the tender which is more secure and support by all leading OEM , Request to relax the clause and allow IPSEC to be used in place of L2TP .Also GRE encapsulates the packet ,no encryption is used in GRE , Request to kindly change the clause by removing GRE encryption and on demand GRE for solution clarity or allow IPSEC / GDOI while the same can be offloaded to external firewall as requested . Requested clause :- The router must support IKEv1, L2TP/IPSEC , IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption/IPSEC	Refer #260

Response to the Pre-Bid Queries

16 92	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 10	10.The router should support 19 Gbps of IPSEC Bandwidth	Request to kindly confirm for offloading the IPSEC to external firewall for leading OEM to participate . The same is also requested in query 1 of core Router	Refer #261

Response to the Pre-Bid Queries

16 93	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 11	11.Implementation Agency should ensure necessary encryption 8.5 Gbps throughput (IMIX, EMIX) supported by proposed device at site from day 1: (IPSEC case of SD-WAN)	Request to kindly remove (IPSEC Case of SDWAN) as the same is creating ambiguity . IPSEC will be used on WAN side for traffic encryption as per the Govt Guide lines and frame work for Financial organization . Request change for leading OEM to participate .	Refer #262

Response to the Pre-Bid Queries

16 94	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 12	12.Router should be scalable to support up to 4000 tunnels (non-SDWAN) / 8000 SD_WAN tunnel (SD- WAN)	Different OEM have different architecture for providing the traffic encryption using IPSEC .SDWAN for all OEM is proprietary and can not integrate with any other OEM , Request to kindly remove SDWAN or clarify that either of 4K (no-SDWAN) / 8K should be supported .	Refer #263

Response to the Pre-Bid Queries

16 95	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 17	17.Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.	Traffic optimization was required on low latency link such as E1 or low speed TDM link which are not used in modern days network , The solution provided will have ethernet connectivity ranging for 1Gps to 100Gbps interface. Also Traffic optimization works on P2P links i.e both side should have functionality . The same is not possible in large and heterogenous network . Request to kindly remove the clause for leading OEM to participate .	Refer #264

Response to the Pre-Bid Queries

16 96	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 21	21. Router should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	Refer #265

Response to the Pre-Bid Queries

16 97	Volume II ,	Annexure L , Core-Router , Manageability -Clause 25	25. Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	Refer #266

Response to the Pre-Bid Queries

16 98	Volume II ,	Annexure L , Core-Router , Manageability -Clause 29	29. Router should be IPv6 Certified/IPv6 logo ready	All reputed OEM support IPV6 functionality from day 1 , we are providing latest hardware / solution which supports all IPV6 features from day1 . Request to amend the clause for leading OEM to participate . Requested Clause :- Router should be IPv6 Certified/IPv6 logo ready / IPV6 Ready	Refer #267

Response to the Pre-Bid Queries

16 99	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 8	8. Minimum WAN throughput: 20 Gbps (scalable to 40 Gbps).	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the WAN throughput asked is 40Gbps which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Minimum WAN throughput: 320 Gbps (scalable to 340 Gbps).	Refer #268

Response to the Pre-Bid Queries

17 00	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 10	10.Forwarding performance: > 30 Mpps.	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the MPPS asked is >30MPPS which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Forwarding performance: > 476Mpps.	Refer #269

Response to the Pre-Bid Queries

17 01	Volume II ,	Annexure L , WAN Router , Performance Requirement -Claus23	23.Stateful firewall capabilities.	Request to kindly change the clause for leading OEM to Participate . Requested clause:- .Stateful firewall capabilities/ ACL/ Firewall filter	Refer #270

Response to the Pre-Bid Queries

17 02	Volume II ,	Annexure L , WAN Router , High Availability -Clause 30,31	30.Non-stop Routing (NSR), Non-stop Forwarding (NSF). 31. Stateful switchover (SSO)	For asked functionality to work redundant CPU / Routing engine is required . Kindly clarify if redundant Routing engine is required from day 1 or only support is asked . Kindly clarify for solution clarity .	Refer #271

Response to the Pre-Bid Queries

17 03	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 9	9.The switch should support 30k multicast routes	30K Multicast is on very high side and not required on spine as they act as transit for traffic , request to reduce the route scale for maximum participation for leading OEM to participate . Requested clause :- .The switch should support 8k multicast routes	Refer #272

Response to the Pre-Bid Queries

17 04	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 25	25.Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP)	MSDP is used on WAN side and is not widely deployed in Spine devices in data center, instead PIM SSM and PIM SM are used request to relax the clause for leading OE tom participate . Requested clause :- Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) / MLD (Multicast Listener Discovery)	Refer #273

Response to the Pre-Bid Queries

17 05	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	17.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Refer #275

Response to the Pre-Bid Queries

17 06	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	23.The Switch should support intelligent buffer management with a minimum buffer of 36 MB.	Request to kindly change the packet buffer to 32Mb for leading OEM to participate Requested clause :- 23.The Switch should support intelligent buffer management with a minimum buffer of 32 MB.	Refer #276

Response to the Pre-Bid Queries

17 07	Volume II ,	Annexure L , LEAF SWITCH ,Network Virtualization Features -Clause 26	26.Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat OpenShift and manage virtualize networking from the single pane of glass	Leaf switch connect to any virtualization platform using VLAN . Switch do not connect to any virtualization Manager . The fabric manager / SDN controller defines the EVPN VXLAN fabric on spine and leaf devices , which can further connect to Orchestrator for single pane of glass management. The clause is restricting leading OEM request to change . Requested clause :- Switch must provide the capability to be integrated with different Hypervisor viz. Vmware, Microsoft Hyper-V , Kubernetes, Redhat OpenShift using standard based VLAN	Refer #277

Response to the Pre-Bid Queries

17 08	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 29	29.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Refer #278

Response to the Pre-Bid Queries

17 09	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	47.Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro- segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification. The solution must also provide micro segmentation capability on application end host at remote location sites in offline mode (once policy is applied from the DC to workloads on remote sites, in case the sites are dis-connected, the enforcement policy is retained). Mentioned feature/capability should be achieved using same OEM products for a seamless integration, without using any external/3rd party solution.	The micro segmentation in data center in virtualized environment is managed by Virtual machine manager and for Switching environment using Fabric manager . They both integrate using Orchestration layer for single plane of management and integration . The functionality asked is achieved through different architecture from different OEM. The clause in current format is restricting leading OEM's .Request to change the clause for leading OEM to participate . Also request to remove virtualization microsegment into the virtual environment security requirement . This will ensure that level playing field is given to all OEM in data center infra domain. Requested clause :- .Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation basis on connected VLAN / Ports .	Refer #279

Response to the Pre-Bid Queries

17 10	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	49.Switch platform should support encryption of traffic i.e. MAC Sec Encryption (802.1AE) in hardware	Spine switch is not asked with MACSEC , this will create confusion in design . Request either remove MACSEC for leaf switch or add the same in SPINE switch for solution clarity .	Refer #280

Response to the Pre-Bid Queries

17 11	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable SDN-based virtualised networking and distributed firewalling.	Change Request : Request you to Change asked Clause as "Enable SDN-based virtualised networking and distributed firewalling using 3rd Part Tools & Automation solution Justification : This is 3rd Party solution Feature , which can be Integrated with Virtualization Platform	Refer #290

Response to the Pre-Bid Queries

17 12	Volume of the RFP (II)	IT Infrastructure Setup and Transition	Set up the new Data Centre (DC), Disaster Recovery (DR) and Near-site Data Centre (NDC) infrastructure — not limited to servers, storage, security and network	Kindly explain what all expected by "setup" here other than Server, Storage, Security & Network implementation	End-to end provisioning, installation, configuration, integration, testing, commissioning, and operationalization of the complete DC/DR/NDC environment including servers, storage, security, network components, associated virtualization platforms, system software, monitoring and management tools, backup and DR mechanisms, rack and cabling, power and connectivity integration, documentation, and ongoing operations and maintenance.

Response to the Pre-Bid Queries

17 13	Volume of the RFP (II)	IT Infrastructure Setup and Transition	Execute lift-and-shift migration of infrastructure from existing DCFs to the new facilities with minimal disruption. Perform comprehensive infrastructure and application-level testing post-migration.	Kindly provide the source DC details and high level HW inventory in the source DC to be lift & shifted	Refer Corrigendum for details of existing inventory. Bidder to analyze and propose HW for Lift and Shift.

Response to the Pre-Bid Queries

17 14	Volume of the RFP (II)	5.1 Track 1: Takeover and Transition	Transition	Is the SI expected to do transition and service take over from each vendor as per the calendar shown ?	Bidder to propose as per RFP requirements

Response to the Pre-Bid Queries

17 15	Volume of the RFP (II)	5.1.5.2 Scope of Work for Operations and Maintenance	Patch management, OS tuning, upgrades, and support.	Please provide the details of patching solutions / tools currently available which can be leveraged	Bugzilla

Response to the Pre-Bid Queries

17 16	Volume of the RFP (II)	5.2.1.1 Facility Requirements, Page 52	The DC should have a Near-site Data Centre (NDC) for storage-to-storage synchronous data replication, connected over Dark Fibres with redundancy.	Dark Fiber connectivity is a challenge now a days. Can we propose metro ethernet ?	As per RFP

Response to the Pre-Bid Queries

17 17	Volume of the RFP (II)	5.2.1.1 Facility Requirements, Page 52	The proposed buildings for DC shall either be owned by the SI or taken on lease, with a minimum unexpired lease period of 10 years as on the RFP submission due date	As the contract is only for 5+1+1 years, 10 years lease with DC provider may not be feasible. Kindly amend this with POSB's contract period with SI and a buffer of 6 months for potential DC migration (if required)	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

17 18	Volume of the RFP (II)	5.2.1.2.8 DR Drills ; Page 68	DR drills	Kindly provide information on DR orchestration, automation tools in place which can be leveraged	Bidder to propose

Response to the Pre-Bid Queries

17 19	Volume of the RFP (II)	5.2.4 Detailed Scope of Work , Point 24, page 84	The SI is required to furnish a Backup Software Solution, supporting Full and Incremental, online, and offline backups, capable of performing backups at DC, DR and NDC locations.	Please provide details of current backup solution. Can SI leverage the backup license or should SI factor additional licenses for the backup software?	As per RFP

Response to the Pre-Bid Queries

17 20	Volume of the RFP (II)	5.2.4.1 Propose and Provision, Point 5, page 86	The SI is required to deliver enterprise-class storage solutions at the DC, DR and NDC sites. The enterprise-class storage proposed by the SI must be compatible with the proposed NDC storage, facilitating synchronous replication with zero data loss.	Pls provide detail of current storage raw & usable capacity in TB. Also please share the details of Tape Library being used.	As per RFP

Response to the Pre-Bid Queries

17 21	Volume of the RFP (II)	5.2.4.1 Propose and Provision, Point 9, page 90	the bidder must uphold the practice of maintaining data backups on external backup tapes, stored securely in a location agreed upon with POSB team.	SI assumes that POSB will provide necessary tape media and external tape vault arrangements. The SI will co-coordinate with external vendor. Please confirm	As per RFP

Response to the Pre-Bid Queries

17 22	Volume II ,	5.2.1.1.9 Structured Cabling and Networking	General	1.Is there any preferred make for Copper and Fiber cabling needs to consider ? 2. Fiber cabling and associated components should be OM3 or OM4?	As per RFP

Response to the Pre-Bid Queries

17 23	Volume of the RFP (II)	5.2.1.1.1 (Pt 2–4)	DC/DR/NDC must be Tier-III certified.	Should Tier-III certificate be submitted with bid or post-award? Justification: For compliance confirmation.	As per RFP

Response to the Pre-Bid Queries

17 24	Volume of the RFP (II)	5.2.4.6	NDC infra scope.	Should NDC include compute infra or only storage?	As per RFP

Response to the Pre-Bid Queries

17 25	Volume of the RFP (II)	Annexure L (Racks)	New racks required.	Is SI required to replace legacy racks being shifted, or only provide new racks?	As per RFP

Response to the Pre-Bid Queries

17 26	Volume of the RFP (II)	Annexure L (RISC)	High-end RISC requirement.	Which workloads must run on RISC vs x86?	Bidder to propose based on given information.

Response to the Pre-Bid Queries

17 27	Volume of the RFP (II)	Annexure L (Storage)	<1 ms latency required.	Will OEM benchmarks be accepted?	Clause is omitted. Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

17 28	Volume of the RFP (II)	Annexure L (Replication)	3-way replication mandated.	Confirm DC↔NDC synchronous & NDC↔DR async?	As per RFP. Pg 102

Response to the Pre-Bid Queries

17 29	Volume of the RFP (II)	Annexure L	70% utilization limit.	Please provide the historic logs	As per RFP

Response to the Pre-Bid Queries

17 30	Volume of the RFP (II)	Annexure L & 5.2.4.4	Backup retention.	Specify retention periods.	Refer #885

Response to the Pre-Bid Queries

17 31	Volume of the RFP (II)	5.2.3.3	Monitoring tools.	Unified suite or multiple tools?	Bidder to propose

Response to the Pre-Bid Queries

17 32		Annexure J EFRM Requirements SNo.10	Support IPV6 addressing and broad device/browser compatibility	Please elaborate and clarify the requirement as the solution nature is more of internal application and not over wider network	Refer #791

Response to the Pre-Bid Queries

17 33		Annexure J EFRM Requirements SNo.28	NLG capabilities to auto-generate insights	Please clarify on the expected NLG capabilities	As per RFP

Response to the Pre-Bid Queries

17 34		Annexure J EFRM Requirements SNo.47	Support for embedding web content and interactive visualizations (D3.js, Google Charts)	Please clarify the requirement in the context of google charts and D3.js. Are these charts indicative in nature?	Refer #792

Response to the Pre-Bid Queries

17 35		Annexure J EFRM Requirements SNo.83	Continuous enrichment with new data sources and third-party intelligence feeds	Please clarify if subscription to third party intelligence feeds will be provided by POSB	The selected bidder shall provision and manage any third-party intelligence feeds/subscriptions required for the proposed solution as part of its scope. DoP shall provide access to internal data sources and facilitate integration, wherever applicable

Response to the Pre-Bid Queries

17 36	II	EFRM 5.2.5.9	Environments	How many environments need to be factored for EFRM solution?	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

17 37	II	Annexure O Key Statistics EFRM	User Metrics	Request to provide following details with respect to EFRM :- 1. Total number of EFRMS users (analyst who will work on alerts) 2. Number of Fraud rules	Refer #48

Response to the Pre-Bid Queries

17 38	II	AML Solution Annexure E	Environments	How many environments need to be factored for AML solution?	As per RFP

Response to the Pre-Bid Queries

17 39	II	Annexure O Key Statistics AML	User Metrics	Request to provide following details with respect to AML :- 1. Total number of AML users (analyst who will work on alerts) 2. Total number of AML users (including branch users if alerts are assigned for EDD) 3. Number of AML rules	Bidder to propose based on given information.

Response to the Pre-Bid Queries

17 40	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-2	Storage solution should provide the native capability to replicate data of existing storage between DC, DR and NDC without using any additional Hardware and software.	Clarification Request : This is a restrictive clause. Request POSB to remove this clause for wider participation. Justification: In case a Native replication with existing storage is required then only an existing storage OEM can qualify which eliminates all other OEM participation. Hence request POSB to remove this clause	Refer #85

Response to the Pre-Bid Queries

17 41	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-3	SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage without using external/3rd party hardware or Software.	Clarification Request : SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage with/without using external/3rd party hardware or Software. Justification: This is a restrictive clause. Request POSB to modify this clause wider participation. Hence request to modify this clause	Refer #86

Response to the Pre-Bid Queries

17 42	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-8	Storage solution should support all Leading enterprise servers and Operating Systems: - CISC-based Servers running Windows, Linux, HP Enterprise Servers running HP/UX, IBM Enterprise Servers running AIX, SUN Enterprise Servers running Solaris, IBM Linux on the POWER platform. It should also support VMWare APIs - VAAI, VASA and RESTful API.	Modification Request :Storage solution should support all Leading enterprise servers and Operating Systems: - CISC-based Servers running Windows, Linux, HP Enterprise Servers running HP/UX, IBM Enterprise Servers running AIX, SUN Enterprise Servers running Solaris. It should also support VMWare APIs - VAAI, VASA and RESTful API. Justification: Since most of the application are going to be on x86 CISC based platform as asked in the RFP which is going to be virtualised with industry standard hypervisor and container platform/operating system, Sun Ent server running solaris, IBM linux on power platform is a niche OS which is not widely deployed, hence it should be modified.	Refer #236

Response to the Pre-Bid Queries

17 43	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-9	The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture with cache across configured controllers.	Clarification: We understand active active multi controller means all luns should be accesible to all the controllers in case of controller failure. please confirm if our understanding is correct.	Refer #237

Response to the Pre-Bid Queries

17 44	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-12	The proposed storage should have No Single Point of Failure (NSPOF) and, automatic failover architecture. All components must be redundant & hot swappable.	Clarification:We understand that POSB is asking for storage array with No Single Point failure shall include all components in controllers power supplies , IO cards , boot drives etc. please confirm if our understanding is correct.	Refer #238

Response to the Pre-Bid Queries

17 45	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-13	The Storage system must provide cache protection in case of power failure through de-staging to nonvolatile media or a 72-hour battery backup.	Modification Request :The Storage system must provide protection of data written in the cache/Memory in the event of complete power failure through de- staging of cache to non- volatile media or battery backup for at least 72 hours. Justification: Every OEM has different architecture with respect to system cache hence request you to modify this clause.	Refer #239

Response to the Pre-Bid Queries

17 46	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-17	Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes.	Modification Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes or as per OEM guidelines to deliver the performanc e & capacity . Justification: To deliver the performance and capacity, OEM applies their own best practice to configure the storage with the best possible configuration of drives. Hence request to modify this clause.	Refer #91

Response to the Pre-Bid Queries

17 47	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-32	The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 256GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall dynamically support read and write i/o	Modification Request :The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 2 controllers with cache size 256GB at NDC (scalable up to 1TB), protected by vault /battery/destaging. Justification: As POSB has asked for 4 controllers at DC and DR, two controllers are sufficient for NDR site. cache shall be protectected as per OEM best practice architecture. Request POSB to modify this clause.	Refer #241

Response to the Pre-Bid Queries

17 48	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-44	Must support compression supported for replicated traffic (FC/Ethernet) or as per OEM recommendation, redundant FCIP if required.	Modification: This clause provided undue advantage to an OEM offerings hence, request you to delete this clause for wider participation. In case FCIP routers are required , its shall be asked from all the OEM's. Justification: In a critical banking environment, FCIP routers are must from best practice point of view. Hence request POSB to please make FCIP as a mandatory ask from all the OEM.	Refer #242

Response to the Pre-Bid Queries

17 49	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-54	Must support advanced management: end-to-end mapping, monitoring, capacity planning, alerts, reports.	Modification: Must support advanced management: monitoring, , alerts, reports. Justification : This applicable(end-to-end mapping, capacity planning,) to a public cloud offering hence remove this clause.	Refer #243

Response to the Pre-Bid Queries

17 50	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-67	Must support consistency groups for multiple volumes across arrays with DB- consistent copies.	Modification: Must support consistency groups for multiple volumes across arrays with Block level/DB consistent copies. Justification: DB consistant copies are a feature of Data base only hence request to modify this clause.	Refer #244

Response to the Pre-Bid Queries

17 51	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-71	Must support high-availability 3-way / 4-way ZDL solutions for Oracle, Windows, UNIX, and databases.	Modification: Must support high-availability 3-way solutions for Oracle, Windows, UNIX, and databases. Justification: request to modify this clause.	Refer #245

Response to the Pre-Bid Queries

17 52	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-72	Must optimise WAN replication traffic with compression; redundant FCIP routers if needed.	Modification: This clause provided undue advantage to an OEM offerings hence, request you to delete this clause for wider participation. In case FCIP routers are required, its shall be asked from all the OEM's. Justification: In a critical banking environment, FCIP routers are must from best practice point of view. Hence request POSB to please make FCIP as a mandatory ask from all the OEM.	Refer #246

Response to the Pre-Bid Queries

17 53	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-77	Must support cyber recovery orchestration with ransomware protection.	Modification: Must support cyber recovery orchestration with inbuilt inline ransomware detection & protection. Justification: Kindly modify this clause with addition of detection feature also.	Refer #247

Response to the Pre-Bid Queries

17 54	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-78	Must support immutable DB- consistent backup copies with WORM/Equivalent, RBAC, SCN-based restore, etc.	Modification: Must support immutable block level/DBconsistent backup copies with WORM/Equivalent, RBAC, SCN-based restore, etc. Justification:DB consistant copies are a feature of Data base only hence request to modify this clause.:	Refer #248

Response to the Pre-Bid Queries

17 55	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-85	Storage management must support customised reports, topology monitoring, chargeback, and trending.	Modification:Storage management must support customised reports, topology monitoringand trending. Justification: we believe POSB is not going to use this Infra for cloud setup. Request to remove the charge back from the specification.	Refer #249

Response to the Pre-Bid Queries

17 56	Volume of the RFP (II)	Annexure L Page No- 260 Clause No SAN Storage-86	Must integrate with existing backup infrastructure.	Justification: This a restrictive clause.please remove this point as this will give undue advantage to existing OEM. Kindly share backup software compliance for wider participation.	Refer #250

Response to the Pre-Bid Queries

17 57	Volume of the RFP (II)	Annexure L Page No- 260- Backup Solution Clause No 1	Enterprise backup platform supporting three-site architecture with central console and role-based access.	Clarification: we understand this is a backup software solution requirement Enterprise backup platform supporting three-site architecture with central console and role- based access.	Refer #251

Response to the Pre-Bid Queries

17 58	Volume of the RFP (II)	Annexure L Page No- 260- Backup Solution Clause No 18	Multi-site, dedupe-enabled appliances with replication; Hot-swap disks/power; Dual controllers.	Modification: Multi-site, dedupe-enabled appliances with replication; Hot-swap disks/power, Dual controller/as per OEM architecture. Justification: This is a restrive clause The proposed backup appliance provides equivalent or superior availability, data integrity, and recoverability. Redundancy and high availability are achieved through a combination of fault-tolerant hardware components. request to modify this clause for wider participation.	Refer #252

Response to the Pre-Bid Queries

17 59	Volume of the RFP (II)	Annexure L Page No- 260 San Switch Clause No 1	SAN switch shall be configured with 48 ports, each supporting minimum 32 Gbps FC, with backward compatibility to 16G and forward compatibility preferred.	Clarification:From a technology vs cost point of view we suggest to consider SAN switch based architerture which can support upto 96 port per switch and will deliver more deloydment feseability options in current sized landscape. We request POSB to modify this request.	Refer #253

Response to the Pre-Bid Queries

17 60	Volume of the RFP (II)	Annexure L Page No- 260 Tape Library Clause No 4	Min 250 slots, scalable upward; adequate media & cleaning cartridges	Modification: Min 240 slots, scalable upward; adequate media & cleaning cartridges. Justification: please change this clause for wider participation	Refer #254

Response to the Pre-Bid Queries

17 61	Volume of the RFP (II)	Annexure L Page No- 260 Tape Library Clause No 8	High-availability robotic subsystem; dual accessor preferred	Justification: please remove this point as this is giving an undue advantage to a specific OEM	Refer #84

Response to the Pre-Bid Queries

17 62	Volume of the RFP (II)	Annexure L Page No- 260 x86 Server Clause No 1	Form Factor-Rack 1U form factor	Modification Request : Pls help to ammend asked clause as" 1U/2U /4U Form factor " Justifictaion : This will enable Flexiblity to sizie solution as per Application OEM sizing Requirement Based on CPU/Local Drives & GPU Requirement	Refer #256

Response to the Pre-Bid Queries

17 63	Volume of the RFP (II)	Annexure L Page No- 260 x86 Server Clause No 6	Storage Controller Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60	Modification Request : Pls help to ammend asked clause as Integrated/PCIe 4.0/5.0 12Gb/s/24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60 Justification : Industry Standard SAS Controller works on 12Gb/s with PCI 4.0 technology . Pls update asked clause to make its as Industry standard technology	Refer #100

Response to the Pre-Bid Queries

17 64	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 2	2.Router should have a physical separation between control and data planes processor. Router should support inline hardware accelerated encryption for high-throughput Ipsec	As per the clause 16 in specification of core Router external appliance is allowed for firewall Functionality , Request to kindly allow to have IPSEC functionality offloaded to external device . This will remove ambiguity in design and will also insure high scale along with maximum participation while insuring maximum return on investment with next generation architecture	Refer #258

Response to the Pre-Bid Queries

17 65	Volume II ,	Annexure L , Core-Router , General Requirement -Clause 3	3. Load balancing feature to be present in routers and must work mainly for internet terminated links. Internet and MPLS both will be terminated in router and the same must work seamlessly in different routing planes without affecting security and maintaining IT security compliance.	we understand that Load balancing / Load Sharing on the internet side can be achieved by BGP learned routes or through Policy based Routing , Kindly confirm	Refer #259

Response to the Pre-Bid Queries

17 66	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 9	9. The router must support IKEv1, L2TP, IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption for traffic from any location to other location on demand and also should be able to create GRE tunnel.	L2TP is a legacy unencrypted protocol , IPSEC is already asked in the tender which is more secure and support by all leading OEM , Request to relax the clause and allow IPSEC to be used in place of L2TP .Also GRE encapsulates the packet ,no encryption is used in GRE , Request to kindly change the clause by removing GRE encryption and on on demand GRE for solution clarity or allow IPSEC / GDOI while the same can be offloaded to external firewall as requested . Requested clause :- The router must support IKEv1, L2TP/IPSEC , IKEv2, GRE and IPSEC from day 1. The proposed solution should serve the GRE encryption/IPSEC	Refer #260

Response to the Pre-Bid Queries

17 67	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 10	10.The router should support 19 Gbps of IPSEC Bandwidth	Request to kindly confirm for offloading the IPSEC to external firewall for leading OEM to participate . The same is also requested in query 1 of core Router	Refer #261

Response to the Pre-Bid Queries

17 68	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 11	11.Implementation Agency should ensure necessary encryption 8.5 Gbps throughput (IMIX, EMIX) supported by proposed device at site from day 1: (IPSEC case of SD-WAN)	Request to kindly remove (IPSEC Case of SDWAN) as the same is creating ambiguity . IPSEC will be used on WAN side for traffic encryption as per the Govt Guide lines and frame work for Financial organization . Request change for leading OEM to participate .	Refer #262

Response to the Pre-Bid Queries

17 69	Volume II ,	Annexure L , Core-Router , Performance Requirement -Clause 12	12.Router should be scalable to support up to 4000 tunnels (non-SDWAN) / 8000 SD_WAN tunnel (SD- WAN)	Different OEM have different architecture for providing the traffic encryption using IPSEC .SDWAN for all OEM is proprietary and can not integrate with any other OEM , Request to kindly remove SDWAN or clarify that either of 4K (no-SDWAN) / 8K should be supported .	Refer #263

Response to the Pre-Bid Queries

17 70	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 17	17.Router should Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided.	Traffic optimization was required on low latency link such as E1 or low speed TDM link which are not used in modern days network , The solution provided will have ethernet connectivity ranging for 1Gps to 100Gbps interface. Also Traffic optimization works on P2P links i.e both side should have functionality . The same is not possible in large and heterogenous network . Request to kindly remove the clause for leading OEM to participate .	Refer #264

Response to the Pre-Bid Queries

17 71	Volume II ,	Annexure L , Core-Router , Layer3 Features & Security -Clause 21	21. Router should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance should be able to do deep packet inspection and identify applications at layer-7 and we should be able to define QoS and access control based on application. It should be possible to identify at least 1000 common applications by Device.	Refer #265

Response to the Pre-Bid Queries

17 72	Volume II ,	Annexure L , Core-Router , Manageability -Clause 25	25. Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	The asked feature is the core functionality of firewall , since the external firewall is allowed for building the solution we kindly request to change the clause for leading OEM to participate . Requested clause :- Router/ external firewall appliance Router should support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	Refer #266

Response to the Pre-Bid Queries

17 73	Volume II ,	Annexure L , Core-Router , Manageability -Clause 29	29. Router should be IPv6 Certified/IPv6 logo ready	All reputed OEM support IPV6 functionality from day 1 , we are providing latest hardware / solution which supports all IPV6 features from day1 . Request to amend the clause for leading OEM to participate . Requested Clause :- Router should be IPv6 Certified/IPv6 logo ready / IPV6 Ready	Refer #267

Response to the Pre-Bid Queries

17 74	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 8	8. Minimum WAN throughput: 20 Gbps (scalable to 40 Gbps).	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the WAN throughput asked is 40Gbps which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Minimum WAN throughput: 320 Gbps (scalable to 340 Gbps).	Refer #268

Response to the Pre-Bid Queries

17 75	Volume II ,	Annexure L , WAN Router , Performance Requirement -Clause 10	10.Forwarding performance: > 30 Mpps.	As per the clause 13, 14,15 in Interface requirement total number of interface are 8X10G + 4X1/10G+ 2X40/100G which totals to 320Gbps . While the MPPS asked is >30MPPS which is blocking architecture . We highly recommend to change the clause for Line rate equipment which will not have bottleneck when 100G interfaces are activated . This will ensure optimum and proper solution and provides ROI to end user . Requested Clause :- Forwarding performance: > 476Mpps.	Refer #269

Response to the Pre-Bid Queries

17 76	Volume II ,	Annexure L , WAN Router , Performance Requirement -Claus23	23.Stateful firewall capabilities.	Request to kindly change the clause for leading OEM to Participate . Requested clause:- .Stateful firewall capabilities/ ACL/ Firewall filter	Refer #270

Response to the Pre-Bid Queries

17 77	Volume II ,	Annexure L , WAN Router , High Availability -Clause 30,31	30.Non-stop Routing (NSR), Non-stop Forwarding (NSF). 31. Stateful switchover (SSO)	For asked functionality to work redundant CPU / Routing engine is required . Kindly clarify if redundant Routing engine is required from day 1 or only support is asked . Kindly clarify for solution clarity .	Refer #271

Response to the Pre-Bid Queries

17 78	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 9	9.The switch should support 30k multicast routes	30K Multicast is on very high side and not required on spine as they act as transit for traffic , request to reduce the route scale for maximum participation for leading OEM to participate . Requested clause :- .The switch should support 8k multicast routes	Refer #272

Response to the Pre-Bid Queries

17 79	Volume II ,	Annexure L , SPINE SWITCH ,Performance Requirement -Clause 25	25.Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP)	MSDP is used on WAN side and is not widely deployed in Spine devices in data center, instead PIM SSM and PIM SM are used request to relax the clause for leading OE tom participate . Requested clause :- Switch should provide multicast traffic reachable using PIM-SM, PIM-SSM and Multicast Source Discovery Protocol (MSDP) / MLD (Multicast Listener Discovery)	Refer #273

Response to the Pre-Bid Queries

17 80	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	17.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Refer #275

Response to the Pre-Bid Queries

17 81	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 17	23.The Switch should support intelligent buffer management with a minimum buffer of 36 MB.	Request to kindly change the packet buffer to 32Mb for leading OEM to participate Requested clause :- 23.The Switch should support intelligent buffer management with a minimum buffer of 32 MB.	Refer #276

Response to the Pre-Bid Queries

17 82	Volume II ,	Annexure L , LEAF SWITCH ,Network Virtualization Features -Clause 26	26.Switch must provide the capability to be integrated with different Hypervisor Managers viz. Vmware vCenter, Microsoft Hyper-V with System Center, Kubernetes, Redhat Openshift and manage virtualize networking from the single pane of glass	Leaf switch connect to any virtualization platform using VLAN . Switch do not connect to any virtualization Manager . The fabric manager / SDN controller defines the EVPN VXLAN fabric on spine and leaf devices , which can further connect to Orchestrator for single pane of glass management. The clause is restricting leading OEM request to change . Requested clause :- Switch must provide the capability to be integrated with different Hypervisor viz. Vmware, Microsoft Hyper-V , Kubernetes, Redhat Openshift using standard based VLAN	Refer #277

Response to the Pre-Bid Queries

17 83	Volume II ,	Annexure L , LEAF SWITCH ,Performance Requirement -Clause 29	29.The switch should have MAC Address table size of 500k	The asked MAC scale is very high on leaf Switch . Request to reduce the scale for leading OEM to participate . Requested clause :- The switch should have MAC Address table size of 250k	Refer #278

Response to the Pre-Bid Queries

17 84	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	47.Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation rules and policies for the Virtualized and Non - Virtualized environment (Bare metal and Container) workloads connected to DC fabric for east-west traffic. It must also support micro- segmentation based on VM attributes like hostname, OS, VM Tags, FQDN, Microsoft AD based classification. The solution must also provide micro segmentation capability on application end host at remote location sites in offline mode (once policy is applied from the DC to workloads on remote sites, in case the sites are dis-connected, the enforcement policy is retained). Mentioned feature/capability should be achieved using same OEM products for a seamless integration, without using any external/3rd party solution.	The micro segmentation in data center in virtualized environment is managed by Virtual machine manager and for Switching environment using Fabric manager . They both integrate using Orchestration layer for single plane of management and integration . The functionality asked is achieved through different architecture from different OEM. The clause in current format is restricting leading OEM's .Request to change the clause for leading OEM to participate . Also request to remove virtualization microsegment into the virtual environment security requirement . This will ensure that level playing field is given to all OEM in data center infra domain. Requested clause :- .Switch should support control plane Protection from unnecessary or DoS traffic by control plane protection policy. Switch must provide the capability of micro-segmentation basis on connected VLAN / Ports .	Refer #279

Response to the Pre-Bid Queries

17 85	Volume II ,	Annexure L , LEAF SWITCH ,Security - Clause 47	49.Switch platform should support encryption of traffic i.e. MAC Sec Encryption (802.1AE) in hardware	Spine switch is not asked with MACSEC , this will create confusion in design . Request either remove MACSEC for leaf switch or add the same in SPINE switch for solution clarity .	Refer #280

Response to the Pre-Bid Queries

17 86	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Clarification Page No- 260 X86-Based Hypervisor & Virtualization	Clarification :RFP Annexure L Have specification section Named as " X86-Based Hypervisor & Virtualization " , Pls clarify which specification to be followed .	Refer #281

Response to the Pre-Bid Queries

17 87	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Solution shall support migration of physical Windows and Linux workloads to virtual environments.	Clarification :We understand Migration of physical Windows and Linux workloads to virtual environments will be Planned & offline activity which may need data Migration manually or using 3rd party tools based on Migration approach . Pls confirm	Refer #282

Response to the Pre-Bid Queries

17 88	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Single-click upgrade or update capability for all compute, hypervisor, and SDS components.	Clarification : We understand SDS - Software Defined Storage is not in scope of this RFP architecture requirement , Pls Remove ask of SDS Solution Requirement Justification : SAN Storage is asked , Hence SDS is not in scope for architecture Requirement	Refer #283

Response to the Pre-Bid Queries

17 89	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor Clause no 3	Licenses to deploy a purpose- built, bare-metal hypervisor with in-built SDS support.	Clarification : We understand SDS - Software Defined Storage is not in scope of this RFP architecture requirement , Pls Remove ask of SDS Solution Requirement Justification : SAN Storage is asked , Hence SDS is not in scope for architecture Requirement	Refer #284

Response to the Pre-Bid Queries

17 90	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Zero downtime host patching with automated workload migration.	Change Request : Request you to Change asked Clause as "Zero downtime or Planned host patching with automated workload migration. Justification : IN pRoduction environment - Updates/Upgrades required Plananed workload Host Migration .	Refer #285

Response to the Pre-Bid Queries

17 91	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Continuous availability using live shadow VMs for fault tolerance.	Change Request : Request you to Change asked Clause as "Continuous availability using live shadow VMs for fault tolerance/ Highavailability Feature with Live Migration" Justification : fault tolerance can be implemented with High availability Live Migration Feature"	Refer #286

Response to the Pre-Bid Queries

17 92	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support remote port mirroring and 802.1q VLAN configurations.	Please remove asked clause, asked remote port mirroring and 802.1q VLAN configurations is not supported in Virtualization environment	Refer #287

Response to the Pre-Bid Queries

17 93	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide VM-level encryption for data at rest and in motion (AES-256).	Change Request : Request you to Change asked Clause as"Provide VM-level encryption for data at rest and in motion (AES-256) using Security Infrastructure . Justification : Encryption for data in motion (AES-256) will be Feature of Firewall / Security Infrastructure	Refer #288

Response to the Pre-Bid Queries

17 94	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide visibility of east-west and north-south network traffic between VMs.	Change Request : Request you to Change asked Clause as"Provide visibility of east- west and north-south network traffic between VMs using 3rd Part Tools & Automation solution Justification : This is 3rd Party solution Feature , which can be Intregrated with Virtualization Platform	Refer #289

Response to the Pre-Bid Queries

17 95	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable SDN-based virtualised networking and distributed firewalling.	Change Request : Request you to Change asked Clause as"Enable SDN-based virtualised networking and distributed firewalling using 3rd Part Tools & Automation solution Justification : This is 3rd Party solution Feature , which can be Intregrated with Virtualization Platform	Refer #290

Response to the Pre-Bid Queries

17 96	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support distributed routing and security system policy migration with VMs.	Change Request : Request you to Change asked Clause as"Support distributed routing and security system policy migration with VMs Nativly or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #291

Response to the Pre-Bid Queries

17 97	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support network analytics, flow assessment, and zero-trust policy enforcement.	Change Request : Request you to Change asked Clause as"Support network analytics, flow assessment, and zero-trust policy enforcemen or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #292

Response to the Pre-Bid Queries

17 98	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable multi-site network and micro-segmentation across workloads.	Change Request : Request you to Change asked Clause as"Enable multi-site network and micro-segmentation across workloads. or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #293

Response to the Pre-Bid Queries

17 99	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Provide service chaining for north-south/east-west traffic inspection.	Change Request : Request you to Change asked Clause as"Provide service chaining for north-south/east-west traffic inspection. or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #294

Response to the Pre-Bid Queries

18 00	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support secure VPN connectivity between data centres and clouds.	Change Request : Request you to Change asked Clause as"PSupport secure VPN connectivity between data centres and clouds. or with network & Security devices intregartion . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #295

Response to the Pre-Bid Queries

18 01	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support IPv4 and IPv6, extendable overlay and VLAN subnet capabilities.	Change Request : Request you to Change asked Clause as"Support IPv4 and IPv6, extendable overlay and VLAN subnet capabilities or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #296

Response to the Pre-Bid Queries

18 02	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Offer an automated micro- segmentation policy recommendation engine.	Change Request : Request you to Change asked Clause as"Offer an automated micro-segmentation policy recommendation engine. or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #297

Response to the Pre-Bid Queries

18 03	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support virtual edge devices for routing, NAT, and security system functions.	Change Request : Request you to Change asked Clause as"Support virtual edge devices for routing, NAT, and security system functions or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #298

Response to the Pre-Bid Queries

18 04	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Enable per-workload stateful firewalling and ALGs with central management.	Change Request : Request you to Change asked Clause as"Enable per-workload stateful firewalling and ALGs with central management or with network & Security devices intregation . - Justification: This is Network switch & Security Devices Intregation Feature	Refer #299

Response to the Pre-Bid Queries

18 05	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	Support AES-256 encryption for data at rest and in transit with KMIP 1.1 compliance.	Change Request : Request you to Change asked Clause as"Support AES-256 encryption for data at rest and in transit with KMIP 1.1 compliance nativly or via external KMIP solution intregration - Justification: Option of external KMIP solution intregration will be allowed	Refer #300

Response to the Pre-Bid Queries

18 06	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should edit or add network adapters, including multiple NIC models, Masquerade, and MAC address customization.	Removal Request : Please remove ask of Masquerade, and MAC address customization. Justification : This is not nactive Feature of Hypervisor , Pls remove this ask of Masquerade, and MAC address customization.	Refer #301

Response to the Pre-Bid Queries

18 07	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should include a compute virtualization layer on bare metal hardware with no dependence on a general- purpose OS, featuring proactive HA, DRS, replication, fault tolerance with continuous availability, and hot add of CPU, memory, and devices for Windows and Linux VMs.	Change Request : Request you to Change asked Clause as "The solution should include a compute virtualization layer on bare metal hardware with no dependence on a general- purpose OS, featuring proactive HA, DRS, replication, with continuous availability, and hot add of CPU, memory, and devices for Windows and Linux VMs. Justification: Please Remove ask of fault tolerance feature , as this specific to single OEM	Refer #302

Response to the Pre-Bid Queries

18 08	Volume of the RFP (II)	Annexure L Page No- 260 X86-Based Hypervisor & Virtualization	The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption.	Change Request : Please Change asked Clause as "The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption & using of San Stoarge base Relication Feature with or with out downtime . Justifictaion : asked solution need to be implemmeted with Storage Based Replication Feature with Downtime .	Refer #303

Response to the Pre-Bid Queries

18 09	Volume of the RFP (II)	Annexure L Page No- 260 Automation	The software should support system tracking to audit and verify that machines comply. It should help to discover how a machine has changed over time or compare machines in running cluster to see how they are different.	Clarification: we Understand this is Inventory Tracking & Discovery Feature ask, Pls Confirm	Refer #304

Response to the Pre-Bid Queries

18 10	Volume of the RFP (II)	Annexure L Page No- 260 Container Management Platforms	The container platform should be compatible and certified across MEITY empanelled cloud platforms/ Hyperscalers with Enterprise support. It must also provide a single cloud native platform support if and when need be.	Request to change to : The container platform should be - compatible with certified across MEITY empanelled cloud platforms/ Hyperscalers with Enterprise support. It must also provide a single cloud native platform support if and when need be. An equivalent offering may also be quoted	Refer #305

Response to the Pre-Bid Queries

18 11	Volume of the RFP (II)	Annexure L Page No- 260 Container Management Platforms	The Container Platform should offer container scanning capability.	Clarification's help to explain the ask here , we Understand this is Security Infrastructure Feature to scan the Containers from security POV	Refer #306

Response to the Pre-Bid Queries

18 12	Volume II	Page no. 51 Clause: 5.2.1.1 Facility Requirements Sub Clause: 5.2.1.1.1 General Requirements	The proposed DCF shall have a minimum Tier-III standard certificate by an agency such as Uptime Institute or a TIA 942 design certificate.	We adhere to TIA-942 Rated-3 standards. The redundancy and uptime SLA requirements defined under TIA-942 Rated-3 are equivalent to Uptime Institute Tier III. In addition, TIA-942 also comprehensively addresses architectural and network redundancies. Hence, we request you to kindly consider and include the Rated classification as well.	Refer #376

Response to the Pre-Bid Queries

18 13	Volume II	Annexure I Section B: Physical Security Requirement Point no. 4	The proposed facility shall have 24x7 surveillance (CCTV with built-in intelligence and auto triggering of alert/response for unusual activities).	The proposed facility is equipped with a comprehensive 24x7 CCTV surveillance system covering all critical areas, integrated with a centralized monitoring mechanism and defined incident response procedures. While video analytics / built-in intelligence with auto-triggered alerts is not currently implemented, continuous live monitoring by trained security personnel is in place to detect and respond to any unusual or suspicious activities in real time. The existing surveillance and response framework ensures effective security oversight and meets the intent of the clause. Hence, relaxation is requested for the requirement of video analytics-based auto alerting.	Refer #377

Response to the Pre-Bid Queries

18 14	Volume II	Annexure I Section B: Physical Security Requirement Point no. 4 (subpoint 4)	Surveillance should be integrated with IBMS as well as the NOC central monitoring.	Dual integration with both IBMS and NOC is not available. The existing IBMS integration adequately supports continuous monitoring and response procedures. Relaxation is requested to permit integration with IBMS only.	Refer #378

Response to the Pre-Bid Queries

18 15	Volume II	Annexure I Section B: Physical Security Requirement Point no. 7	The hosting space entrance & exit should be accessible using the biometric access system with minimum two-factor authentication (fingerprint sensor + access card control system) in addition to the physical lock (Palm sure scanner, iris scanner, face scanner may be considered).	The hosting space entrance and exit are secured through a two-factor authentication access control system, comprising fingerprint biometric verification and access card control, in addition to physical locking mechanisms. Advanced biometric modalities such as palm vein (PalmSure) and iris scanners are not deployed at the facility. Facial recognition-based access control may be considered, subject to client requirement and mutual agreement. The existing authentication framework ensures controlled access, traceability, and compliance with security objectives. Accordingly, relaxation is requested for the requirement of palm vein and iris scanners.	Refer #379

Response to the Pre-Bid Queries

18 16	Volume II	Annexure I Section B: Physical Security Requirement Point no. 9	The DCF Provider shall provide a dual door/trap door solution at the main entry of the Server Room to avoid tailgating. Apart from this, the main entrance to the DC area should have a half-height Turnstile/Tripod/Flap barrier, along with access card access.	While a dual door / trap door solution is not deployed, the facility implements alternative access control measures designed to prevent tailgating and unauthorized entry. These include full-height turnstiles and access-controlled lifts with card-based authentication and monitoring. Relaxation is requested to accept the existing configuration.	Refer #380

Response to the Pre-Bid Queries

18 17	Volume II	Annexure I Section C: Power Point no. 2	The proposed co-location facility for Data Centre hosting shall have the incoming utility power supply from two different sub-stations (redundancy planning) as the primary source, and automatic switchover to Data Centre Continuous Rated Diesel Generators set as a secondary source. In case of power failure, automatic switchover to the DG set as a secondary source provision should be available. The Diesel Generators shall have sufficient fuel to cater to the infrastructure for a minimum of 72 hours in the event of a major outage. The fuel lines providing fuel to the Diesel Generators shall be in redundancy along with the supply pumps as well.	Relaxation is requested to modify the diesel fuel storage requirement from 72 hours to a minimum of 24 hours, in alignment with industry-accepted standards and best practices.	Refer #381

Response to the Pre-Bid Queries

18 18	Volume II	Annexure I Section C: Power Point no. 3	Backup generators (Redundant) should be capable of providing power backup for 72 hours. Backup generators should be capable of providing power continuously for at least 72 hours, and even during the refilling period of fuel tanks. The capacity of each set of diesel generators should be sufficient to take care of the entire power load of the Data Centre. The DCF Provider should ensure an uninterrupted supply of diesel to the DG with an adequate storage facility. The Diesel Generators shall be of Data Centre Continuous (DCC) rating type.	Relaxation is requested to modify the diesel fuel storage requirement from 72 hours to a minimum of 24 hours, in alignment with industry-accepted standards and best practices.	Refer #382

Response to the Pre-Bid Queries

18 19	Volume II	Annexure I Section C: Power Point no. 5	DCF Provider shall provide an adequate number of single-phase and three-phase power sockets to support POSB's equipment in the server area with appropriate connectors for connectivity with rack PDUs and at the network communication area.	We request Dept of Post to kindly share the number of Single and three Phase sockets required	As per RFP

Response to the Pre-Bid Queries

18 20	Volume II	Annexure I Section C: Power Point no. 7	Two separate power paths from the UPS are to be provided to the Server room area and the network communication area. The UPS should be configured in parallel active mode, and each should not be loaded more than % of its capacity.	Dept of Post is requested to kindly share the understanding of UPS configured in parallel active mode as we have UPS with N+N Redundancy	Refer #383

Response to the Pre-Bid Queries

18 21	Volume II	Annexure I Section C: Power Point no. 9	The UPS systems should be fault-tolerant with 2 separate paths for the power supply to each rack. Adequate battery backup should be available for maintaining the uptime requirement of the IT Infrastructure.	In the previous point , the UPS redundancy has been specified as N+1 and fault-tolerant. However, as per TIA-942 Rated-3 / Uptime Tier III requirements, the UPS system is required to be concurrently maintainable and not fault-tolerant. Fault-tolerant design is a requirement for Tier IV (Rated-4) facilities. We seek clarification here.	Refer #384

Response to the Pre-Bid Queries

18 22	Volume II	Annexure I Section F: Server Room Area Point no. 2	The server room area should have a raised floor height of 2ft.	The Server Room area is designed with a raised floor height of minimum 2 feet. Modern Data Centre designs increasingly aPOSBt raised floor heights exceeding 2 feet to effectively support medium- and high-density deployments, improved airflow management, enhanced cable routing, and scalability requirements. In view of evolving industry practices, we request the clause be revised from "raised floor height of 2 feet" to "raised floor height of minimum 2 feet."	Refer #385

Response to the Pre-Bid Queries

18 23	Volume II	Annexure I Section F: Server Room Area Point no. 4	DC Power (UPS output/ power input).	Dept of Post is requested to clarify that do we need DC power in Data Centre.	Refer #386

Response to the Pre-Bid Queries

18 24	Volume II	Annexure I Section F: Server Room Area Point no. 26	Perimeter Wall and Doors should have at least 1 1-hour fire Rating.	The previous clauses are requesting the same as 2 hours. Please clarify.	Refer #387

Response to the Pre-Bid Queries

18 25	Volume II	Annexure I Section H: Building Management System Point no. 5	The DCF Provider shall furnish a complete water leak detection system, including (but not limited to) electronic alarm modules, water sensing cable, graphic display map, auxiliary equipment, etc. The system shall be capable of automatically detecting the presence of water or any other liquid at any point covering the entire DC and should be able to generate an alarm and locate, with a digital display, the point of contact.	We install the Water leak detection system in the PAHU Galleries area prone to water leakage , So we request to please modify the same.	Refer #388

Response to the Pre-Bid Queries

18 26	Volume II	Annexure I Section H: Building Management System Point no. 14	Shall provide on monthly basis and/or upon request from POSB, the details of people accessing all the facilities provided to POSB such as server room area, communication area by sharing entries made in the security register that contains the name, company and contact details of persons entered, purpose of entry, etc. along with reports, access logs, CCTV video clips etc.	We only share the entire of the customer specified area that is caging and not for the communication room as ours is a shared facility so request Dept of Post to modify the clause accordingly.	Refer #389

Response to the Pre-Bid Queries

18 27	Volume II	5.1.5.1 General A. Core Responsibilities	Ensure uninterrupted availability and reliability of IT services in compliance with applicable regulatory and security standards, including RBI, CERT-In, and PMLA.	PLs provide which RBI and ISO standards needs to be additionally provided for existing system for bidder to plan. There is no mention of which particular standards that need to be followed as a priority for compliance standards.	Bidders are expected to ensure adherence to relevant RBI, CERT-In, DPDP Act, and other applicable regulatory and statutory compliances

Response to the Pre-Bid Queries

18 28	Volume II	5. Detailed Scope of Work	Track 2: Operations and Maintenance of IT Infra at new DC, NDC and DR	RFP asks for Zero RPO - but when the operations transfer to DR then how will Zero RPO be maintained without a NDR site. We request Zero RPO to be removed when moving to DR site.	Refer #529

Response to the Pre-Bid Queries

18 29	Volume II	3.2 Broad Scope of Work Sub Point : 3. Application Development and Enhancements Page 14	Establishment of separate environments for development, user acceptance testing (UAT), and sandbox/pre-production. Each environment should simulate a near-production network, security, and data flows.	There needs to be percentages defined for each environment for app Non production (in relation to production)else there will be no way to assess and compare one Bidder's Sizing to another objectively. Typicall in any Banking set up - percentages are defined for each enviornment like (for example:) 10% of Prodcution for Development (example) 30% for UAT (example only) 100% for Pre Prod (example only) 100% for Load Testing (with say 60% utilisation) - example only 100% for DR	Bidders may refer to the Functional Requirements as mentioned in the Corrigendum along with the technical annexure for updated details of the requirements.

Response to the Pre-Bid Queries

18 30	Volume II	5.2.5.10, Page Number 117, Point no 2	The solution must handle a sustained throughput of at least 20,000 transactions per second (TPS) with the capacity to scale up to 50,000 TPS to accommodate future growth over the contract period	1. It is written Sustained TPS of 20000 - or middleware should support upto 20000 TPS. Assumed this TPS is for WebSphere Application Serve. Please confirm? 2. Please confirm the 20000 TPS is sustained on WebSphere Application Server as its not aligned with Annexure O - Where Online + Offline and TPS comes around to be 2000? 3. Please give me the expected TPS required for ESB and WebSphere Application Server sepearately?	Refer #6

Response to the Pre-Bid Queries

18 31	Volume II	Annexure O	User Metrics	Can TPS advised for Online and Offline TPS be used for TPS for API Gateway?	Refer #7

Response to the Pre-Bid Queries

18 32	Volume II	Annexure J Middleware Tab	Cross-language client SDKs with support for programming languages including but not limited to Java, C, C++, C#, Ruby, Perl, Python, PHP, and VB6.	Assume Cross Language SDKs are required to develop microservices? Are you looking to modernize WebSphere Application Server Services to microservices on Kubernetes Environment?	Refer #8

Response to the Pre-Bid Queries

18 33	Volume II	Annexure J Middleware Tab	Support for multiple messaging protocols including OpenWire, STOMP, AMQP, MQTT, and JMS.	Assume this requirement is for services running on WebSphere Application Server. Please confirm ? Also, Please specify the number of interfaces using these messaging protocols in current environment	Refer #9

Response to the Pre-Bid Queries

18 34	Volume II	Annexure J Middleware Tab	Support for pluggable transport protocols such as In-VM, TCP, SSL, NIO, UDP, multicast, JGroups, and JXTA.	Assume, this requirement is for services running on WebSphere Application Server. Please confirm? Also, if you can specify if you are willing to use it in microservices ?	Refer #10

Response to the Pre-Bid Queries

18 35	Volume II	Annexure J Middleware Tab	The ESB shall allow integration with multiple programming environments, including Java, .NET (C#, VB, F#, etc.), PHP, ESQL, and C++.	Is there any requirement to run PHP In ESB or Can it be removed ?	Refer #11

Response to the Pre-Bid Queries

18 36	Volume II	Annexure J Middleware Tab	Guaranteed and assured message delivery.	It seems there is requirement for IBM MQ. Can you please specify if you have MQ or needs to be supplied as part of middleware? If needs to be supplied then please specify the number of interfaces which will depend on MQ with approximate size of message	Refer #12

Response to the Pre-Bid Queries

18 37	Volume II	Annexure J API Gateway Tab	It shall support active-active clustering to provide high availability and resiliency.	Assuming Active-Active DR is required and High Availability is being considered through Container native solutions ? Please confirm	Refer #13

Response to the Pre-Bid Queries

18 38	Volume II	Annexure J API Gateway Tab	Support for runtime policy enforcement, circuit breakers, hard timeouts, service discovery, and load balancing of microservices is required.	Do you need to implement circuit breaker on API Gateway ? Can you please explain the use case of Circuit breaker ?	Refer #14

Response to the Pre-Bid Queries

18 39	Volume II	Annexure J API Gateway Tab	It shall enable bi-directional data format conversion between multiple widely used formats such as ISO, JSON, XML, CSV, and flat files.	Can the conversion be achieved using ESB as supplementary tool for some complex scenarios?	Refer #15

Response to the Pre-Bid Queries

18 40	Volume II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	Since the Middleware Server used as WebSphere Application Server along with ESB- (TIBCO). Can you please share the number of interfaces implemented on WebSphere Application Server and TIBCO separately?	Refer #16

Response to the Pre-Bid Queries

18 41	Volume II	Infra- Software Pg 237	IBM WebSphere Application Server Network Deployment	There are single specifications given for Middleware. Can you please help me with ESB Particulars?	Refer #17

Response to the Pre-Bid Queries

18 42	Volume I	Section 5.20, Page 98	Form A 20	Can the Manufacturers'/ Producers' Authorization Form be submitted in Standard OEM format	Refer #18

Response to the Pre-Bid Queries

18 43	Volume II	Section x, Page 38	Reports	We understand that data lake house setup is out of the scope for this RFP	Refer #19

Response to the Pre-Bid Queries

18 44	Volume II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	The Environments are not defined in Scope and Compliance Sheet. Do you require separate Environment for all these multiple Environments ?	Refer #20

Response to the Pre-Bid Queries

18 45	Volume II	Annexure J Middleware Tab	Environments are not defined	Can I assume the environment similar to API Gateway tab? If yes, then can you please specify the TPS required for ESB	Refer #21

Response to the Pre-Bid Queries

18 46	Volume II	Annexure J API Gateway Tab	The solution shall be deployed across multiple environments, including Development, User Acceptance Testing (UAT), Sandbox/Pre-Production, and Production, closely simulating live operations.	Can you please define TPS for these environments separately?	Refer #22

Response to the Pre-Bid Queries

18 47	Volume II	Annexure J API Gateway Tab	Facilities for seamless integration with developers' IDEs and support for issue resolution workflows must be provided.	Can you please specify the workflows for issue resolution in IDE? Do you mean API Debugging ?	Refer #23

Response to the Pre-Bid Queries

18 48	Volume II	Annexure J API Gateway Tab	Compliance with relevant regional, national, and international regulations such as the Reserve Bank of India (RBI) guidelines, ISO 27001, Financial Data Exchange (FDX), and data privacy laws including the Indian Personal Data Protection Bill (PDP Bill) shall be ensured.	This requirement should be for complete API Solution instead of just API Gateway. API Gateway may work with other products to implement these framework. Can you please update the statement according to API Gateway as API Gateway only store information as defined by the solution	Refer #24

Response to the Pre-Bid Queries

18 49	Volume II	Annexure L Container mgmt	The container platform should be one that provides a developer portal, plugins, middleware and inbuilt integrated IDE for developers to easily work on the same container platform to bring consistence and faster application lifecycle.	There is a separate requirement of middleware in the rfp with API gateway and ESB. Are you also planning to leverage a separate middleware of the container platform?	Refer #25

Response to the Pre-Bid Queries

18 50	Volume II	Annexure B	Microsoft Biztalk	Assuming all Biztalk interfaces can be migrated or modernized to new ESB Solution. Please confirm?	Refer #26

Response to the Pre-Bid Queries

18 51	Volume II	Infra- Software Pg 238	IBM WebSphere Application Server Network Deployment	Are you looking to modernize WASND runtime?	Refer #27

Response to the Pre-Bid Queries

18 52	Volume II	Annexure L Container mgmt		What is the total worker node core that you are expecting for container mgmt platform to manage?	Refer #28

Response to the Pre-Bid Queries

18 53	Volume II	Annexure J Archival	SI must include and provide the Solution capacity sizing, which shall include sizing for Hardware and Software based on the requirement in Annexure- Bill of Material (BoM). For the Database, POSB shall provide Oracle licenses, and SI need not factor the cost for the database licenses.	Should Database not be considered for any of the module mentioned in the RFP? Will this be taken care by POSB?	Refer #29

Response to the Pre-Bid Queries

18 54	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 1. Network Security	Furthermore, the framework requires specialized Operational Technology (OT) Security for industrial assets	Is the requirement for a separate IAM setup for the OT environment? If yes, please provide the following details: 1. Is there a separate air gapped Ot environment in POSB's environment for which a separate IAM setup is needed? Or does the POSB intend to leverage a central IAM setup for both IT and OT assets? 2. What are the use cases that are needed to be implemented for IAM in the OT environment? For e.g. JML automation, SoD, strong authentication, privileged access management, remote privileged access etc.) 3. Please provide the count of users for the following: a. Admin users b. Non-admin users/end users c. non-human privileged identities 3. What are the different OT assets to which the access has to be secured? SCADA/HMI/PLCs etc.	Refer #30

Response to the Pre-Bid Queries

18 55	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 4. Identity Management	The solution is required to provide a comprehensive Identity & Access Management (IDAM) system to govern user identities.	Please provide the following details: 1. Count of users: a. Internal users/Employees b. External users (third party/contractors etc.) 2. Are there any legacy/in-house developed applications? Do these applications expose any APIs? If no, then do these applications support SCIM for provisioning/deprovisioning? 3. What is the authoritative source for the user identities? 4. What are the use cases that are needed to be implemented for identity management: For e.g. - a. User lifecycle management b. role based/attribute based access control c. role optimization d. access recertification campaigns e. role based/business activity based separation of duties f. access provisioning/deprovisioning to hosts, etc.	Refer #31

Response to the Pre-Bid Queries

18 56	Volume II	5.2.4.8.1 Security Requirement, Page 96, Clause: 4. Identity Management	To balance security with user experience, the framework must support Single Sign-On (SSO) for seamless access across platforms, reinforced by Multi-Factor Authentication (MFA) to ensure robust identity verification before granting access.	1. What are the directories that POSB is currently using? AD/LDAP/databases etc. 2. Does POSB need to provide Federation as part of SSO/MFA? 3. Please provide the count of users: a. internal users b. external users (third party/customers) c. customers 4. Is API authentication to be implemented? 5. Is the solution expected to support consent management for consumers?	Refer #32

Response to the Pre-Bid Queries

18 57	Volume II	Annexure N - MFA & SSO, Item No. 21	Solution should be able to provide an option to enforce capturing of each step taken during a web session for selected users, without changing the code of the application, for audit purposes at least 50 license only.	Please confirm if this capability is required to be users for admin users only	Refer #33

Response to the Pre-Bid Queries

18 58	Volume II	Annexure N - MFA & SSO, Item No. 22	Solution should allow captured recording to be filtered by type of actions without changing the code of the application	Please confirm if this capability is required to be users for admin users only	Refer #34

Response to the Pre-Bid Queries

18 59	Volume II	Annexure N - MFA & SSO, Item No. 23	Solution should allow captured recordings to be searchable by keyword or date without changing the code of the application	Please confirm if this capability is required to be users for admin users only	Refer #35

Response to the Pre-Bid Queries

18 60	Volume II	Annexure N - MFA & SSO, Item No. 35	Proposed services and sub-processors must be hosted in India for customer data protection	Does POSB want an on-prem solution for SSO/MFA or is looking for a SaaS based solution for this?	Refer #36

Response to the Pre-Bid Queries

18 61	Volume II	Annexure N - PAM, Item No. 3	Vendor must to rotate password, support authentication against AD,run account discovery and also function as RDP and SSH jumphost with ONLY ONE windows service.	Is there any specific need for mandating a single windows service or is the requirement just to simplify management of privileged access across all endpoints?	Refer #37

Response to the Pre-Bid Queries

18 62	Volume II	Annexure N - PAM, Item No. 10	The proposed solution must support but not limited to the major types of accounts for password changing out-of-the-box. Active Directory (All Account) Windows Local User & Administrative Accounts Linux Local User & Administrative Accounts (Any Distribution) Unix Local Users & Administrative Accounts (Any Distribution) Network System Accounts Out-of-Band Management Systems AWS IAM Access Keys MS Azure Office 365 SSH Keys Database Accounts LDAP Accounts.	Please provide the following details on the AWS IAM and SSH Keys: 1. Does POSB want the solution to act as a certificate authority for the AWS IAM keys and the SSH keys? 2. If yes, please provide the number of applications/clients that need access to these keys 3. Does POSB require the proposed solution to generate new keys as part of credential rotation? Or does the new key generation need to be handled by AWS IAM/POSB's Certificate Authority? 4. If POSB's existing Certificate Authority is to be leveraged, please share its name and version details.	Refer #38

Response to the Pre-Bid Queries

18 63	Volume II	Annexure N - PAM, Item No. 102	Solution must support real-time reputation checking	Please elaborate on what do you mean by reputation checking	Refer #39

Response to the Pre-Bid Queries

18 64	Volume II	Section 6.7 / Pg135/ 6.7.1	6.7.1	No.of Users for L1, L2, L3	Refer #40

Response to the Pre-Bid Queries

18 65	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Leverage AI/ML techniques with no-code/low-code interfaces, enabling business users and data scientists to develop and refine fraud detection models.	Does POSB expect business users to independently configure and retrain fraud models using no-code/low-code interfaces, or should such activities be restricted to SI or data-science teams? If yes then please confirm on the number of such developers from POSB.	Refer #41

Response to the Pre-Bid Queries

18 66	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Support real-time case management features, including alert assignment, prioritized queues, case notes, attachments, escalation, reminders, and reporting.	POSB is expecting a full-featured case management system with configurable workflows, SLAs, escalations and document management system. Please confirm	Refer #42

Response to the Pre-Bid Queries

18 67	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	We understand that POSB expects EFRM reporting to be delivered via an embedded reporting layer, which should be a part of the overall solution. Please confirm	Refer #43

Response to the Pre-Bid Queries

18 68	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm average and peak daily transaction volumes across all channels to enable accurate sizing of real-time fraud detection infrastructure.	Refer #44

Response to the Pre-Bid Queries

18 69	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Please indicate expected daily fraud alert volumes and number of concurrent investigation users for case management sizing(workflow management)	Refer #45

Response to the Pre-Bid Queries

18 70	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	What is the historical data window in years or TB expected to be provided for fraud model training and back-testing?	Refer #46

Response to the Pre-Bid Queries

18 71	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm the expected number of dashboards, & reports to be created as a part of the solution	Refer #47

Response to the Pre-Bid Queries

18 72	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Reporting and Business Intelligence	Please confirm on the total number of viewers, users, editors and administrators of such reports	Refer #48

Response to the Pre-Bid Queries

18 73	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Incorporate continuous model lifecycle management, including development, deployment, monitoring, model governance, retraining, and scorecarding.	If AI/ML or Generative AI solutions are proposed, are there any specific governance, explainability, auditability or model-risk requirements expected by POSB beyond standard RBI, CERT-In and DPDP compliance?	Refer #528

Response to the Pre-Bid Queries

18 74	Volume II	Section 5.2.5, Page number 117, Clause number 5.2.5.9 EFRM	Investigations and Case Management	Does POSB intend to standardize document management, records retention and audit evidence on a centralized Enterprise Content Management (ECM) platform and scanning solution(for physical documents), or should existing document repositories continue without transformation? If a new solution is needed, kindly confirm on the average number of documets to be digitized and number of concurrent users for the platform.	Refer #50

Response to the Pre-Bid Queries

18 75	Volume II	Section 5.2.5, Page number 116, Clause number NA	Application Development & Integration of new functionalities	For use cases involving forms, certificates, KYC documents or regulatory submissions, should the solution propose ntelligent Document Processing (OCR + AI classification and extraction) capabilities. If yes, then please confirm the average document volume to be extracted in a year.	Refer #51

Response to the Pre-Bid Queries

18 76	Volume II	Section 5.2.5, Page number 116, Clause number 5.2.5.9 EFRM	Fraud Detection and Analytics	Please confirm the expected no. of machine learning or scoring models that will be deployed for the solution	Refer #52

Response to the Pre-Bid Queries

18 77	Volume II	Section 5.2.5, Page number 115, Clause number 5.2.5.9 EFRM	Rule Management and Scenario Tuning	Pleasee confirm on the concurrent number of rules which can be triggered for seamlessly running the various transactions related to eFRMS.	Refer #53

Response to the Pre-Bid Queries

18 78	Volume II	Annexure N / Database Activity Monitoring	Solution should provide functionality to test policies before enabling	Ideal method to test security policies are in UAT enviornment and not on production setup , it is thus requested to remove the clause and leverage UAT for testing purpose	Refer #54

Response to the Pre-Bid Queries

18 79	Volume II	Annexure N / Database Activity Monitoring	The solution should have an agentless DAM architecture that can monitor database activity without the need for deploying agents on the database servers or enabling native logging eliminating performance impacts on database.	We understand the expectation is to have solution which support both agent based and agent less solution. Since one method is required atleast for collection or generation of logs	Refer #55

Response to the Pre-Bid Queries

18 80	Volume II	Annexure N / Database Activity Monitoring	The solution should be able to integrate with the existing Data Activity Monitoring and Governance solution into a consolidated dashboard.	Dam solution allow forwarding security logs to technology such as siem and ticketing solution to help in overall security monitoring and governance. Hope the same is acceptable to the client.	Refer #56

Response to the Pre-Bid Queries

18 81	Volume II	Annexure N / Database Activity Monitoring	The proposed consent management solution should be capable of being deployed On-prem.	Consent management is not part of the DAM solution it is thus requested to move this clause to the relevant solution such as IAM.	Refer #57

Response to the Pre-Bid Queries

18 82	Volume II	Annexure N / Database Activity Monitoring	The solution SAAS platform should be hosted in India.	The RFP talks about On- prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Refer #58

Response to the Pre-Bid Queries

18 83	Volume II	Annexure N / Database Activity Monitoring	The SAAS platform must be SOC2 type 2,SOC type 3, ISO/IEC 27001:2022, 27018:2019 and 27017:2015 compliant	The RFP talks about On- prem solutions while the clause talk about SAAS , looking at the criticality of the project we request the client to reconsider this clause and request for on-prem deployment.	Refer #59

Response to the Pre-Bid Queries

18 84	Volume II	5.1.2.3 Transition of Applications. Page 27	• Finacle Core Banking Solution (CBS) v10.2.13 and all associated customisations and interfaces. • Internet Banking, Mobile Banking, and other POS channel integrations. • Allied enterprise applications, Risk-Based Authentication (RBA), AML/CFT solution, Aadhaar Data Vault and eKYC, Cheque Truncation System (CTS), Middleware solutions, APIs, and batch processing systems.	Please confirm if PLI is under the scope of this RFP, as PLI is not specifically mentioned.	Refer #60

Response to the Pre-Bid Queries

18 85	Volume II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if the existing hardware will be used while performing the upgrade and during parallel run	Refer #61

Response to the Pre-Bid Queries

18 86	Volume II	5.1.3 Upgrade of Finacle CBS and Alert Solution, Page 28	Installation and configuration of Finacle version 10.2.25, incorporating the latest service packs and patches, along with the migration of the database from version 10.2.13 to 10.2.25, ensuring complete preservation of data integrity.	Please confirm if PLI Application will also be part of this application upgrade. Since PLI is running on EOSL hardware, upgrade of hardware may require PLI application upgrade also, please confirm if PLI application version is EOSL or not, if under mainstream support, will it support the upgraded hardware.	Refer #60

Response to the Pre-Bid Queries

18 87	Volume II	Bill of Quantity, 1. Compute, Page 212	SI No 15 to 42, IBM Power Systems 780 & HMC - CR7 are EOSL	Please confirm if this hardware is under this RFP Scope & will be considered as part of SLA defined in this RFP as these are already EOSL hardware	Refer #63

Response to the Pre-Bid Queries

18 88	Volume II	7. Physical Server Details, Page 239	SL no - P780 - AMC Validity Status - 29-09-2026	AMC Validity Status for P780 is not matching with AMC Date specified on Page 212. Please confirm the correct AMC Vailidity Date. Please confirm the AMC type - Best Effort/Non SLA Based or Mainstream support as EOSL is already bypassed	Refer #64

Response to the Pre-Bid Queries

18 89	Volume II	Annexure H – Specification of Existing Racks, Page 254	<<General Query>>	Please confirm the availability of Free Rack Space, PDU points & Power, incase any additional hardware needs to be provisioned during Track 1 in existing DC, especially during Finacle Upgrade	Refer #65

Response to the Pre-Bid Queries

18 90	Volume II	5.1.4 Operations and Maintenance of Existing Applications	The entire system should meet the requirements detailed in the RFP. It should also meet the expected performance levels and desired uptime as per Section 5 – Service Level Agreement, with respect to various fault tolerance/DR practices envisaged in the RFP. With reference to this, below are the key requirements:	Please confirm if all applications will be under this RFP Scope & will be considered as part of SLA defined in this RFP, especially if any application (or hardware they are running on) are already EOSL.	Refer #66

Response to the Pre-Bid Queries

18 91	Volume II	ii. System Support	h. The SI shall be responsible for fixing all bugs and program errors, whether identified by POSB or detected by the SI during testing, operations, or monitoring — across both existing and newly developed modules.	Please confirm the scope and SLAs incase the application is running with EOSL version or running with hardware with EOSL, where OEM doesn't extend mainstream support	Refer #67

Response to the Pre-Bid Queries

18 92	Volume II	2.24 Procurement through Local Suppliers (Make in India)	<< General Query >>	Please provide exception for IBM Hardware (Power Systems) as POSB is already using Power Systems	Refer #68

Response to the Pre-Bid Queries

18 93	Volume II	C. Ongoing Support Services, Page 45	10. The incumbent vendor, HPE, is currently responsible for the Operations and Maintenance of certain common infrastructure and security solutions deployed at the existing DC/DR locations, which are shared between POSB and PLI. The SI shall work in conjunction with HPE to maintain the existing IT infrastructure and services specific to POSB till the new DCF is setup and operational, post which the SI shall be responsible for providing the same as mentioned in the RFP. The details of the common solutions are listed in Annexure B.	Please clarify this point. If PLI is not under scope of this RFP, then how the shared resources will be divided between POSB & PLI	Refer #69

Response to the Pre-Bid Queries

18 94	Volume II	5.2.4 Detailed Scope of Work, Page 82	22. The SI is required to follow the below matrix for installing the application instances in DC, DR and NDR environments within the infrastructure.	Please confirm the current availability of - Development/SIT/PREPROD of CBS Resources in DC - Training/PREPROD/UAT of CBS Resources in DR	Refer #70

Response to the Pre-Bid Queries

18 95	Volume II	Annexure L - RISC Server	Minimum one RISC processor module with 60 active compute cores, supporting simultaneous multithreading and hardware accelerators for encryption, compression, and isolation.	Please clarify if the server is asked with Single socket of 60 Cores or 60 Cores can be spread on multiple sockets but part of Single Unit/Module. Please change the word "hardware accelerators" with "hardware based capability for encryption & isolation"	Refer #71

Response to the Pre-Bid Queries

18 96	Volume II	Annexure L - Server Rack	42U - Rack should be 800mm (Width) x -1200mm (Depth).	Please change this criteria to include 600 mm or more as width as certain manufacturers build compact rack to optimize space requirements	Refer #72

Response to the Pre-Bid Queries

18 97	Volume II	Annexure L - Server Rack	The 19" mounting angles should be provided 2 Nos. on the front and rear sides of the Rack. It should be adjustable full depth. 19" Mounting Angles made up of Steel 2mm Thickness, with better mounting flexibility and maximises usable mounting space.	Please remove the Point - "It should be adjustable full depth."	Refer #73

Response to the Pre-Bid Queries

18 98	Volume II	Annexure L - Server Rack	Each rack should have a provision for a horizontal cable manager.	Please remove this point as cable managers are usually provided alongwith component being installed based on specifications	Refer #74

Response to the Pre-Bid Queries

18 99	Volume II	Annexure L - Server Rack	The Hexagonal Perforated Dual Rear Door will be Lockable, and a 3 Point Lock should be provided.	Please allow single Rear Door also with Lock & Key	Refer #75

Response to the Pre-Bid Queries

19 00	Volume II	Annexure L - Server Rack	Rack should be Castor wheels 4 Nos. (i.e. 2 front wheels with brake and 2 rear without brake) with adjustable levellers. The rack shall not have an External height >1991mm, including levelling legs and Castors.	Please allow External Hieght > 2050mm, wheels without brake (considering mechnism which restricts rack movement)	Refer #76

Response to the Pre-Bid Queries

19 01	Volume II	Annexure L - Server Rack	Minimum 2 × enterprise SSD (hot-plug) in RAID 1 or OEM-equivalent mirroring.	This point is contradictory with Point 5. Latest Generation Servers are equipped with NVMe Disks. Please delete this point as the requirement is fulfilled in Point 5 already	Refer #77

Response to the Pre-Bid Queries

19 02	Volume II	Annexure L - Server Rack	Integrated/optional RISC-compatible controller supporting RAID 0/1/5/6/10 or OEM equivalent.	NVMe protocol is PCI based protocol & doesn't support RAID, therefore change "RAID 0/1/5/6/10" to "OS Mirroring"	Refer #78

Response to the Pre-Bid Queries

19 03	Volume II	Annexure L - Server Rack	Server should have below security essentials and certificates: • shall include FIPS 140-2, TPM 2.0 v5 & UEFI with secure boot. • cryptographically verified trusted booting standards meeting basis NIST SP 800-147B, BIOS Integrity measurement proposed guidelines basis NIST SP 800-155, protection standards meeting NIST SP 800-193 and standards & secure media sanitization standards meeting NIST SP 800-88. • real time firmware security scanning to protect against firmware which executes before the OS boots. • maintain repository for firmware and should be able to rollback, if required. • configuration upgrades should be only with cryptographically signed firmware and software from the server OEM. • End-to-end supply chain controls to ensure component integrity, security, and vendor responsibility. • Secure Erase • Data at Rest Encryption (SEDs with local or external key mgmt) • Chassis Intrusion Detection • Server OEM Security bezel with lock function • CNSA • ASHRAE A3/A5	Please review these points as some of these points are either related to OEM Specific or Storage related like Data at Rest Encryption is storage term & chassis Intrusion Detection is more related to Blade/Chassis Servers. Please either delete this point or limit to standard RAS/security features like Quantum safe encryption etc.	Refer #79

Response to the Pre-Bid Queries

19 04	Volume II	Annexure L - Server Rack	Integrated service processor with remote console; local VGA/DP/HDMI as supported.	Please add local with RJ45 connectivity also	Refer #80

Response to the Pre-Bid Queries

19 05	Volume II	Annexure L - Server Rack	OEM need to submit latest and valid FCC Class A, Energy Star, CE Certification, OEM, BIS Certificate	Please allow some of them to be submitted incase any such is not valid for specific OEM/Country of Origin	Refer #81

Response to the Pre-Bid Queries

19 06	Volume II	Annexure L, Page #- 260, Tape Library	Enterprise-class, rack-mountable, LTO-9 or higher, SAN integration	Enterprise class library consist of Drives & Slots in a Frame based architecture rather than rack-mountable design. Also, LTO 10 is the latest drive available in the industry. Request you to kindly amend this clause as "Enterprise-class, Frame based library, LTO-10 or higher, SAN integration"	Refer #82

Response to the Pre-Bid Queries

19 07	Volume II	Annexure L, Page #- 260, Tape Library	Native read/write speeds as per LTO gen; Data Rate Matching	Data Rate matching (DRM) terminology is for specific OEM, We offer "Speed Matching" Technique to achieve the same functionality. Request you to kindly amend this clause as "Native read/write speeds as per LTO gen; Data Rate Matching/Speed Matching"	Refer #83

Response to the Pre-Bid Queries

19 08	Volume II	Annexure L, Page #- 260, Tape Library	High-availability robotic subsystem; dual accessor preferred	Enterprise class library benefits with Dual accessor/robotics in terms of High Availability as well as load sharing. Keeping it is as "preferred" encourage the bidder to quote with single accessor. Request to amend this clause as "High-availability and load sharing robotic subsystem with dual accessor and dual gripper on each accessor "	Refer #84

Response to the Pre-Bid Queries

19 09	Volume II	Annexure L, Page #- 260, SAN Storage	Storage solution should provide the native capability to replicate data of existing storage between DC, DR and NDC without using any additional Hardware and software.	As per the industry standard, Same family of Storage can replicate with each other or must require additional Hardware or software for the same. Request you to kindly amend this clause as "Storage solution should provide the capability to replicate data of existing storage between DC, DR and NDC. If any additional Hardware and software required to achieve this capabilities shall be included in the solution."	Refer #85

Response to the Pre-Bid Queries

19 10	Volume II	Annexure L, Page #- 260, SAN Storage	SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage without using external/3rd party hardware or Software.	Migration of data from existing storage to new storage would require to follow certain process and tools. Request you to kindly amend this clause as "SI should ensure easy integration into the current environment and provide an easy technique to migrate data from existing storage. ."	Refer #86

Response to the Pre-Bid Queries

19 11	Volume II	Annexure L, Page #- 260, SAN Storage	Storage must be scalable to at least double capacity without adding any additional controllers with the same set of drives and RAID.	Base Controller enclosure has certain number of NVMe drives that saturate the performance of a storage and increasing the number of drives beyond base Controller enclosure would not help in linear capacity and performance increment. Also, Storage solution support Scale-out design that anyways help to increase the capacity. and performance by adding additional pair of controllers. Request you to kindly amend this clause as "Storage must be scalable to at least double capacity by adding any additional controllers with the same set of drives and RAID. "	Refer #87

Response to the Pre-Bid Queries

19 12	Volume II	Annexure L, Page #- 260, SAN Storage	The storage solution should be supplied with a three-phase power supply connectivity.	Power supply configuration depends on the storage power consumption and configuration. Request you to kindly amend this clause as "The storage solution should be supplied with a single-phase or three-phase power supply connectivity. . "	Refer #88

Response to the Pre-Bid Queries

19 13	Volume II	Annexure L, Page #- 260, SAN Storage	The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture with cache across configured controllers.	Each drive has only 2 physical ports that can connect to 2 controllers only that can work in HA mode by mirroring the cache of between 2 controllers. Spreading cache across more than 2 controllers would require to do cache virtualisation that will lead to cache coherency and reduce the performance drastically along with increase in the complexity of solution. Request you to kindly amend this clause as "The Storage System should be the latest generation Enterprise Storage product providing enterprise-class data availability, end-to-end NVMe support, and supporting zero data loss 3-way DR replication. Proposed storage must be an active-active multicontroller, scale-up and scale-out architecture. "	Refer #89

Response to the Pre-Bid Queries

19 14	Volume II	Annexure L, Page #- 260, SAN Storage	The proposed Storage System should be Unified Storage (Block & File), capable of delivering 99.9999% uptime, with no single point of failure for active/passive components, supporting Block & File on a single platform with common management or redundant gateways.	We understand that the existing Storage is SAN storage which is meant for high performance. As per the best practice for core banking solution, SAN Storage is the preferred storage while for unstructure data for some other application can be storage on separate NAS/File storage. Keeping both SAN & NAS on same controller or stoarge would lead to no special benefit rather it lower the performance and increase complexity. Request you to kindly amend this clause as "The proposed Storage System should be SAN Storage, capable of delivering 99.9999% uptime, with no single point of failure for active/passive components"	Refer #90

Response to the Pre-Bid Queries

19 15	Volume II	Annexure L, Page #- 260, SAN Storage	Must support dual-port NVMe TLC SSDs (3.84TB / 7.68TB / 15.36TB) with mixing of drive sizes.	There are multiple type of NVMe drives available in like SLC, MLC, TLC, QLC with their own pros and cons in terms of performance and reliability. NVMe TLC has standard performance and Reliability as it supports 3-4K P/E Cycle while IBM invented their own NVMe drives (or Computational storage device) with leading chip manufacturer "Micron" that is know as FCM (FlashCore Module) that has P/E cycle of 15K i.e. ~5X better than traditional NVMe TLC drive with higher capacity of 9.6TB, 19.2TB & 38.4TB. Request you to kindly amend this clause as "Must support dual-port NVMe SSDs for not more than 40TB and mixing of drive sizes shall be possible."	Refer #91

Response to the Pre-Bid Queries

19 16	Volume II	Annexure L, Page #- 260, SAN Storage	Must support unified Block & File protocols (FC, iSCSI, NVMe-oF, NFS). In the absence of a native file, a redundant NAS gateway must be provided.	We understand that the existing Storage is SAN storage which is meant for high performance. As per the best practice for core banking solution, SAN Storage is the preferred storage while for unstructure data for some other application can be storage on separate NAS/File storage. Keeping both SAN & NAS on same controller or stoarge would lead to no special benefit rather it lower the performance and increase complexity. Request you to kindly amend this clause as "Must support SAN Block protocols (FC, iSCSI, NVMe-oF).	Refer #92

Response to the Pre-Bid Queries

19 17	Volume II	Annexure L, Page #- 260, SAN Storage	The proposed storage system must be configured with minimum 4 Controllers & cache sizes of 2TB at DC and DR and 256GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall dynamically support read and write i/o	As per the asked performance in Point no.1 i.e. 3 Lac scalable to 5 Lac can be easily maintained with Dual controller with all the consideration asked in the RFP in cost-effective way. Min. 4 controllers will increase the commercials as well as complexity to manage the same. Also, Cache for NDC site should be atleast 25% of DC that too DRAM as in industry SSD Cache or PMEM is also available which is not true cache rather just a standard Flash drive that act as Cache and not recommended for CBS or critical applications. Request you to kindly amend this clause as "The proposed storage system must be configured with minimum Dual Controllers & cache sizes of 2TB DRAM at DC and DR and 512GB at NDC (scalable up to 1TB), protected by vault /battery. Cache shall be mirrored across controllers, dynamically utilised for both read and write operations, protected against power failures, and must be adequate from Day One to meet performance requirements, with any future upgrades (hardware/software) provided at no additional cost. The entire cache/memory shall	Refer #93

Response to the Pre-Bid Queries

				dynamically support read and write i/o ".	

Response to the Pre-Bid Queries

19 18	Volume II	Annexure L, Page #- 260, SAN Storage	DC/DR: min 16x 32/64Gb FC ports, 16x 25GbE ports,. NDC: min 8x 32/64Gb FC, 8x 25GbE for ISCSI /NAS	We understand that the SAN Switch has been asked in the RFP which is meant for FC connectivity only and 25G iSCSI is not require in this case. Also, NAS shall not be the part of SAN Stoarge requirement as justified in above points. Request you to kindly amend this clause as "DC/DR: min 16x 32/64Gb FC port,. NDC: min 8x 32/64Gb FC.	Refer #94

Response to the Pre-Bid Queries

19 19	Volume II	Annexure L, Page #- 260, SAN Storage	Must support NVMe backend with PCIe drive connectivity.	Base Controller enclosure has certain number of NVMe drives that saturate the performance of a storage and increasing the number of drives beyond base Controller enclosure would not help in linear capacity and performance increment. Also, Storage solution support Scale-out design that anyways help to increase the capacity. and performance by adding additional pair of controllers. Request you to kindly amend this clause as Must support SAN backend connectivity.	Refer #95

Response to the Pre-Bid Queries

19 20	Volume II	Annexure L, Page #- 260, SAN Storage	Must support 10/25GbE connectivity for replication (native or external). Any extra HW must be bundled.	Recommend to use FCIP router for better reliability and faster data replication as it uses WAN Optimisation. Hence 10/25G ports are not required. Request you to kindly delete this clause.	Refer #96

Response to the Pre-Bid Queries

19 21	Volume II	Annexure L, Page #- 260, SAN Storage	Must integrate with VMware, Nutanix, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible).	Nutanix is a HCI appliance that uses internal disk of node to create SDS layer and don't use external storage. Request you to kindly amend this clause as Must integrate with VMware, Hyper-V, KVM, Containers, support plugins (VVol, VAAI, vRA, CSI, Ansible).	Refer #97

Response to the Pre-Bid Queries

19 22	Volume II	Annexure L, Page #- 260, X86 server	Intel Platinum/ AMD processor @ 2.0 GHz or higher 64 Cores in 2 Sockets	As per the current clause, AMD has an edge to quote any series of processor while Intel has to quote Platinum mandatorily which is not a level playing field. Request you to kindly amend this clause as Intel / AMD processor @ 2.0 GHz or higher 64 Cores in 2 Sockets	Refer #98

Response to the Pre-Bid Queries

19 23	Volume II	Annexure L, Page #- 260, X86 server	2 TB DDR5 RAM- Minimum 32 DDR5 DIMM slots RDIMMS 8TB Max, supporting speeds of min 4800MT/s	2TB RAM would require 8 x 256GB capacity per DIMM from Day 1 while the supply of 256GB is limited and commercial high and considering 64GB capacity per DIMM would consume all 32nos. of DIMM slots and would have no further scope of increment of RAM Capacity. Hence scalability is not possible. Request you to kindly amend this clause as 2 TB DDR5 RAM- Minimum 32 DDR5 DIMM slots RDIMMS, supporting speeds of min 4800MT/s	Refer #99

Response to the Pre-Bid Queries

19 24	Volume II	Annexure L, Page #- 260, X86 server	Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS doesn't work on Raid card and hence not applicable for SDS solution. Request you to kindly amend this clause as Integrated/PCIe 5.0 24Gb/s SAS Raid Controller with 8GB Cache supporting RAID 0, 1, 5, 6, 10, 50, 60 (Not applicable in case of SDS)	Refer #100

Response to the Pre-Bid Queries

19 25	Volume II	Annexure L, Page #- 260, X86 server	Dual Port 10/25 Gbps SFP+ SR ethernet adapter with minimum four SFP modules of 10Gbps and 25 Gbps each	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS require higher bandwidth. Request you to kindly amend this clause as Dual Port 10/25 Gbps SFP+ SR ethernet adapter with minimum four SFP modules of 10Gbps and 25 Gbps each (It should be Dual port of 100GbE in case of SDS Solution)	Refer #101

Response to the Pre-Bid Queries

19 26	Volume II	Annexure L, Page #- 260, X86 server	Dual port 64 Gbps Fiber Channel HBA	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and utilise internal drives only and hence not applicable for SDS solution. Request you to kindly amend this clause as Dual port 64 Gbps Fiber Channel HBA (Not applicable in case of SDS)	Refer #102

Response to the Pre-Bid Queries

19 27	Volume II	Annexure L, Page #- 260, X86 server	Integrated Graphics controller with at least 8MB of video frame buffer/ memory	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and utilise dedicated node of GPUs and hence not applicable for SDS solution. Request you to kindly amend this clause as Integrated Graphics controller with at least 8MB of video frame buffer/ memory (Not applicable in case of SDS)	Refer #103

Response to the Pre-Bid Queries

19 28	Volume II	Annexure L, Page #- 260, X86 server	• Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of NICs & system health	We understand that the entire solution also include SDS (Software defined storage) which will consume same x86 hardware and SDS doesn't work on Raid card as well as External storage and hence not applicable for SDS solution. Request you to kindly amend this clause as Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of NICs & system health (RAID management, external storage management not applicable for SDS solution)	Refer #104

Response to the Pre-Bid Queries

19 29	Volume II	Annexure L, Page #- 260, X86 server	The Offered server should have certification with latest OS version of Microsoft, VMWare, RHEL, UBUNTU and SUSE	We understand that the entire solution also include SDS (Software defined storage) and Virtualisation as well which will consume same x86 hardware and required these Host OS on either Bare metal or Virtualisation platform. Also, VMware is not OS rather its one type of Hypervisor layer. Request you to kindly amend this clause as The Offered server should have certification with latest OS version of Microsoft, RHEL, UBUNTU and SUSE as host OS in case of Bare metal OR Virtualisation platform.	Refer #105

Response to the Pre-Bid Queries

19 30	Volume II	Annexure L, Page #- 260, SAN Director	The switch should support Virtual SAN and inter VSAN routing for sharing resources across VSAN. Switch should be able to deliver line-rate routing between any ports in a system or fabric without the need for external routing appliances.	Are we referring Vmware vSAN (SDS) here as it will limit the participations . Please clarify.	Refer #106

Response to the Pre-Bid Queries

19 31	Volume II	Annexure L, Page #- 260, Backup Solution	Disk-based backup appliances, SAN/NAS, VTL; Support for multi-site storage targets.	Tape library has been asked in the solution and that make recommended Backup strategy as D2D2T and hence VTL is not required. Request you to kindly amend this clause as Disk-based backup appliances, SAN/NAS, ; Support for multi-site storage targets.	Refer #107

Response to the Pre-Bid Queries

19 32	Volume II	Annexure L, Page #- 260, Backup Solution		POSB is already using IBM Storage protect backup perpetual licenses and all the backup is currently in its own format on tapes. Having different Backup solution procurement will lead to migrate all the existing data to new backup solution and also make commercial impact by not utilising the existing licenses. Request to kindly ask for additional capacity for existing licenses to avoid any migration efforts and economical solution.	Refer #108

Response to the Pre-Bid Queries

19 33	Volume II	Annexure J EMS	EMS must support Server Automation and Patch Management	Please provide the expectations/ requirements for server automation.	Refer #109

Response to the Pre-Bid Queries

19 34	Volume II	Annexure J EMS	EMS must provide Centralised Log Management and a Unified Dashboard.	Our submission to please rephrase the clause as "EMS must provide Centralised Event Management and a Unified Event Dashboard."	Refer #110

Response to the Pre-Bid Queries

19 35	Volume II	Annexure J EMS	EMS OEM must be ISO 27034 certified; solution must have ISO 27001:2013 & ISO 9001 certification.	ISO27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. ISO 9001 certification validates an organization's ability to consistently provide quality products/services, meet customer needs, and adhere to regulations through a globally recognized Quality Management System (QMS) framework, enhancing efficiency, reducing errors, boosting customer confidence, and providing a competitive edge for businesses of any size or sector. However ISO 27034 is not OEM certifications as its provides only guidance to assist organizations in integrating security into the processes used for managing their applications. ISO27034 is applicable to in-house developed applications, applications acquired from third parties, and where the development or the operation of the application is outsourced.	Refer #111

Response to the Pre-Bid Queries

				Since this certification is for guidance only to assist the organisation who are running and managing the in house applications, they utilize the principles outlined within its broader security framework and offerings, particularly for application security management during their Software development Cycle (SDLC) but it's not mandatory for every OEM to certified their products under this certification. Our submission is to please rephrase this clause as : EMS OEM must have ISO 27001:2013 & ISO 9001 certification	

Response to the Pre-Bid Queries

19 36	Volume II	Annexure J EMS	EMS must support discovery mechanisms (Active Directory, DNS) and service discovery.	Our submission is to please rephrase the clause as "EMS should provide the ability to integrate with Active Directory and DNS and should provide the ability to monitor active directory as well."	Refer #112

Response to the Pre-Bid Queries

19 37	Volume II	Annexure J EMS	EMS must provide Runbook Automation, OOTB workflows (1000+), integration with CMDB, and intuitive workflow/dashboard creation.	While tools can provide OOTB workflows and also provide the capability to create new workflows; our submission is to remove the (1000+) as every customer environment is different and workflows should be designed and used as per the project requirement.	Refer #113

Response to the Pre-Bid Queries

19 38	Volume II	Annexure J EMS	EMS must integrate with external systems (CyberArk, Systems Monitoring, RSA, PostgreSQL, Kerberos), support debugging, and process automation libraries.	Please provide the details of the systems monitoring tool to integrate with. Also, please share/ provide the detailed requirements/ expectation regarding each of the integrations asked within the clause.	Refer #114

Response to the Pre-Bid Queries

19 39	Volume II	Annexure J EMS	NMS must support wireless discovery, SD-WAN monitoring, security system monitoring, and telemetry-based data collection.	Please provide share OEM, Make and Model or Wireless Lan Controller.	Refer #115

Response to the Pre-Bid Queries

19 40	Volume II	Annexure J EMS	NMS must support zero-touch automation via APIs, integration with NetDevOps (GitHub), and scheduled/ad-hoc scans.	Our submission is to please rephrase the clause as "NMS must support zero-touch automation via APIs/ scripts/ ansible playbooks, integration with NetDevOps (GitHub), and scheduled/ad-hoc scans." Please elaborate the requirement with a use case for integration with NetDevOps (Github).	Refer #116

Response to the Pre-Bid Queries

19 41	Volume II	4 Current System Overview	Card Management System	Is there 3rd party product being used for Card Issuance and Management? If yes, please provide the details.	Card Management System is not in scope. Selected Bidder has to ensure integration with the solution.

Response to the Pre-Bid Queries

19 42	Volume II	4 Current System Overview	ATM Switch	Is there 3rd party product being used for ATM Switch and Management? If yes, please provide the details	ATM switch is not in scope. Selected Bidder has to ensure integration with the solution.

Response to the Pre-Bid Queries

19 43	Volume II	4 Current System Overview	CTS	Is there 3rd party product being used for CTS and Management? If yes, please provide the details	Kindly Refer Table 6 (Volume 2).

Response to the Pre-Bid Queries

19 44	Volume II	5.1.3	Upgrade of Finacle CBS and Alert Solution	As part of the upgrade, are there any payments specific enhancements required to be incorporated?	Bidder to propose

Response to the Pre-Bid Queries

19 45	Volume II	5.1.3	Integration and migration of all existing channels, including Connect 24, onto the upgraded version. Porting and fine-tuning of all existing customisations, including custom menus, API communications, and external integrations, to ensure full functional compatibility with the upgraded version.	It has been assumed that the existing payment integration end points to be migrated to the upgraded version. No new integration end points are required to be built. Is this correct?	As per RFP

Response to the Pre-Bid Queries

19 46	Volume II	viii. Interfaces and Integrations Management Services	SI shall manage, maintain and support all existing interfaces taken over from existing vendors and any new interfaces that may come up during the term of the contract for the smooth running of systems. The indicative list of such applications/ Solution components and interfaces with the CBS and allied applications is provided in the RFP	From payments processing standpoint, the interfaces (i.e. internal IT systems of DoP) involved in payments processing - NEFT/RTGS/NACH/CTS / Cards - are these existing integrations?	As per RFP

Response to the Pre-Bid Queries

19 47	Volume II	viii. Interfaces and Integrations Management Services	SI shall manage, maintain and support all existing interfaces taken over from existing vendors and any new interfaces that may come up during the term of the contract for the smooth running of systems. The indicative list of such applications/ Solution components and interfaces with the CBS and allied applications is provided in the RFP	It has been assumed that the maintenance or changes to the internal IT systems of DoP are out of scope. Is this correct understanding?	As per RFP

Response to the Pre-Bid Queries

19 48	Volume II	Page 36	Any interface required as per Regulatory and statutory requirements (RBI, SEBI, IBA, FIU, MoF, DoP, UIDAI, Government of India, etc) from time to time shall be provided by SI at no additional cost to DoP. The SI shall also be responsible for maintaining these interfaces throughout the contract period.	Please provide example any such requirements in the past where additional interfaces were needed? It is difficult to quantify the amount of change or number of interfaces required for the unforeseen regulatory requirements.	As per RFP

Response to the Pre-Bid Queries

19 49	Volume II				As per RFP

Response to the Pre-Bid Queries

19 50	Volume II	5.1.3	Upgrade of Finacle CBS and Alert Solution	As we understand Finacle is being used to process the payments NEFT/RTGS/NACH/CTS / Cards - are there any separate applications or services being used to message transformation, enrichment, last mile integration etc..? If yes please provide the details.	NEFT/RTGS integrated with IPPB SFMS, CTS application provided by Oritso vendor integrated with Finacle, CMS provided by YSP vendor has been integrated with CBS.

Response to the Pre-Bid Queries

19 51	Volume II	Page 39	Reports - The SI shall develop, customise, and deliver reports as required by DoP, i	Can you provide volume and complexity of reports - daily, adhoc, weekly, monthly, annual etc.	Approx 40 to 50 reports as per Banking Industry Standard including but not limited to: - CBS availability - Transaction Volume Trends - Batch Processing Status - Reconciliation Reports - Channel wise usage (IB/MB/Branch, etc.) - Customer Onboarding metrics - Failed Transaction Analysis, etc.

Response to the Pre-Bid Queries

19 52	Volume II	Page 39	Reports - The SI shall be responsible for ensuring the seamless, accurate, and timely flow of all POSB-related data from the respective source systems into the DoP Data Lake/Data Mart environment.	Any changes to the DoP Data Lake/Data Mart environment are in scope of this engagement?	Data lake house setup is not in scope. Bidder shall integrate with DoP implemented central data lakehouse.

Response to the Pre-Bid Queries

19 53	Volume II	5.1.3	Upgrade of Finacle CBS and Alert Solution	Is there any separate payment engine or system or Finacle Payments Capabilities are being used for this purpose?	As per RFP

Response to the Pre-Bid Queries

19 54	Volume II	Page 42 5.1.4.5	Operations and Maintenance Support for the Centralised Cheque Clearing System (CTS)	Please can you share the existing team size of CTS vendor supporting the work?	As per RFP

Response to the Pre-Bid Queries

19 55	Volume II	5.2.5.2 FINnet 2.0	Deploying, integrating and supporting the FINnet 2.0 reporting solution as mandated by the Financial Intelligence Unit – India (FIU-IND), ensuring timely, secure, automated 105 Selection of System Integrator (SI) for Post Office Savings Bank (POSB) under IT Modernization Project – DoP IT 2.0 Volume 2: Scope of Work submission of all prescribed regulatory reports and full alignment with current and future FIU guidelines	It has been assumed that DOP will provide the specifications or requirements related to FINNET 2.0 solution.? Is this correct?	As per RFP

Response to the Pre-Bid Queries

19 56	Volume II	5.2.5.2 FINnet 2.0	Deploying, integrating and supporting the FINnet 2.0 reporting solution as mandated by the Financial Intelligence Unit – India (FIU-IND), ensuring timely, secure, automated 105 Selection of System Integrator (SI) for Post Office Savings Bank (POSB) under IT Modernization Project – DoP IT 2.0 Volume 2: Scope of Work submission of all prescribed regulatory reports and full alignment with current and future FIU guidelines	The reports mentioned in the sections are existing reports (e.g. CTR, STR, CCR etc.) or to be generated as new?	Reports are generated manually in the current system. Bidder to propose as per RFP requirements.

Response to the Pre-Bid Queries

19 57		5.2.5.5	Aadhar Enabled Payment System (AePS) The SI shall be responsible for integrating the Aadhaar Enabled Payment System (AEPS) with the existing Core Banking Solution and allied banking infrastructure of DoP, to enhance the delivery of Aadhaar-based financial services.	It has been assumed that AePS integration is required with upgraded Finacle platform, is this correct?	As per RFP

Response to the Pre-Bid Queries

19 58		5.2.5.7 IMPS	Develop a robust, scalable IMPS application encompassing all functionalities specified in the FRS, such as fund transfer, beneficiary management, transaction status tracking, and dispute handling.	Does the IMPS development required as a separate payment system from scratch or it would be embedded and enhance as part of Finacle product? Does IMPS supported today in DOP? If Yes, please share the details of the existing IMPS system.	Bidder to propose. IMPS is not implemented currently.

Response to the Pre-Bid Queries

19 59		5.2.5.8	Two-Factor Authentication to log in to the Core Banking System (Finacle) via Biometric/OTP.	It has been assumed that this requirement is for Internal DOP Users only. Is this correct?	As per RFP

Response to the Pre-Bid Queries

19 60		5.2.5.10	Middleware	Is there any existing Middleware being used for payments processing?	POSB is not using any Middleware

Response to the Pre-Bid Queries

19 61		5.4.1	Development of Comprehensive Learning Materials	Is there any existing repository of the training material which can be reused?	Relevant SOPs and operational documents are prepared and updated periodically in line with system changes. These documents may be shared with the selected bidder for reference and knowledge transfer purposes.

Response to the Pre-Bid Queries

19 62		General	Application development	Please highlight the reusability possibility for Mobile Banking, CTS, Cards,	Bidder to propose.

Response to the Pre-Bid Queries

19 63	Volume II	4 Current System Overview	Card Management System	Is there 3rd party product being used for Card Issuance and Management? If yes, please provide the details.	Card Management System is not in scope. Selected Bidder has to integrate it with the solution.

Response to the Pre-Bid Queries

19 64	Volume II	General	general	Please share existing system or business architecture for better understanding across multiple tracks like Payments, Fraud, KYC etc	As per RFP

Response to the Pre-Bid Queries

19 65	Volume I	Page 37	Bidder's Credential Strength - Banking (Max Marks: 14) A1. Core Banking Solution Note: If the Bidder submits any project citation(s) for Finacle CBS, an additional score of 1 mark shall be awarded.	The core of this RFP is selection of a partner who can confidently takeover the CBS and allied applications and operate it seamlessly offering an upgrade to the Finacle CBS within the first year. Owing to the criticality of the core banking system we request DOP to consider additional 6 marks instead of 1 mark for any bidder with multiple <u>citations on Finacle CBS within India</u> (Indian banking ecosystem is different from CBS deployments in rest of the world). Hence enhancing the weightage of Bidder's Credential Strength in Banking to at least 20 marks instead of 14 marks as present.	As per RFP

Response to the Pre-Bid Queries

19 66	Annexure L- Container Management Platforms	Point No 6	The Container Platform shall support deployment and orchestration of multiple container formats (docker, cri-o etc) for preventing any technology lock in.	This point is proprietary and specific to an particular OEM bundle offering. Request to modify this point. We also observed that containerd which is another CNCF project is not included. Kindly re-write the statement as: The Container Platform shall support deployment and orchestration of multiple container formats (docker, containerd, cri/ cri-o etc) for preventing any technology lock in.	The clause is revised as: "The Container Platform shall support deployment and orchestration of multiple container runtimes and formats (including at least Docker-compatible, containerd/CRI/CRI-O) for preventing any technology lock-in."

Response to the Pre-Bid Queries

19 67	Annexure L- Container Management Platforms	Point No 8	The Container Platform shall have inbuilt automated application container build capability – from source code to a runnable container image.	This point is proprietary and specific to an particular OEM bundle offering. Request to modify this point. Kindly re-write the statement as: The Container Platform shall allow integration with CNCF certified for automated application container build capability – from source code to a runnable container image.	The clause is revised as: "The Container Platform shall allow integration with CNCF certified for automated application container build capability – from source code to a runnable container image."

Response to the Pre-Bid Queries

19 68	Annexure L- Container Management Platforms	Point No 10	The container platform should be one that provides a developer portal, plugins, middleware and inbuilt integrated IDE for developers to easily work on the same container platform to bring consistence and faster application lifecycle.	IDE, middleware are not related to container platform and must be asked separately. This is proprietary and specific to an particular OEM bundle offering. Request to delete this point. It also restricts other leading OEMs including VMware to participate in this tender due to such proprietary points.	Refer #25

Response to the Pre-Bid Queries

19 69	Annexure L- Container Management Platforms	Point No 11	The container platform should provide inbuilt (enterprise supported) capabilities such as inbuilt application Catalog (Spring, Node.js) etc AI/ML, Serverless, Kubernetes native CI/CD capabilities etc.	This point is proprietary and specific to an particular OEM bundle offering. Request to modify this point. Kindly re-write the statement as: The container platform should support (enterprise supported) capabilities such as application Catalog (Spring, Node.js) etc AI/ML, Serverless, Kubernetes native CI/CD capabilities etc.	The intent is that the platform can offer, expose or integrate with an enterprise-supported catalog of common application frameworks, and support AI/ML, serverless and K8s-native CI/CD use cases. It is not mandatory that every one of these capabilities is “hard-wired” into the core product. Therefore, the clause is revised as: “The container platform should provide or support (with enterprise support) capabilities such as application catalogs (for common frameworks like Spring, Node.js etc.), and should enable AI/ML, serverless and Kubernetes-native CI/CD use cases through native features or integrated components supplied as part of the solution.

Response to the Pre-Bid Queries

19 70	Annexure L- Container Management Platforms	Point No 13	The container platform should have a cluster manager with key features such as application management and application monitoring dashboard, policy-based governance and cluster lifecycle management. It must provide capability to provide direct networking between Pods in different Kubernetes clusters and Service Discovery, either on-premises or in the cloud.	This point is proprietary and specific to an particular OEM bundle offering. Request to modify this point. Kindly re-write the statement as: The container platform should have a cluster manager with key features such as application management and application monitoring dashboard, policy-based governance and cluster lifecycle management. It must provide capability to provide direct networking between Pods in different Kubernetes clusters and Service Discovery, either on-premises or in the cloud.	As per RFP

Response to the Pre-Bid Queries

19 71	Annexure L- Container Management Platforms	Point No 23	The Container Platform should offer a suitable IDE for developing container-based applications.	This is proprietary and specific to an particular OEM bundle offering. Request to delete this point. It also restricts other leading OEMs including VMware to participate in this tender due to such proprietary points.	The clause is revised as: “The solution should provide tooling and integrations (e.g., plugins, extensions, or CLIs) that allow developers to use popular IDEs and development tools for building and deploying container-based applications on the platform.”

Response to the Pre-Bid Queries

19 72	Annexure L- Virtualization	Point No 15	The solution should integrate with various authentication providers: HTPasswd, Keystone, LDAP v3, Active Directory, OpenLDAP, Request Header, Github, Google, OpenID Connect, GitLab.	This point is propriety and specific to an particular OEM bundle offering. Request to modify this point. Kindly re-write the statement as: The solution should integrate with various authentication providers (minimum 3): HTPasswd, Keystone, LDAP v3, Active Directory, OpenLDAP, Request Header, Github, Google, OpenID Connect, GitLab.	The revised clause to be read as : "The solution should integrate with at least three of the following authentication providers: HTPasswd, Keystone, LDAP v3, Active Directory, OpenLDAP, Request Header, GitHub, Google, OpenID Connect, and GitLab." Bidders may refer to Corrigendum Annexure L for updated details of the requirements.

Response to the Pre-Bid Queries

19 73	Volume II, Page 23	General	Figure II : Scoped Items this RFP have different dates for AMC/ATS and manpower validity by existing partners	Kindly clarify the existing scoped item shall be maintained by existing vendor for atleast 4 months (Knowledge aquisition + handholding/shadow support + acceptable exit documentation) so that bidder can takeover a seamless transition.	Refer #554

Response to the Pre-Bid Queries

19 74	Volume II, Page 23	General	Figure II : Scoped Items this RFP have different dates for AMC/ATS and manpower validity by existing partners	Scoped Items which have different dates for support end for both product+support, should be maintained via existing contract with DoP if the bidder has a plan to replace the solution with a better proposition, for which bidder shall propose a plan for replacing the existing application with the new one and till the date proposed for replacement existing DOP partner support shall be enabled. This is to avoid any kind of monopoly or cost arbitrage which may arise by the existing OEMs, hence leading to a healthy competition within the BFSI ecosystem towards a fair price evaluation.	Bidder to propose

Response to the Pre-Bid Queries

19 75	Volume II, Page 211	General	Bill of Quantity (Annexure A)	1. Kindly clarify the existing "application sizing" which is spread across the compute layer across AIX/non-AIX for the bidder to propose an effective migration plan. In absence of application sizing bidder shall remain unaware of any deficit which may have to be planned for fulfillment for takeover/upgrade/lift&shift 2. Kindly also offer the Serial No. of all the assets for bidders to inspect its current and probable support available to cover the entire duration of the project accurately. 3. Kindly confirm if enough compute is available for performing the upgrade of the CBS and requisite functions, and any hardware requisite during the time of upgrade shall be taken care by DOP. Bidder shall factor additional hardware for new and deficit after migration/left&shift for new developments/applications and enhancements to existing apps respectively.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

19 76	Volume III	Pg 15/16 Section 1.5.5	Liquidated damages will be capped at 10% of the Total Contract Value (TCV)	Liquidated damages / <u>SLA Penalty</u> will be capped at 5% of the Quartely value .	Bidders may refer to the Corrigendum for updated details.

Response to the Pre-Bid Queries

19 77	Volume II	Pg 174/ se-6.10.1	SLAs for conducting DR Drills	SLA for conducting DR Drills should be part of Overall LD/SLA penalty cap of 5% of Quartely Invoice value. conducting DR Drills- 1.0% of Total Quartely Invoice value per week of delay . Submission of DR Drill Report -0.5% of Total quartely value, per week of delay	As per RFP

Response to the Pre-Bid Queries

19 78		AMC/ATS	1. Please help to share the complete Inventory details covering below basic information which needs to be covered under AMC (Annual Maintenance Contract) Ø Machine Serial Number Ø Make/OEM Name Ø Complete Model details with Configuration Ø Asset wise Current AMC/Warranty support end dates Ø Asset wise Address Details with Pin codes Ø Support Model- Need OEM Back-to-Back Support or Non-OEM support Ø Asset wise SLA Ø Provide CSI number if any inventory of Oracle is part of Contract Ø Need License ID or Subscription ID if any ATS (License Support) is part of contract Ø For CISCO Devices- Need assets wise SLA confirmation (Smartnet SLA or Partner Support SLA) and Support Window confirmation (8x5xNBD or 24x7x4) 2. Contract Period- AMC Start Date and End Date 3. Complete Scope of Work to be covered as part of AMC 4. Payment Term for AMC component	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

19 79	Volume II, Page no 35	General	vii. Database Administration	Please share the count of each database flavour, including versions, instance counts, cluster details, and environment split (Prod/Dev/UAT/DR). Please include cloud-wise and on-premise distribution.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

19 80	Volume II, Page no 35	General	vii. Database Administration	Please share the EOL/EOS database server details, if any. Please confirm the YoY growth in databases.	Bidders may refer to the Corrigendum for additional details.

Response to the Pre-Bid Queries

19 81	Volume II, Page no 35	General	vii. Database Administration	What monitoring tools are used for managing different database flavours? Please share the current patching process. Is the patching automated for each and every flavors of Database? Please specify the database patching tools used.	No tools are used. Patching process is manual.

Response to the Pre-Bid Queries

19 82	Volume II, Page no 116	General	6. Security, Scalability, and Performance	Please confirm data warehouses, and big data platforms, including Exadata, Teradata, Hadoop, MongoDB is part of the scope . if Yes , Please share the detail inventory (Teradata, Hadoop, MongoDB instances) ,	Data lake house/warehouse setup is not in scope. Bidder shall integrate with DoP implemented central data lakehouse.

Response to the Pre-Bid Queries

19 83	Volume II, Page no 116	General	6. Security, Scalability, and Performance	Please provide details of Exadata and ExEaCC servers, including versions.and count . Also confirm is the Exadata DMA support, Exadata Patching and admin=stration is part of scope or only the database on the Exadata is part of scope .	As per RFP

Response to the Pre-Bid Queries

19 84	II	Annexure L, X86-Based Hypervisor, Clause No. 19	Support SAN and IP-based storage for shared datastore access.	To provide more options, please rephrase the clause to "Support SAN and IP- based storage for shared datastore / storage class access."	Refer #681

Response to the Pre-Bid Queries

19 85	II	Annexure L, X86-Based Hypervisor, Clause No. 28	Continuous availability using live shadow VMs for fault tolerance.	To provide more options, please rephrase the clause to "Support high availability for virtual machines through automatic recovery on node failure."	Refer #682

Response to the Pre-Bid Queries

19 86	II	Annexure L, Virtualization, Clause No. 18	The solution should support live VM migration over long distances (up to 150 milliseconds round trip time) without disruption.	To provide more options, please rephrase the clause to "The solution should support VM migration over long distances with low network latency"	Refer #683

Response to the Pre-Bid Queries

19 87	II	Annexure L, Virtualization, Clause No. 18	The solution should create a cluster out of multiple storage datastores and automate load balancing using storage characteristics.	To provide more options, please rephrase the clause to "The solution should provide policy-based storage provisioning for virtual machine workloads by supporting multiple storage providers"	Refer #684

Response to the Pre-Bid Queries

19 88	II	Annexure L	X86-Based Hypervisor	Since in same Annexure L there is already a Virtualization technical spceifications section so the technical spceifications section on Hypervisor should be removed.	Refer #685

Response to the Pre-Bid Queries

19 89	II	Annexure J, Middleware, Clause No . 4	Cross-language client SDKs with support for programming languages including but not limited to Java, C, C++, C#, Ruby, Perl, Python, PHP, and VB6.	VB6 is now legacy. Request you to please remove the same. The STOMP protocol provides this connectivity without a propriety adapter. Request to please remove VB6.	Refer #8

Response to the Pre-Bid Queries

19 90	II	Annexure J, Middleware, Clause No . 5	Support for multiple messaging protocols including OpenWire, STOMP, AMQP, MQTT, and JMS.	The OpenWire protocol is considered deprecated in modern enterprise messaging platforms.	Refer #9

Response to the Pre-Bid Queries

19 91	II	Annexure J, Middleware, Clause No . 8	Support for pluggable transport protocols such as In-VM, TCP, SSL, NIO, UDP, multicast, JGroups, and JXTA.	The in-VM protocols is considered legacy architectural patterns for modern, cloud-native deployments. Request to pelase remove this. JXTA is a legacy peer to peer protocol which industry moved away from the past 10-15 years. Modern peer to peer is handled now via JGroups now. Request to please remove the same.	Refer #10

Response to the Pre-Bid Queries

19 92	II	Annexure J, Middleware, Clause No . 10	Appliance-based deployment options should be supported.	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	Refer #689

Response to the Pre-Bid Queries

19 93	II	Annexure J, Middleware, Clause No . 15	Support for message groups, virtual destinations, wildcards, and composite destinations.	VirtualDestinations element is now legacy and the same is acheived through Addresses, Queues, and Routing. Composite Destination can also be acheived using multicast Addresses.	Refer #690

Response to the Pre-Bid Queries

19 94	II	Annexure J, Middleware, Clause No . 22	Compliance and support for BOLA (Broken Object Level Authorization) mitigation and adherence to OWASP Top 10 security testing.	While middleware technologies provide native security capabilities, external security and native-kubernetes networking protocols etc help acheive this requirement. Request to please remove the same as it will not be catered by middleware directly.	Refer #691

Response to the Pre-Bid Queries

19 95	II	Annexure J, Middleware, Clause No . 29	Solution should support deployment flexibility including appliance, container, and Kubernetes environments.	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	Refer #692

Response to the Pre-Bid Queries

19 96	II	Annexure J, Middleware, Clause No . 39	The ESB should offer integrated support for IBM MQ Server on the same hardware as a single unit-of-work transaction.	Request to pelase remove this point as it opints to a specific vendor.	Refer #693

Response to the Pre-Bid Queries

19 97	II	Annexure J, Middleware, Clause No . 40	The ESB shall allow integration with multiple programming environments, including Java, .NET (C#, VB, F#, etc.), PHP, ESQL, and C++.	Request to please remove ESQL for larger participation. Apache Camel is the standard defacto open source standard offering more flexibility compared to vendor locked ESQL.	Refer #11

Response to the Pre-Bid Queries

19 98	II	Annexure J, Middleware, Clause No . 65	Platform should contain client development kit available for all the programing languages including VB6	VB6 is now legacy. Request you to please remove the same. The STOMP protocol provides this connectivity without a propriety adapter. Request to pleae remove VB6.	Refer #695

Response to the Pre-Bid Queries

19 99	II	Annexure J, Middleware, Clause No . 66	Platform should support appliance based deployment options	Containerized middleware gives the flexibility for scaling, resource optimization, high-availability, self-healing capabilities, portability etc. Request to please remove or rephrase to the middleware technology should be platform agnostic i.e. provides flexibility to be installed on any platform.	Refer #696

Response to the Pre-Bid Queries

20 00	II	Annexure J, Middleware, Clause No . 78	Maven based repository for OSGi modules and plugins	Apache Camel, the defacto open-source standard for ESB now does not mandate the complexity of OSGI at runtime. Camel technologies can now run on Kubernetes as lightweight, immutable containers.	Refer #697

Signature Not Verified

Digitally signed by AJAY KUMAR
Date: 2026.03.10 15:37:09 IST
Location: eProcure-EPROC

