RESPONSE TO QUERIES SET 1 OF NISG RFP NISG/SLUDI-2025

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
1	Volume-2	5	19	The MSI shall provide a detailed cutover plan before migrating from the legacy system and a roll out plan. Upon providing the plans the approval must be taken from GoSL.	As discussed with NISG, there will be no migration of existing data. The MSI is only required to integrate the SL-UDI with the current system to retrieve pre-existing citizen information from the existing database. Kindly confirm..		Yes the understanding is correct
2	Volume-2	5.2.1.1	49	The MSI should augment a fiber-based connectivity for data replication between the two sites, if required. The MSI shall undertake a capacity assessment and undertake capacity augmentation to meet the required requirement and performance levels mentioned in the RFP.	As discussed with NISG, all link-related activities will be managed by the MSP, not the MSI. Accordingly, connectivity between the DC and DR, along with uptime requirements, will be handled by GoSL or the MSP. Kindly confirm.		Yes the understanding is correct
3	Volume-2	5.2.1.1 (iii)	49	Should provide Access cards, Gate passes to the GoSL personnel / GoSL appointed system integrators as and when they require visit the site. (Such access should be provided 24 X 7 and will not have any time restriction).	As discussed with NISG, GoSL will engage a co-location service provider to host the DC & DR services. Therefore, all physical access to the Data Centre will be managed by GoSL, with necessary coordination from the MSI.		Yes the understanding is correct
4	Volume-2	5.2.1.1 (iv)	49	Should regularly monitor the access to the provided space (cage with necessary physical security) by means of access control system, physical security, biometric access, and CCTV (Closed-circuit television) and should always make sure that they are functional 24X7 days.	Since the DC will be hosted at the GoSL-designated co-location service provider, all physical security responsibilities should rest with the service provider and not with the MSI.		Yes the understanding is correct
5	Volume-2	5.2.6	55	**Partner Network** The first TSP will be implemented by MSI where segregation of networks should be implemented.	Since GoSL will manage the links and the service provider, these responsibilities should be assigned to the MSP rather than the MSI.		Appropriate modifcation has been made in the relevant clasue.
6	Volume-2	5.2.6	55	**SL-UDI Wide Area Network** MSI will be required to provide secure and reliable connectivity.	As GoSL will be taking care of the links then it should be removed from the scope of MSI.		GoSL shall provide the connectivty
7	Volume-2	5.2.6	56	**Internet Connectivity** MSI will be required to provide secure and reliable internet dongles for connectivity of mobile registration centers with the DC and DR.	As GoSL will be taking care of the links then it should be removed from the scope of MSI.		Yes this is not a part of MSI scope
8	Volume-2	5.3.1	61	It is required to facilitate Mobile Kits with including the KIT items. **Internet Dongle**	As GoSL/MSP will be responsible for managing the links, the Internet dongle should fall under the MSP's scope, as they will benefit from the associated cost advantages.		Answer is as given in Sr no 7
9	Volume-2	5.8.2.2	87	**Data Backup Strategy** Tapes shall be moved by MSI to offsite location on Daily basis at a geographically separate location with appropriate physical security controls, at par with banking regulator of Sri Lanka for such secure transfer, arranged by MSI.	This clause should be removed, and the responsibility should be mapped under the scope of GoSL.		The storage and movement of tapes shall be the responsibility of GoSl . Hoever backup activity shall be the responsibility of MSI.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
10	Volume-2	5.8.2.3	89	**HSM Recovery** MSI shall ensure HSM encryption keys (signing, encryption keys and master keys) are replicated to the High Availability HSM cluster and backed up every time a new key pair is generated, and the keys are stored securely in HSM.	As the RFP BOQ does not specify the required quantity of HSMs, please confirm whether two HSMs are needed at the DC and two at the DR, or if one HSM per location will suffice.		Refer to response to querry 464
11	Volume-2	5.8.2.3	89	In the event of a catastrophe, such as a flood or fire, it might lose both your working HSMs and locally stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote location.	It has mentioned Locally stored backup, please clarify what does locally stored backup means.		Remote means location other than DC and this will be the responsibility of GoSL Localy stored backup means local backup copies kept at DC or DR location.
12	Volume-2	5.8.2.3	89	Offsite location (other than DC and DR) in fireproof safe. Offsite location (other than DC and DR) in biometric enabled locker with dual access control.	To store the keys in offsite location has be taken care by GoSl itself it should be removed from MSI scope.		Yes, removed from MSI scope , but the copy of backup shall be provided by MSI to GoSL
13	Volume-2	5.8.2.4	89	MSI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible.	What excatly is mean to Data Center staff? Please clarify.		The requirement is self expalnatory
14	Volume-2	5.8.2.4	89	Key staff to run the operations from locations designated by GoSL, if data center site is physically inaccessible.	What excatly is mean to key staff along with what type of VPN require Site to Site or RAVPN? Please confirm.		The requirement is self expalnatory
15	Volume-2	5.8.4.1	97	GoSL will be required to provide necessary IT (Hardware, Software, Network) and Non- IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialer, Telephones, Headsets, etc.).	As per the the clause Contact center equipment will be provided by GoSL, requesting GoSL to include Voice Gateway as well.		Requirment of Voice gateway is dropped. MSI to provide required PBX and IP Phones.
16	Volume-2			General Query	Please share the location of the NOC, SOC and IT-Helpdesk.		Location will be shared later with the successful bidder.
17	Volume-2			General Query	As per the asked BOQ for NOC L3 device is missing then who will perform the routing. Please include and share the technical specification as well if L3 device is not present there same with IT-Helpdesk location as well.		Bidder to call and propose L3 device if required.
18	Volume-2	5.9.1.1	107	An indicative manpower for SOC is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of manpower required: (i) Analysts – 2 (ii) Technical Manager – 1 (iii) Supervisor - 1 (iv) Total - 4	Please confirm whether the total number mentioned in the clause is calculated per shift. If it is per shift, then the requirement appears higher, and typically a Supervisor is required only during the general shift.		The numbers provided in the RFP as indicative reqt/per shift. Bidder needs to assess the required number of staff and propose.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
19	Volume-2	5.9.1.1	107	An indicative bill of material for SOC related items is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of components required: 1. Video wall with controllers, speakers, and other accessories 2. LED TV 3. Laptop 4. Desktops / Monitors 5. Keyboards and Mouse 6. IP Phone 7. IP PABX 8. Printer (Network) 9. UPS – 20KVA	As per the asked BOQ for SOC L3 device is missing who will perform the routing. Please include and share the technical specification as well.		Please see answer in Sl No 17
20	Volume-2	7	156	General Query	As per the BOQ bifurcation of the component is not mentioned, please clarify bidder need to consider qty as per the best of solution or not? Additionally, certain BOQ line items specify quantities—for example, 32 blade servers are mentioned in the RFP. Please confirm whether we need to consider all 32 units at each location (DC and DR), or 16 units per location.		The quantity may be read as NIL. However the sizing and the form factor has to be done by MSI according to its solution requiremnt .
21	Volume-2			General Query	Please share the locations of the DC and DR, along with the distance between them. Additionally, kindly provide the maximum rack capacity that the MSI can be allocated, along with the maximum supported power load for both the DC and DR.		Location will be shared later with the successful bidder. Distance between the DC and DR is 20 Km(approx.). Refer to answer 512 for more details.
22	Annexure 12	12.1	3	**DRP Regional Offices:** Kurunegala Galle Vavunia Batticaloa Nuwara Eliya	Please confirm whether these sites will be connected to both the DC and DR over MPLS. If MPLS connectivity to the DC and DR is required, then routers/L3 device supporting the BGP routing protocol should be present at mentioned sites.		Yes this will be connected over MPLS but a dedicated pipe will be provided by GoSL.Any device required for backup and replication has to be provided by MIS
23	Volume-2			General Query	If the bidder can deliver a fully RFP-compliant solution using fewer equipment than specified in the RFP, will GoSL still permit such a solution? Kindly confirm.		Please configure the solution as per FR, NFR, Performance and SLA asked in the RFP and position BoQ accordingly
24	Annexure-10			General Query	As Annexure-10 does not provide a bifurcation of DC and DR manpower, our understanding is that the same NOC and SOC teams will manage both DC and DR operations. Please confirm if this understanding is correct.		NOC and SOC will me masnaged by MSI.Please refer to answer at Sr. No 18
25				General Query	As per discussion with NISG some Nos of Biometric scanner has already been procured by GoSL last year kindly share the count, Make, Model and their validity.		Already answered in S.No. 663
26	Annexure-3	3.6.2.4		General Query	As per BOQ rack has been asked but specification is not there, kindly share the Rack specification.		Racks are to be provided by MSI as per specifcatios and OEMs as per magic quadrant of Gartner

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
27	Annexure-16	1.1 RACI Matrix	3	12. Data Centre Hosting Space, Physical Infrastructure (entire non-IT), non-DC space for contact centre & helpdesk, bandwidth	Please confirm bandwidth, Data Centre Hosting Space, Physical Infrastructure (entire non-IT), non-DC space for contact centre & helpdesk will be provided by GoSL. Kindly note that there is discrepancy between Annexure-16 1.1 RACI Matrix (Point#12). PageNo.3 and Page#12 Annexure 16 1.1 Point#5. Please check various annexures as there are discrepancies on provision of bandwidth and data centre hosting space.		Yes your understanding is correct. Bandwidth sizing and its calculation has to be provided by MSI in its proposal.
28	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	Software Solution Section 5.1	24	Indicative COTS Components (Section 5.1.3) [GoSL shall provide the list of COTS products to be integrated with SL-UDI system] MSI shall be responsible for integration and customization of following COTS applications: • Business Intelligence and Data Analytics • Customer Relationship Management • Document Management System • Identity and Access Management • Knowledge Management Solution • Learning Management Solution • Fraud Management Solution	Please confirm final the list of COTS products to be considered for SL UDI Project. If we have to use existing COTS product purchased by ICTA/GoSL then the same should be supported products for the duration of the project. Plesae confirm the list of such products with Name of OEM and support status. Please confirm back to back (AMC/ATC) support shall be provided by GoSL/ICTA. As discussed during SL Visit, we understand Datawarehouse is not required but BI Analytics and ETL are required. Our understanding is MOSIP will not be providing any data points except for the logs for Analytics, please confirm. Please provide functional requirement for Document Management System. MOSIP does not use DMS and packet containing data and attachments will be stored in a object store - please confirm if DMS is still required		GoSL has no COTS products. All the COTS products required for the solution as mentioned in the RFP have to be provided by MSI with enterpirse support. Your understating of MOSIP data store is correct but DMS is required for storing the document load generated in the SL UID information system other than thedata store requirment.Please see baseline specs in the Annexure 3.
29	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	Section 3.4.17	93	Tape Library	As the back up is already configured on VTL. Is there a need for Physical Tape Library.		VTL requirement is dropped.
30	General				As discussed during SL Visit it was mentioned Enrolment volume per day is 38000 but in the peak they may get 75000, accordingly the sizing needs to be done. Please Confirm our understanding is correct.		Your understanding is correct
31	Annexure 10: Manpower Requirement	10.1	4	Offsite Support During O&M	As the MOSIP support will be taken over by MSP during O&M period however there is a need to have connectivity from Development centre in India to the Production Environment in Sri Lanka for entire duration of the project to provide support for Software and solution other than MOSIP. Please confirm that the connectivity between DC-DR setup and Offshore development and support centre in India will be provided.		GoSL shall provide the approval after discussion however the connectivy requirments will have to planned and procured by MSI

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
32	Vol-3 of 3	14.3	64	14. Taxes and Duties In this Procurement the following taxes are exempted. • Value Added Tax (VAT) • Ports and Airport Development Levy (PAL) • CESS • Customs Import Duty (CID) • Social Security Contribution Levy (SSCL)	Please clarify that these exemptions are applicable upon procurement through MSI's subcontractor in Sri-Lanka. Also Please confirm if the Withholding Tax in Sri Lanka is also exempted for all the procuremenst related to the project.		The exemptions are applicable for the procurement done only for SL-UDI project under this RFP in SriLanka. As per G2G MoU between India and Sri Lanka, responsibility of GoSL includes "Exemption of Contractor(s) from payment of VAT on project related procurement. Local Taxes, levies etc. on project related procurement to the extent permitted by applicable laws of Sri Lanka
33	SL-UDI-Volume-02-of-03-Annexure-6-Exit-Management	6.3	13	Exit Management schedule	During the site visit it was mentioned that the system has to go-live in 2026 -2027 Q3 - hence, the section has to be updated accordingly and also need clarity on the MSP scope (Taking over the components from MSI)		Please refer Volume 02 of 03 - section 3.2 SL-UDI Implementation, Operations, Support and Maintenance and Annexure 16 : RACI matrix.
34	SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology	3.7	42	d) Mobile Application	During site visit it was mentioned that no deciated mobile will be required, only SL UDI module will have to be provided to the Sri Lankan govt. Super App - Please confirm on this requirement		Query is not clear
35	SL-UDI Volume 2 of 3– Annexure 3 Minimum Technical	3.2 Product Benchmarking	3	a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023	Products appearing in all the three years i.e. calendar year 2021, 2022 and 2023 is restructive. Clause should be modified to Reports eligible for reference must be published **in any of the 4 years**, i.e. calendar years 2021, 2022, 2023, 2024.		Agreed
36	SL-UDI Volume 2 of 3– Annexure 3 Minimum Technical	14.1. List of Indicative Trainings	3	List of Indicative Trainings - Technical and Support Function	Kindly let us know the number of batches and number of users per batch per domain.		Batch size is limited to 10 per batch, for Techncial Training. It is further clarifed that for EO training three batches of 25 each shall be considered for train the trainers programme.
37	SL-UDI-Volume-02-of-03-Annexure-4-Software-Engineering.pdf	4.1.4	3	Development and Customization- As far as possible, MSI must ensure the open-source technologies and products are utilized for solution platform	It contradicts with the minimum tech requirement ask of using enterprise version and gartner magic quadrant, so can we consider this and go ahead with all open source products with enterprise support?		No. Please refer to Section3.2 Product Benchmarking in Volume 02 of 03 - Annexure 3: Minimum Technical Specification

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
38	Annexure-10	10.1 Professional Staff and Engagement Approach	4	Project Manager, Infrastructure Engineer, Network Engineer, CRM Engineer, BI Reporting and Data Analytics Engineer, Application Engineer, Information Security Manager etc.	The onsite deputation and full time deployment of applicable resources of MSI will depend upon the prevailing VISA policies of GoSL. We recommend following options: Due to practical standpoint and current VISA policy we recommend special provision from the MEA, GoSL which will allow MSI resouces to be placed for 6-12 months on work visa without Tax Liability in Sri Lanka.		The Visa will be facilitated by the GoSL.
39	Annexure 5: Demand Capacity	5.1.4. Estimation of Foundational ID platform users and Supporting Application Users	6	IT Helpdesk	(i) Kindly confirm the working days/hours for IT helpdesk team. (ii) Kindly confirm the GoSL delivery center location/ pin code for the IT helpdesk team setup. (iii) We undertand that a maximum of 5 (First Shift) + 5 (Second Shift) + 2 (Third Shift) + 2 supervisors refer to the helpdesk capacity to be considered by MSI for O&M phase of the project. (iv) Kindly confirm if the IT and Non IT infrastructure provided by GoSL for helpdesk team. (v) Kindly confirm if GoSL will provide the connectivity between the DC and place where the helpdesk team is located. (vi) Kindly confirm if GoSL will provide the necessary audio connectivity and associated audio routing equipments. if audio calls are there.		1. Please refer Annexure on Demand Capacity at Section 5.1.4 . 2. GoSL delivery centre id DC location , amnd IT helpdesk shall be located at the same place . 3. Refer to 1 above 4 IT infra has to be provided by MSI, connectivity shall be provided bu GoSL-Non IT shall be provided by GoSL 5 As above in 4 6. Yes it is required MSI has to provision this
40	SL-UDI-Volume-02-of-03-Annexure-1A-As-Is Functional System.pdf	1.4	7	Enrollment Kits Already Purchased and Deployed	During Sl visit it was mentioned that some of the Field devices including Biometric equipment have already been purchased by GoSL. Please confirm the list of the components already purchased and to be used by MSI. Also please mention the make and Model for the same. Also please confirm who will support the warranty for the devices. MSI will not be responsible if device fail to work during the intial installation and will not replace the faulty device at its own cost.		Already answered in S.No. 663
41	Annexure 11: Technology Overview	2.3	7	Integration Middleware	Integration middleware is not part of MOSIP component. In other part of rfp also it is mentioned under MOSIP components. Clarification required on the same. In case of Integration Middleware middleware requirement please provide the detailed specification and functional requirements.		Yes this has be dropped.
42	SL-UDI Volume 2 of 3– Annexure 11: Technology Overview	Sec 2.3.1	8	19. TSP and UA Software (Three sample applications – two in JAVA and one in .Net)	Under the Key Components section there is a mention of a TSP and UA software wherein 3 sample applications are asked. This has not been elbaorated in the sections below. Please clarify the scope of the MSI for these 2 applications.		Please read it as as 3 application. The stack is (i) Java (ii) Java Script (iii) .Net
43	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.3.1.1	8	Persons who obtain citizenship through Registrar General's Department - The prescribed details of a Person, who have obtained "Citizenship by Descent" at the time of birth, must be sent to DRP by Registrar General's Department (RGD) within the prescribed time after birth of such person and after verification of parents' details,	The parents/guardian/introducer have to be enrolled as a pre-requisite in SL-UDI system		Yes . But this can be clarified during project planning stage

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
44	SL-UDI Volume 2 of 3	Annexure 6: Transition and Exit Management	9	6.2.2 Hosting Infrastructure (i) Data Centre: The MSI **will hire the colocation space in the two tier-III data centers in Sri Lanka.** The MSI will setup the hosting infrastructure for the project **in a caged environment within the data centers, a separate cage (within overall cage) may be planned for security components (esp. Hardware Security Module).**	As per SL-UDI-Volume-02-of-03-Annexure-16- RACI Matrix document, pg 3, Sl. No 12, under Task / Activity - Data Centre Hosting Space, Physical Infrastructure (entire non IT), non-DC space for contact centre & helpdesk, bandwidth, the responsibility lies with GOSL. Accordingly, request to ammend the 6.2.2 clause and remove the underlined clauses from MSI's responsibility.		Yes GoSL shall provision this requirement
45	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	1.6 Targeted Performance Parameters (Throughput, Accuracy, Availability, Integration)	9	The SL-UDI should be designed considering the 20-year scale (2025 – 2045) i.e., population size of 33 million citizens. (Refer Annexure 5: Demand Capacity)	Since the project is only for the 4 years, does the MSI has to do the Hardware sizing and infrastructure for 20 years? As no hardware has a life span of more than 7 years and will have to be refreshed at that time asking the MSI to design size and supply the infrastructure to take care of 20 years scale will not be cost effective. Kindly let us know YoY increase in population for the next 5 years.		Hardware and software sizing has to be done for 30 million Unique Records
46	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	1.7 Components and their Procurement Strategy	9	(i) The MSI will have end-to-end responsibility of system integration, and the MOSIP & Non-MOSIP software components. The MSI will also be responsible for the entire hosting infrastructure and security infrastructure. (ii) The MSI will be responsible for procurement, supply and maintenance of biometric devices (enrolment and authentication devices) as well as biometric solutions (ABIS, SDK, Manual Adjudication, etc.) and corresponding hosting infrastructure (server, storage, tape library, etc.)	It is mentioned elsewhere in the RFP that Data hosting is to be provided by the GoSL. Kindly confirm that the hosting charges will be paid by GoSL.		Yes
47	SL-UDI-Volume-02-of-03	Annexure-3-Minimum Tech	10	Data Centre Space - 39 Data Centre Hosting Space (Primary Site) MSI - 40 Data Centre Hosting Space (Secondary Site) MSI	Request to change the provider from MSI to GoSL as the DC Hosting space in both Primary and Secondary sites will be provided by GoSL		Yes agreed
48	SL-UDI-Volume-02-of-03	Annexure-3-Minimum Tech	11	Network Connectivity Sl. No 66 to 76 - Provider MSI	Request to change the provider from MSI to GoSL as these are mentioned in multiple places in the RFP sections that these will be provided by GoSL		Yes agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
49	SL-UDI Volume 2 of 3	Annexure 6: Transition and Exit Management	11	6.2.10 Contract Management The MSI is expected to sign the contract with the Service Providers **(Data Centre, Network,** OEMs, etc.) in such a manner wherein the components can be transitioned in the name of GoSL or nominated party with provision to continue the services beyond the contract duration on same terms and conditions (including commercials, services, support, etc.).	As per SL-UDI-Volume-02-of-03-Annexure-16- RACI Matrix document, pg 3, Sl. No 12, under Task / Activity - Data Centre Hosting Space, Physical Infrastructure (entire non IT), non-DC space for contact centre & helpdesk, bandwidth, the responsibility lies with GOSL. Accordingly, request to remove the Data Center and Network Service Providers from MSI's contractual obligations.		Agreed
50	SL-UDI Volume 2 of 3	Annexure 6: Transition and Exit Management	11	6.2.10 Contract Management (i) Data Centre (DC and DR): At the end of contract, GoSL or nominated party may want to continue the deployment of SL-UDI systems in the data centers **hired by the MSI**. The **MSI should provision for adequate space in the data centers in such a manner to allow for gradual future expansion.** The **MSI through Data Centre Provider should ensure provisions for physical security, robust and spacious civil setup, reliable and consistent electrical setup (with power backup), and other industry standard facilities.** The Data Centre Provider should allow all major network service providers to terminate their connection in their data center premises proposed for this project.	As per SL-UDI-Volume-02-of-03-Annexure-16- RACI Matrix document, pg 3, Sl. No 12, under Task / Activity - Data Centre Hosting Space, Physical Infrastructure (entire non IT), non-DC space for contact centre & helpdesk, bandwidth, the responsibility lies with GOSL. Accordingly, request to rephrase this entire clause by changing the responsibility to GoSL.		Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
51	Annexure-6	6.2.10 Contract Management	12	(ii) IT Infrastructure: IT Infrastructure: The IT Infrastructure (servers, storage, enrolment kit, etc.) will be procured by MSI through multiple OEMs (including product's support and maintenance). GoSL will continue to utilize the IT Infrastructure beyond MSI's contract. In such a situation, the MSP will be required to provide the annual maintenance services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance contract services to be provided by MSP. In case parts are required for product, the OEM should maintain the same. For scaling of infrastructure, GoSL should not be bound to procure additional infrastructure from same OEM. For replacement of unrepairable product, the OEM should offer either same or better product meeting the specifications specified in the RFP (or as amended in the service order).	The MSI will get into contract with various OEMs with the validity of contract governed by the exit period. As the selection and governance of MSP will be done by GoSL, hence at the end of the MSI exit period, the MSP has to get into direct agreement with OEM for future AMC / ATS. **MSI will have no further responsibility after the exit period. Hence the clasuse needs to be modified/removed accordingly.**		Yes correct, but MSI has to support the transfering the EULA to the GoSL or its agency.
52	Annexure-6	6.2.10 Contract Management	12	(iii) Software Software: The Software Infrastructure (system software, application software, etc.) will be procured by MSI through multiple OEMs (including product's support and maintenance). GoSL will continue to utilize the Software Infrastructure beyond MSI's contract. Wherever possible, the perpetual product should be offered as part of the MSI. In such a situation, the MSP will be required to provide the annual maintenance support services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance support services to be provided by MSP. Wherever enterprise support as well as community edition support is available, for the period beyond MSI contract, the GoSL should be able to choose suitable support at its own discretion. For scaling of software, GoSL should not be bound to procure additional licenses for the same product. Wherever support is available through multiple agencies, GoSL should be able to choose the support agency at its own discretion.	The MSI will get into contract with various OEMs with the validity of contract governed by the exit period. As the selection and governance of MSP will be done by GoSL, hence at the end of the MSI exit period, the MSP has to get into direct agreement with OEM for future AMC / ATS. **MSI will have no further responsibility after the exit period. Hence the clasuse needs to be modified/removed accordingly.**		Same as above in Sr no 51

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
53	Annexure-6	6.2.10 Contract Management	12	(iv) Information Security and Business Continuity Information Security and Business Continuity: For security hardware and security software components, please refer to respective bulleted points above in Hardware and Software points.	The MSI will get into contract with various OEMs with the validity of contract governed by the exit period. As the selection and governance of MSP will be done by GoSL, hence at the end of the MSI exit period, the MSP has to get into direct agreement with OEM for future AMC / ATS. **MSI will have no further responsibility after the exit period. Hence the clasuse needs to be modified/removed accordingly.**		Same as above in Sr no 51
54	SL-UDI Volume 2 of 3	Annexure 6: Transition and Exit Management	12	6.2.10 Contract Management (ii) IT Infrastructure: The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance contract services to be provided by MSP.	All OEM contracts will have GoSL as the end user Hence the responibility extended to the MSI is GoSLs responsibility. Hence this clause be removed.		Already answered in S.No. 51
55	SL-UDI Volume 2 of 3	Annexure 6: Transition and Exit Management	12	6.2.10 Contract Management (v) Network: The network connectivity will be procured by MSI through network service providers and these connections should be scalable. The GoSL will continue to utilize the network beyond MSI's contract. The GoSL may choose to provide the network connectivity through the same or different network service provider.	As per SL-UDI-Volume-02-of-03-Annexure-16- RACI Matrix document, pg 3, Sl. No 12, under Task / Activity - Data Centre Hosting Space, Physical Infrastructure (entire non IT), non-DC space for contact centre & helpdesk, **bandwidth**, the responsibility lies with GOSL. Accordingly, request to remove the network connectivity procurement from MSI's SoW.		Yes understanding is correct
56	Annexure-6	6.2.10 Contract Management	12	(ii) IT Infrastructure: IT Infrastructure: The IT Infrastructure (servers, storage, enrolment kit, etc.) will be procured by MSI through multiple OEMs (including product's support and maintenance). GoSL will continue to utilize the IT Infrastructure beyond MSI's contract. In such a situation, the MSP will be required to provide the annual maintenance services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance contract services to be provided by MSP. In case parts are required for product, the OEM should maintain the same. For scaling of infrastructure, GoSL should not be bound to procure additional infrastructure from same OEM. For replacement of unrepairable product, the OEM should offer either same or better product meeting the specifications specified in the RFP (or as amended in the service order).	**Kindly modify the marked part as-** The MSI will get into contract with various OEMs with the validity of contract governed by the exit period after the end of the exit period the MSP has to get into direct agreement with OEM for future AMC / ATS. MSI will have no further responsibility after the exit period.		Same as above in Sr no 51

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
57	Annexure-6	6.2.10 Contract Management	12	(iii) Software Software: The Software Infrastructure (system software, application software, etc.) will be procured by MSI through multiple OEMs (including product's support and maintenance). GoSL will continue to utilize the Software Infrastructure beyond MSI's contract. Wherever possible, the perpetual product should be offered as part of the MSI. In such a situation, the MSP will be required to provide the annual maintenance support services for the aforementioned products. The agreement (or work order, purchase order, etc.) between MSI and OEM, should allow for such annual maintenance support services to be provided by MSP. Wherever enterprise support as well as community edition support is available, for the period beyond MSI contract, the GoSL should be able to choose suitable support at its own discretion. For scaling of software, GoSL should not be bound to procure additional licenses for the same product. Wherever support is available through multiple agencies, GoSL should be able to choose the support agency at its own discretion.	The MSI will get into contract with various OEMs with the validity of contract governed by the exit period after the end of the exit period the MSP has to get into direct agreement with OEM for future AMC / ATS. MSI will have no further responsibility after the exit period.		Same as above in Sr no 51
58	Annexure-6	6.2.10 Contract Management	12	(iv) Information Security and Business Continuity Information Security and Business Continuity: For security hardware and security software components, please refer to respective bulleted points above in Hardware and Software points.	The MSI will get into contract with various OEMs with the validity of contract governed by the exit period after the end of the exit period the MSP has to get into direct agreement with OEM for future AMC / ATS. MSI will have no further responsibility after the exit period.		Same as above in Sr no 51
59	Annexure-6	(v) Network:	12	Network: The network connectivity will be procured by MSI through network service providers and these connections should be scalable. The GoSL will continue to utilize the network beyond MSI's contract. The GoSL may choose to provide the network connectivity through the same or different network service provider.	As per RACI Matrix Annexure-16 1.1 RACI Matrix (Point#12). PageNo.3 the bandwidth is to be provided by GoSL and MSI has nothing to do with this. Hence thi clause may be approporiately changed.		Yes Agreed. MSI will support in integrating the SLUDI system
60	SL-UDI-Volume-02-of-03-Annexure-9-Service-Levels.pdf	9.4	12	Service Levels for Biometric Registration Kits - The GoSL (or their representatives) may make a complaint about the equipment/ service through letter, fax, e-mail, phone, SMS or any other means and updated on the respective issue management system, as the GoSL thinks fit or convenient to the Technical Helpdesk of MSI.	As there is a mention that there are some biometric devices procured by GoSL, should those devices be excluded from SLAs here? Or get KT and support details, the responsibility and accountability has to be defined clearly here.		It will be discussed in due course.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
61	Annexure-6	6.3.2 Continuation Of Project	13	a) In case of the Agreement being terminated by GoSL, GoSL reserves the right to ask the MSI to continue running the project operations for a period of 3 months after termination orders are issued and the MSI shall be obliged to provide such services for such period without any additional cost and expense to GoSL and without any impediment in the quality of services (measured against the target service levels defined in the Service Level Agreement of the RFP).	Beyond the end of contract which is triggered through a "TERMINATION PROCESS" MSI will have no contractual obligations to continue Services. **Hence this clause should be removed.** **This is a showstopper.**		The clause remains unchanged
62	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	1.8 Key Considerations (Summary of who does what as per MOSIP)	13	20. Card Activation At the time of issuance, the card is in inactive state and before usage of card, it needs to be activated. MSI needs to build and provide the functionality to activate the cards in both online and offline manner.	Kindly elabaorate. Is it OTP based activation system. Need clarification		Not needed
63	SL-UDI-Volume-02-of-03-Annexure-9-Service-Levels.pdf	9.6	18	Service Levels for Application and Software Services	Category is for Internal Facing critical applications, the formula says % of uptime for external facing components, this should be corrected.		The formula is corrected for your reference
64	Volume 2	5 Scope of Services	20	The proposed services/modules offered/interfaced to/with the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English).	We assume that the corresponding language text/translation will be provided by the customer and will be integrated/used/configured in the portal. No language translation tools are to be used. Kindly confirm that Srilanka Govt will provide any translation tool.		MSI to deliver the required Transliteration engine as per RFP requirement.
65	Annexure 9: Service Levels	9.8 Service Levels for Business and Technical Services	22	While the service desk shall only be measured on response to incidents, other teams like incident management and problem management shall be measured on restoration of service and resolution of the issues.	Kindly confirm the service Levels for service desk response time for incidents .		Refer Annexure 9: Service Levels. Section 9.8
66	Volume 2	5 Scope of Services	22	The MSI should provide both soft and hard copies of user manuals (e.g., Printed documents). All manuals should be in tri-languages (Sinhala, Tamil, and English)	The understanding is only the user manuals needs to be translated into Sinhala and Tamil language. The video, audio and certificate will be only in English language. We assume that the manuals are being referred to the user manuals of the application being developed		Yes only Application user manauls are to be translated
67	SL-UDI Volume 2 of 3– Schedule of Requirements	5 Scope of Services	24	MSI shall be responsible for integration and customization of following COTS applications:- Fraud Management Solution	The Fraud Managemnet solution is not mentioned in the SL-UDI Volume 2 of 3– Annexure 11: Technology Overview, where all the componnets are elaborated. Hence is Fraud Managemnet systme is in scope? However a section is there in "Volume 02 of 03 - Annexure 3: Minimum Technical Specification" for fraud Managemnet system		Yes Fraud Management System is required.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
68	Vol-2 of 3	Indicative COTS Components (Section 5.1.3)	24	MSI shall be responsible for integration and customization of following COTS applications: • Business Intelligence and Data Analytics • Customer Relationship Management • Document Management System • Identity and Access Management • Knowledge Management Solution • Learning Management Solution • Fraud Management Solution	Please confirm if the list of COTS component mentioned are to be procured by MSI as the compliance for the same has to be submitted along with the response. However the clause indicates that these products would be procured by GoSL. Request clarity on the same as this will have impact on system design and infrastructure sizing and implementation.		Yes to be procured by MsI with enterprise support
69	Volume 2	MOSIP Components / MOSIP Application (Section 5.1.2)	24	MSI shall be responsible for integration and customization of following COTS applications: Learning Management Solution	GoSL has an existing Learning Management System (LMS)? Is it going to be continued and managed by MSI or Is GoSL looking implementation and maintenance of new Learning Management System (LMS)?		No. GoSL does not have an LMS
70	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5 Scope of Services	24	2. Software Solution Section 5.1 [GoSL shall provide the list of COTS products to be integrated with SL-UDI system]	Kindly share the list of COTS products to be provided by GoSL which are to be integrated.		List of COTS products have been provided in the RFP. GoSL shall not provide any COTS product.
71	Volume 2	3.7. Web Portal	25	SL-UDI-Vol-2-of-Vol-3.pdf	Is development of TSP and UA Applications part of MSI scope? Kindly confirm. If Yes, Kindly provide the detailed specifications and functionalities of the TSP and UA applications.		Yes, development of 3 sample TSP application are part of MSI scope. A brief scope outline was provided in the bidder's conference in Colombo.
72	SL-UDI-Vol-2-of-Vol-3.pdf	5.1.4	25	TSP and UA Application (maximum of 2 sample)	Ideally the UI should be created by the TSP and the UA, here we can provide test clients/sandbox environment which is included as part of MOSIP, and then the APIs are exposed, to help with Authentication/eKYC etc..		Sample applications are being sought in the required languages.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
73	VOI-3	14. Taxes and Duties	26	14.1 For IT Products and/or Services supplied from outside the Employer's country, the Contractor shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies, payable in the Employer's country. Any duties, such as importation or customs duties, and taxes and other levies, payable in the Employer's country for the supply of Products and Services from outside the Employer's country are the responsibility of the Employer unless these duties or taxes have been made part of the Contract Price in Article 2 of the Contract and the Price Schedule to which it refers, in which case the duties and taxes will be the Contractor's responsibility 14.2 For IT Products and/or Services supplied locally, the Contractor shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Products or Services to the Employer. The only exceptions are taxes or duties, such as value-added or sales tax or stamp duty as apply to, or are clearly identifiable, on the invoices and provided they apply in the Employer's country, and only if these taxes, levies and/or duties are also excluded from the Contract Price in Article 2 of the Contract and the Price Schedule to which it refers .	Please confirm: 1) Is withholding tax applicable on MSI Invoice in Sri-Lanka. 2) If yes do we have to built in our price or is there any exemption on the same.		Already answered in S.No. 32
74	Volume 2	IT Helpdesk (Section 5.8.6)	27	Training to helpdesk manpower	Does GoSL is looking for any Train The Trainer sessions or only training would be provided using Training materials developed?		There will be train the trainer program for operators manning the enrollment centers. Training material in the form of PPT, video, voice over, and training booklets with application screenshot shall be provided by MSI. Howover, the trainer batch is limited to 3 batches of 25 each.
75	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.3	27	ECP-01 - Application form to be designed by DRP	Will DRP design and provide pdf forms, and should we host them on the website and make it available for citizens?		MSI will jointly develop the application form with GoSL and this should be hosted on the Citizen portal.
76	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.3	29	ECP-06- 6.6 - Facility must be given to "Add Minutes" to be checked at Green/Amber/Red	What is the business logic to "Add Minutes"?		Query is not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
77	Vol 1 of 3	3.1.2.2 Technical Score Parameter- Criteria A: MSI's Credentials and Experience	29	General	**The requirements given in** "Section 4.6.3 Bidder's Overall Technical Solution" & "Section 4.6.3.2 Overall Approach and Methodology & Work Plan" **are not in sync with** "Section 3.1.2.3 Technical Score Parameter- Criteria B: Evaluation of Proposed Technology Solution" & "Section 3.1.2.4 Technical Score Parameter- Criteria C: Overall Approach and Methodology". Please check and modify appropriately.		Already answered in Pre-qualification stage. S.No. 127
78	Volume 2	5.1.1 Phase-wise Implementation of SL-UDI Software System	31	Release_2: Subsequent version of the SL-UDI Software System i.e., 'Release_2' is planned in T+15 months. Release_2 shall consist of 'Release_1' applications and the rest of the support applications such as Fraud Management, Business intelligence and analytics, etc.	Please confirm if IT Helpdesk (Section 5.8.6) is part of Release_1 or Release_2 phase ?		IT helpdesk has to be implemented 60 days before Go- Live , hence, point of Release_1 or Release_2 is not relevent.
79	Annexure 11: Technology Overview	2.6.2	31	HSM Key(s): The BSP should provision its HSM and the BSP should ensure availability of key to the DRP from the time of installation of hardware	Confirm if the HSM is required seperately for BSP setup apart from the one which will be used for authentication services. Or can we leverage the common HSM for the whole setup ? During the site visit it was clarified that no dedicated HSM is required for Biometric Solution, please confirm		HSM is not required seperatetly for the BSP setup. Common HSM cannot be leveraged for the whole setup.
80	Annexure 10: Manpower Requirements	10.2 Minimum Qualifications of Key Professional Staff	33	CRM Engineer	In case MSI provides a COTS CRM the necessary CRM engineer (L1/L2) would need to be subcontracted from the CRM OEM/vendor.Please confirm if the CRM engineer can be direcrtly subcontracted from COTS OEM/Vendor?		Agreed
81	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.1.3 COTS Application	33	5.1.3.1 Business Intelligence and Analytics	Kindly provide details of the advanced analytics use cases.		Please refer to section 5.1.3.1 of Volume 2 of 3.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
82	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.3	33	ECP-21 - 21.1 - Scan and Tag additional documents	If the packet is not uploaded to the server then the changes can be made, however if the packet is uploaded to the server then it has to go through the process, which can either create the UIN or Reject the packet based on the information provided.		*"[DO/CO] Already scanned documents must be loaded. Scan and tag any missing supportive documents that were not submitted by the applicant initially. Facility must be provided to Remove selected images (not to delete but only mark "cancelled") or clear the images only to the current scanned documents, (not for previously scanned documents). Facility must be given to "Add Minutes" to be checked at Green/Amber/Red Channels."* --- *The above should be read as "After enrollment the applicants data including the scanned document and the democratic data shall be converted into an encrypted packet using the HSM key. This packet would be uploaded for checking at the backend and a workflow would have to be designed for decryption of the packet and validation by GoSL and*
83	Volume 2	5.1.3.2 Customer Relationship Management	34	8. GoSL shall provide the MSI with a toll-free number(s) for contact center.	(i) We understand GoSL will also provide the terminating PRI/SIP for the contact center (toll free mapping). Kindly confirm. (iii) We understand MSI scope of work for GoSL contact center involves Provisioning and integration of CRM solution ONLY.Kindly confirm.		(i) Agreed. PRI sizing requirement will be given by the MSI.
84	Volume 2	5.1.3.2 Customer Relationship Management	34	15. The CRM solution shall support IVR, Voice, Email and Web based complaint lodging, resolution, and response features using channels such as Voice, SMS, Email, WhatsApp and Web.	We understand that all the whatsApp business platform related licensing/ subscription and uage costs will be borne by GOSL.Kindly confirm.		This requirment is dropped.
85	Vol-2 of 3	5.1.3.3	35	Documents would be indexed using various unique numbers (internal and external)	What type of documents will be added to the Document Management System?		Please refer to minimum technical specification annexure 3.3.3.8 Document Management System

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
86	Vol-2 of 3	5.1.3.3	35		How much content will be added to the Document Management System - Per Day/Month or year?		Already answered in S.No. 98
87	Vol-2 of 3	5.1.3.3	35	The CRM system shall be integrated with the Knowledge Management System and Document Management System of SL-UDI Information System through suitable APIs.	Please clarify if all the content of the CRM System shall be integrated with the Document Management System? If so please provide how much content will need to be migrated?		Interfacing with DMS is required but there is no legacy data to be migrated to DMS.
88	Vol-2 of 3	5.1.3.3	35	General	Will there be any workflows integrated with the Document Management System? If so please provide the details?		Please refer to minimum technical specification annexure 3.3.3.8 Document Management System
89	Vol-2 of 3	5.1.3.3	35	General	Is there any existing Document Management system that should be considered? If so please provide details.		No
90	Vol-2 of 3	5.1.3.3	35	Annexure 6: Transition and Exit Management	How many users are expected to use the Document Management System?		It is expected that MSI will propose an open source COTS DMS with enterprise support.
91	Volume 2	5.1.3.2 Customer Relationship Management	35	18. The solution should support call routing functionalities.	Call routing is function of voice (ACD/IVRS) solution and nor CRM.Kindly remove this point for CRM scope of work.		Agreed
92	Annexure-1-Functional Overview	RCP-2	35	2.3 [System] If the “Application Language” is Sinhala, only auto transliterated edit-allowed Sinhala data fields shall be edited but English and Tamil data fields must be disabled for editing.	There is a mention of edit in the details submitted for processing in this section. As per mosip, once submitted the edit will not be allowed to the citizen data as it will lead to integrity failure of the respective packet. It can be approved or rejected only. Please confirm and elobrate on the requirement. All the data entry and verification needs to be done at enrolement client side / resident services portal by operator or resident as the case may be. Once packet created and sent for processing, it can't be edited or modified.		Agreed
93	Annexure-1-Functional Overview	RCP-4	36	If current record does not match with any records exist on DRP database and NRP Database, without any Biometric matching, System must set Biographic Verification status as “Pass.”	Please provide details on DRP and NPR databases mentioned in the RFP. As per MOSIP we have only ID repository.		Not applicable.
94	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.1.4.1 SL-UDI Citizen Portal	37	(viii) The portals should support Sinhalese, Tamil, and English languages.	The translation to Sinhalese and Tamil will be provided by GoSL. Kindly confirm.		Already answered in S.No. 64
95	SL-UDI Volume 2 of 3– Annexure 11: Technology Overview	3.3 Customer Relationship Management	38	Multilingual Support: CRM would be capable of multilingual support in French and Arabic language.	As the entire portal and application is supported in English, Tamil and Sinhalese Kindly remove the requirement of support for French and Arabic in CRM.		Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
96	Vol 2	5.1.4.6 Single Sign On (SSO) Module	39	The GoSL wishes to utilize the unique identity allocated to citizens to be used for the purpose of SSO within the SL-UDI modules as well as in the private and public sector services. For this purpose, the MSI needs to develop, operate, maintain, and support the SSO modules which works on open authentication protocol (AUTH 2.0). The SSO module should provide multi-factor authentication.	Can eSignet module of MOSIP be positioned here instead of developing from scratch?		Bidder may choose to develop/other open source or use any MOSIP module.
97	Volume 2	5.1.4.4 Knowledge Management System	39	The Knowledge Management System should capture meta data when adding a document such as keywords, date, title, description, target audience, date of issue, date of expiry etc.	What types of content will be published in the Knowledge Base (like what file types of pdf, audio, video and file formats would be supported). We understand that all KMS contents would be stored in CMS solution, please confirm.		The content will comprise of any Docx document including PPT, Excel, PDF, Audio, video files. There is no requirement of CMS.
98	Annexure 3: Minimum Technical Specification	3.3.3.4 Customer Relationship Management	40	7. The CRM solution should provide special functionality of handling handwritten letters as a part of grievance redressal. The letters shall be scanned and maintained in the CRM solution.	(i) The scanned letters will be maintained in DMS solution and not CRM solution.All scanned documents will be uploaded to the DMS via API call. Only the unique DIN (Document identification number) generated by DMS along with specific document details will be tagged to CRM ticket number and will be saved in CRM for future reference.Kindly update accordingly. (ii) Kindly confirm on the avg size and daily count of documents to be scanned.		(i) Agreed. (ii) 100 documents per day with file size of 250kb.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
99	Annexure-1-Functional Overview	RCP-7	40	7.6 [Manual/System] Facility to Preview and check History Records of previous ICs related to current NIC, if necessary (IC Inquires on separate window). 7.7 [Manual/System] Facility to Preview and check one or more Index Records (Index 1.6) related to current NIC, if necessary. (On same window) 7.8 [Manual/System] Last selected Index Records must be shown after the tab window has been changed to View Documents and come back to History Record again. - (switching facility) 7.13 [Manual/System] If the applicant possesses Dual Citizenship under section 19(2), and Dual Citizenship effective date is greater than the issued date of last IC, then forward the application to "Authorization Red" channel with Forward Reasons through Add Minute Form to cancel old indexes, computer records, Number book records 7.14 [Manual/System] If Biometric and Biographic Verification failure occurred, facility to check existence of matching records, following information should be displayed with respect to the current Application details after Biometric and Biographic Verification. (ARN/LRN/CRN/Application No. of existing system, NIC, Old NIC, Name, DOB, Gender, Address, Issued Date, Source, DSD, GND, BC No. Fingerprint Matching %, Photo Matching %, Matched Photo)	Please provide details on the below attributes Previous Ics Index Records computer records Number book records History Records LRN CRN Application No. of existing system		Not applicable.
100	Annexure 3: Minimum Technical Specification	3.3.3.4 Customer Relationship Management	41	17 . The CRM solution shall also measure performance indicators and SLAs for contact center and contact center agents. Some examples of the measurements are a. Response and Resolution times for grievances b. Average Handling Time (AHT) and c. IVRS Efficiency d. First Time Resolution (FTR) e. User interaction drop rates such as call drop rates, user interactions not responded etc.	AHT, IVRS Efficiency , call drop rates are voice solution (IVRS/ACD) reporting metrices.These reporting deliverables fall under the ambit of GoSL and its Voice solution service provider.Kindly update accordingly.		Query is not clear. However, requirement of voice solution is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
101	Annexure 3: Minimum Technical Specification	3.3.3.4 Customer Relationship Management	41	13. The CRM solution shall provision for both inbound and outbound channel support with associated technologies as mentioned below: a.CRM (product) b.IVRS c.ACD d.CTI e.Call logger f.Quality Management System g.Email response system h.Reporting systems i.Scanning Solution for letters & faxes j.Messaging Platforms k.Social Media Platforms management l.Live Chat	Integration with Messaging Platforms, Social Media Platforms management and Live Chat are part of Voice/CTI solution deliverables which should fall under the ambit of GoSL and its voice solution service provider.Kindly update accordingly.		This requirment is dropped.
102	Annexure 10: Manpower Requirements	10.2 Minimum Qualifications of Key Professional Staff	42	IT Helpdesk Agents	Since the IT Helpdesk agent would be proving L1 related support (taking calls, acknowleding, first level analysis/trouble shooting and categorizing tickets) and assigning unresolved tickets to the L2 and L3 product/module owners/ engineers kindly confirm: (i) If IT helpdesk agents can be subcontracted by MSI. (ii) If B.Sc/B.Com graduates with a minimum work experience of 1 year can be considered?		(i) Allowed (ii) Allowed
103	Annexure 1	3.3.3.6 Knowledge and Learning Management System	47	Ability to export report data	We need more details about the reports.		These are normal reports of usage by the users.
104	Annexure-1-Functional Overview	RCP-9	47	9.2 [System] If a Stated NIC No. is “Valid” OR Stated NIC No. is “Invalid” and one of the Related NIC No. is “Valid", Registration should be done with respect to “Valid” NIC No. else Generate “New” NIC No. as per the approved algorithm and Registration should be done with respect to “New” NIC No. 9.3 [System] New No. Confirmation Letter Generation should be flagged as per the conditions described in “New NIC Number Generation Criteria” 9.4 [System] Generate SL-UDI Number, if necessary, Update NPR and links of Family Tree	NIC No. and SL-UDI number mentioned in this clause and also in other clauses of RFP. What is the difference between NIC number and SL-UDI number and which one we need to consider for Unique Digital Identity number ?		As per the defined process, NIC no. will be used for reteriving the data from the eNIC for validation/verification of applicants data. SL-UDI number is the 11 digit number to be generated by the SL-UDI information system.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
105	Annexure-1-Functional Overview	RCP-10	48	10.12 [Manual/System] Load Applicant's Relations details, ARN/LRN/CRN/IVRN, TRN, PRN, NIC No., NIC Status, Name, DOB, Place of Birth, Gender, Address, Print Schedule, QA Accepted or Rejected Schedule, Card Scanning Schedule, Dispatch Schedule, Old NIC No., District, DSD, GND if available.	Please provide deails on IVRN mentioned in this requirement.		This process is dropped as the applicant registeration will happen in MOSIP.
106	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	49	(vi) Shall conduct periodic security audits of the data center and report annually.	a)Please confirm GoSL will hire third party security auditor for Application Security Audit, VAPT, Governance Audit. b)GoSL will bear any fee payable to the third party agency/authority for Security Audit. MSP will be only responsible for facilitating the process. Please confirm.		Your understanding is correct
107	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.2 Hosting Infrastructure	49	5.2.1.1 Data Center Strategy of Project GoSL has decided to utilize a two-way setup containing DC and DR sites. The DC and DR sites will be in 1:1 configuration i.e., exact replica of each other. For the entire duration, a mechanism for storage and safe keeping of backup tapes, a remote site will be utilized.	Kindly confirm the Gosl will provide the replication bandwidth between the 2 data centres (DC/DR) based on the requirement given by MSI.		Yes, GoSL will provide the replication bandwidth.
108	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	11.1	50	RCP-11 - Facility should be given to display Requests for Number Book Details through an ordered Queue - ARN/LRN/CRN/IVRN, NIC No. Sent Date, Sent Time, and Status (Pending/Open) of each Request should be displayed	Please provide the exact requirement as the statement is not clear as to what is to be delivered. Need more clarity		This process is dropped as the applicant registeration will happen in MOSIP.
109	VOI-1	ITB 20.5 (a)	50	All the prices should be quoted under the CIP basis to the SL-UDI Sites/Project Sites. In this Procurement the following taxes are exempted. • Value Added Tax (VAT). • Ports and Airport Development Levy (PAL). • CESS. • Customs Import Duty (CID). • Social Security Contribution Levy (SSCL).	We understand that these taxes are exempted for this bid. With respect to Social Security Contribution Levy, please confirm if the Tax levy is also exempted for SI resources travelling to Sri-Lanka and providing services in Sri-Lanka? .		Repeat query

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
110	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.2.6 Network Services	55	SL-UDI Wide Area Network 3. Data Center -Interconnection Network - P2P - MSI will be required to provide secure and reliable connectivity. 4. Data Centers (DC & DR) – NOC - MPLS/SDWAN - MSI will be required to provide secure and reliable connectivity. 5. Data Centers(DC & DR) – SOC - MPLS/SDWAN - MSI will be required to provide secure and reliable connectivity. 6. Data Centers(DC & DR) – Contact Centre - GoSL IPVPN - MSI will be required to provide secure and reliable connectivity. 7. Data Centers(DC & DR) – Technical Helpdesk - MPLS/SDWAN - MSI will be required to provide secure and reliable connectivity.	As per the RACI matrix these will be provided by GoSL. Kindly confirm.		All these requirements will be provided by GoSL
111	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.11 Business Rules Engine	56	The RE must be JSR94 compliant. The JSR 94 defines a standard API for a rules engine. It is important for the rules engine to comply with JSR94, so that it provides a common interface to the application development team	Please let us know whether bidder can propose pre existing proven packaged solution in the areas of Business Rules Engine which are proven across domains, scale and complexity. The pre existing packaged solution will be compliant to all possible Business Rules Engine rules and regulations and be compliant to all functional needs. Please let us know bidder is allowed to propose pre existing functionally compliant Business Rules Engine solution [not officially certified by any agency for JSR 94 standards as of today]		Please refer to Section3.2 Product Benchmarking in Volume 02 of 03 - Annexure 3: Minimum Technical Specification
112	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.2.6 Network Services	56	Internet Connectivity 11. Internet for mobile registration centers - Internet - MSI will be required to provide secure and reliable internet dongles for connectivity of mobile registration centers with the DC and DR	Kindly confirm that internet connection for mobile registration centers will be provided by GoSL. Also please confirm the type of connectivity.		Yes GosL shall provision this requirmenmt
113	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.2.7 IT Infrastructure Requirements	57	6 a. The MSI should not propose any component or sub-component which is likely to be declared end of sale within 36 months of award of contract.	This should be modified to 24 months from award of contract and provided the contract should be awarded within 90 days of the submission of proposal and should be included this in the MAF.		The suggestion of 24 months is accepted
114	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.12 BPM & Workflow (Business Process Management Suite)	58	Support process modelling based on BPMN2 notation standard	Please let us know whether bidder can propose pre-existing proven packaged solution in the areas of BPM and Workflow which are proven across domains, scale and complexity. The pre existing packaged solution will be compliant to all possible workflow business rules and regulations and be compliant to all functional needs. Please let us know bidder is allowed to propose pre existing functionally compliant workflow solution [not officially certified by any agency for BPMN standards as of today]		Please refer to Section3.2 Product Benchmarking in Volume 02 of 03 - Annexure 3: Minimum Technical Specification
115	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.15 Distributed Messaging	62	The SL-UDI services preferably be integrated using open source/standard version of Enterprise Service Integration platforms	ESB for internal access shall be provided by SL-UDI or MSI has to bundle the solution for ESB		This requirement is dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
116	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.3.2 Supply, Installation and Commissioning of Enrolment Kits	62	(iv) In addition to the given quantity (specified in the Schedule of Requirements, Volume 2), additional biometric devices may be procured through the BSP at the rates specified in the contract signed between GoSL and MSI. In such a case, the scope of work for these additional biometric devices will be same as those for the original biometric devices.	For how many years price is to validated.		Query is not valid. Please refer to price bid on unit rates and quantity.
117	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.3.2.1 Pre-Supply Activities	63	Services: All the equipment shall be supplied with the relevant interface cables and necessary standard accessories. Also, all the equipment shall be provided with global standard, 3-pin power square plugs (230V supply voltage and 50 Hz, as required).	Kindly specify enrolment devices enrolment kits has to be delivered at one centre place and GoSL will further do the distribution to the respective sites.		Your understanding is correct.
118	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.3.2.1 Pre-Supply Activities	63	**Custom Clearance:** The MSI is completely responsible for clearing the imported goods through customs in an efficient manner free of any additional cost.	GoSL will provide all the necessary paperwork and support for custom clearance. Please confirm.		Yes GoSL shall support this requirmenmt
119	Vol-1 of 3	4.4.2 Key Personnel Details	66	Date of birth	Since Date of birth is PII (Personal Identifiable Information) we cannot share this detail for employees.		
120	Volume 2	5.6.1 Training Needs Assessment	66	Th training shall be imparted on the Training of trainers (TOT) model where GoSL shall identify the master trainers to be trained by MSI. The master trainers in turn shall train the rest of the stakeholders. Maximum MSI shall train not more than 100 Master trainers.	GoSL is considering Train the Trainer concept. MIS will be only responsible to train the master trainers via conduction training sessions. The end users/stakehodler training is out of scope for SMI. Is the understanding correct?		Yes the understanding is correct
121	Volume 2	5.6.1 Training Needs Assessment	66	Th training shall be imparted on the Training of trainers (TOT) model where GoSL shall identify the master trainers to be trained by MSI. The master trainers in turn shall train the rest of the stakeholders. Maximum MSI shall train not more than 100 Master trainers.	The training to be imparted to the Master Trainers will be in English language only, is the understanding correct?		Understanding is correct
122	Volume 2	5.6.1 Training Needs Assessment	66	(v)Prepare online tutorials, videos, presentations to be which shall be uploaded on the KMS portal. Obtain sign-off on the online tutorials, videos, presentations from the GoSL. Upload the content on KMS post approval.	Online tutorials, videos and presentations' content will be same as Training material prepared for Train the Trainer concept? Pls clarify		Yes the understanding is correct
123	Volume 2	5.6.1 Training Needs Assessment	66	MSI has to ensure that the personnel deployed for training are properly qualified and understand the area of their training in depth.	Here the ppersonel deployed for training are the Master Trainers? Is there any qualification test required for the Master Trainers?		Bidder has to choose qualifed trainers who have the knowledge of SL - UDI Information System

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
124	Volume 2	5.6.1 Training Needs Assessment	67	MSI is expected to design the test methodology in consultation with GoSL. MSI shall also devise a test for trainees, the test questionnaires must be approved by GoSL. GoSL shall also supervise all training provided by MSI and the Master Trainers at the regional level.	The test for trainees? Does it mean that the test is to be provided only to the Master Trainers? Or does it mean the test to be assigned to the end trainees by the Master Trainers? Pls confirm.		The test is only for Master Trainers . But the same test can be used for training the other trainees and MSI shall supoort this.
125	Vol 1 of 3	4.4.3 Current Contract Commitments/Work in Progress	68	Form 4.4.3_Current Contract Commitment / Work In Progress	Text is striked off. Please confirm if it is deleted clause or we need to share.		The requirement is dropped
126	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.7.1 Performance Testing	69	Auth_2 Advanced Performance Test with proposed sizing and associated IT Hardware:	Please confirm server Gallery Size		Already answered in S.No. 717
127	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.7.1 Performance Testing	69	(e). The list of equipment used for the test shall be the same as proposed by the MSI, if however, there is a shortfall in the quantity of the equipment proposed, the MSI shall provide the required quantity of equipment/licenses as the case may- be to achieve the performance testing results and SLA.	Where will the performance testing to be done ? Kindly confirm		In the production environment
128	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8 Information Security and Business Continuity 5.8.1 Information Security	73	The GoSL is preparing the following, but not limited to: (i) Information Security Policy & Plan (ii) Access Control Policy and Procedure (iii) Business Continuity Management Plan (iv) Incident Management Policy and Procedure (v) Information Backup Management Policy and Procedure (vi) Information Security Policy for Technical Users (vii) Vulnerability Management Policy and Procedure (viii) And other policies and guidelines	All these should be made available now, so that the additional needs are taken care of.		Please refer to Volume 2 S.no. 5.8.1
129	Volume 2	5.8.1.8 Security Processes and Procedures	81	2-factor authentication process: MSI shall develop and implement secure login process and avoid unauthorized access via implementation of combination of password, OTP, Biometrics, etc.	2FA authentication is required for all the users or only specific roles?		Already answered in S.No. 405
130	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.1.9 Security Controls - Enrolment related Security	82	11) GPS devices shall be installed at the enrolment system and enrolment software shall capture the Geo location and send along with the enrolment packet to ensure that enrolment is not done outside the country.	Please include the GPS device in the line item under the enrolment kit.		This requirement is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
131	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.2 Business Continuity and Disaster Recovery	85	(ii) MSI shall endeavor zero data loss while switching from Primary Site to Disaster Recovery site by maintaining a very high level of RTO and RPO.	1. As per RPO/RTO specified by GoSL. Zero data loss not possible with 2 site system if the DC are beyond 40Kms. Please modify the RPO accordingly. 2. As per the RACI matrix given on page number 2 of Annexure-16 RPO <=1 hour and RTO <=4 hours Kindly correct the discrepancy		1. The ask is only that MSI shall endeavour to achive this. 2. Yes RTO , RPO given in RACI Matrix holds good.
132	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.2 Business Continuity and Disaster Recovery	86	(ii) Replication built-in feature, virtualization manager replication, storage replications, third-party tools etc. will be defined for each service and application during the design phase. (iii) The Primary and Secondary sites will be configured in an Active-Active (for citizen facing applications, CRM, email, etc.) and Active-Passive mode (for other applications). (iv) Both RPO and RTO will be discussed and agreed between SL-UDI and MSI during the design phase. MSI shall indicate the RTO and RPO of their solution in the technical response to the RFP. (v) Replication between the Primary site and the Secondary site will be enabled and configured. (vi) Virtual servers for DR will be built on top of virtualization manager hypervisor offering an industry-leading virtualized platform and best-of-breed technologies to maximize the reliability and availability of your applications.	1. Please clarify if the values for RTO/RPO given in RACI matrix given on page number 2 of Annexure-16 has to be taken or the section on page-86 has to be followed. 2. RTO & RPO has to be specified by GoSL in the RFP before the submission of the solution as the MSI will size and design the solution accordingly. RTO & RPO has to be specified by GoSL in the RFP before the submission of the solution as the MSI will size the infratstructure accordingly. The same cannot be discuused at design time as it will have commercial impact on the costing.		The values for RTO/RPO given in RACI matrix given on page number 2 of Annexure-16 has to be followed.
133	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.2.1 Process/component wise Recovery Strategy	87	1. Enrolment • Active – Passive (DC – DR), VTL and /or offline tape backup 2. Authentication • Active – Active (DC – DR), VTL and /or offline tape backup 3. Critical portals • Active – Active (DC – DR), VTL and /or offline tape backup 4. Other portals • Active – Active (DC – DR), VTL and /or offline tape backup if any data other than logs 5. Email • Active – Active (DC – DR), VTL and /or offline tape backup 6. CRM • Active – Active (DC – DR), VTL and /or offline tape backup 7. SOC • Active – Active (DC – DR), VTL and /or offline tape backup 8. Admin offices • Active – Passive (DC – DR), VTL and /or offline tape backup	1. Kindly clarify what is meant by applications operating in an active-active mode across DC and DR. 2. Kindly clarify how will data be repolicatd across the Data Centres for applications operating in Active Active mode, and how will data consistency be maintained for active active operations. 3. Please note that it may be possible to have authentication application working in an active-active mode from both Data Centres, However it may be impractical to have applications like enrolment, email, CRM etc. in active-active mode. Request the department to re-look at the deployment.		Item VTL is dropped. Refer to Volume 2 S.no. 5.8.2.1

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
134	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.2.2 Data Backup	87	(i) Data Backup Strategy: Grandfather-Father-Son (GFS): Key Aspects of GFS Strategy, to be implemented by the SL-UDI Master System integrator: a. On the last day of every month, a full backup shall be performed and labelled “grandfather”. The tape shall be stored permanently offsite. b. On the last day of every week, a full backup shall be taken called the “father” and stored offsite. c. Daily incremental backup shall be done called the “son”. Son tapes can be stored onsite or offsite depending on the volume of data changes. Onsite tapes shall be kept in fireproof cabinet. d. Tapes shall be moved by MSI to offsite location on Daily basis at a geographically separate location with appropriate physical security controls, at par with banking regulator of Sri Lanka for such secure transfer, arranged by MSI.	Kindly confirm if the backup has to be taken on both sites for applications which are in active-active state.		yes
135	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.2.5 Disaster Recovery Strategy and Procedures	90	4. Any telecommunication link is down • Dual path telecom connectivity • Dual Service providers • Different Telecom service providers for DC and DR • Failover to DR in case DC is completely down or vice versa	Since dual service providers are required at each of the sites it may be impractical to have different Telecom service providers for DC and DR. Kindly remove the clause since this would mean to interact with 4 telecom providers.		The DC-DR are tier III certified and the network links of multiple telecom service providers are present in the communication room. However, it is for the MSI to select the telecom service provider in the consultation with GoSL and DCSP. The MSI will follow the business continuity policy of DCSP and GoSL.
136	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.3.8 - Damaged /Defaced /illegible/information change (DCP)	95	Handling of card replacements and changes	What are the recommended or required protocols for handling damaged or defaced cards in terms of recycling or responsible disposal?		This is the responsibilty of GoSL
137	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.4 Support (Contact Center and Helpdesk)	97	(v) MSI will be responsible for supplying and implementing Customer Relationship Management (CRM) software to support Contact Center Agents / GoSL Officials at the Contact Center.	How many seats in call centre are required as licesnses are based on seats.		Please refer to clause 5.1.4. Estimation of Foundational ID platform users and Supporting Application Users in Anexure Demand Capacity

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
138	Volume 2	5.8.4.3 Deployment of Infrastructure for Contact Center Operations	98	o. Automatic Call Distributor (ACD) for distribution of incoming calls to Contact Center staff as they are received. MSI shall be responsible for installation of the ACD. ACD should have at least the following features:	ACD is a component of voice solution that includes IVRS as well. We understand that this deliverable (ACD) also falls under the ambit of GoSL and its voice solution service provider.Kindly confirm.		This requirment is dropped
139	Volume 2	5.8.4.3 Deployment of Infrastructure for Contact Center Operations	99	• System shall support the ability to play customized announcements per queue as defined by the administration.	We understand that the voice recordings (recorded in professional studios) for the custom IVRS/ACD announcements and will be provided by GoSL Kindly confirm.		This requirment is dropped.
140	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03	5.8.4.4 Other responsibilities of MSI for Contact Center Operations	99	5.8.4.4 Other responsibilities of MSI for Contact Center Operations	Secondary contact centre with 1/4th capacity should also be maintained at different site for Business Continuity operations.		This requirement is dropped
141	Volume 2	5.8.4.7 Key features of the proposed Contact Center	100	The Contact Center should include mechanism of calls, email, chat, chatbot, voice over IP (VoIP) and website support. Note: Chatbot should be trained to answer questions and should learn based on the responses provided and other	We understand that the chatbot, VOIP and chat are not in the scope of MSI deliverables.These solutions will be provided by GoSL.Kindly confrm.		Yes your understing is curretn but the CRM solution should support this functionality
142	Volume 2	5.8.5 IT Helpdesk	102	(i) Staff the service desk with technically qualified system admin, application, IT infra and Biometric specialists in two shifts 24*7.	Since the MSI will operate a 7x24 hour heldpesk team we would need to manage the staffing within 3 shifts of 8 hr duration each.Kindly update accordingly.		Please refer to section 5.1.4. Estimation of Foundational ID platform users and Supporting Application Users - Demand Capacity Annexure where details of all three shifts requirment are provided.
143	Volume 2	5.8.5.1 Helpdesk Setup and Operations	102	(i) MSI shall be responsible for setting up an IT helpdesk operation to support IT issue resolution.	(i) Kindly confirm the location for settig up the IT helpdesk support team. (ii) Kindly confirm the number of IT helpdesk users that will berequried to operate across the proposed 3 shifts.		(i)The location of helpdesk shall be Primary Data Cntre locatipn or a mutually agreed during project plan workoit with GoSL (ii)MPlease refer to answer in Sr, no 143
144	Volume 2	5.8.5.1 Helpdesk Setup and Operations	102	(iii) MSI shall deploy CRM software / Incident Management module of EMS for the helpdesk which shall be accessible to limited users (maximum 5) of the SL-UDI application for logging issues.	(i) We undertand that these 5 users of SL UDI application will be over an above the 12 seats (Year-1 and Year-2) &10 seats (Year-3).Kindly confirm. (ii) Kindly confirm the total and concurrent number of internal users who be be raisng the tickets via self assit portal of the IT helpdesk solution (EMS).		Yes the understanding is correct

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
145	Volume 2	5.8.5.2 Deployment of Infrastructure for IT helpdesk	103	c. Network Connectivity between IT helpdesk and DC, and IT helpdesk and DR	We understand that SL has its own IP/VPN with Sri Lanka Telecom secure network to connect their fixed registration centers. GoSL will provide secure connectivity (including registration center end-point devices) from this network to the SL-UDI DC and DR.This network will also be extended to establish Connectivity between IT helpdesk and DC, and IT helpdesk and DR.Kindly confirm.		Yes the understanding is correct
146	Volume 2	5.8.5.2 Deployment of Infrastructure for IT helpdesk	103	d. Automatic Call Distributor (ACD) for distribution of incoming calls to IT helpdesk staff as they are received. MSI shall be responsible for installation of the ACD. ACD should have at least the following features: • System should be able to intelligently route the callers to IT helpdesk staff based on their specialization and availability	ACD is a component of voice solution that includes the IVRS as well. We understand that this deliverable (ACD) also falls under the ambit of GoSL and its Voice solution service provider.Kindly confirm.		The requirment is dropped
147	Volume 2	5.8.5.4 Set up IT Infrastructure for Helpdesk Operations	104	f) IT Helpdesk application should record the calls	Call recording is a component of voice solution that includes the IVRS as well. We understand that this deliverable (call recording) also falls under the ambit of GoSL and its Voice solution service provider.Kindly confirm.		This requirment is dropped
148	Volume 2	5.8.5.5 IT Helpdesk operations	104	(i) Log incidents/issues as service requests and provide a unique service request number. Acknowledgement should be sent to user along with service ticket number through an email immediately on issue logging. All issues logged should be assigned a severity level (L1/L2 or L3)	(i) Kindly confirm the monthly/annual estimated/actual volumetrics for IT heldpesk related tickets for the following channels: (a) Voice (b) Email (c)Self assist IT helpdesk portal.		(i) The requirment of logging Voice tickets is dropped ii) Volume of tickets has to be calculated by MSI. However since helpdesk is 24x7 all incidents have to be logged.
149	Annexure-3	3.5.1.9 Internet Dongle	304	Internet Dongle	Kindly confirm that all the necessary paper work as per Sri Lankan law for procurement of dongles has to be facilitated by GoSL.		This requirement is dropped
150	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.6	54 - 88	Registration Support Processes	Need more clarity on this process, is it in the scope of MSI?		Registration enrollment centers shall be manned by the GoSL staff. However, for example but not limited to, MSI is required to monitor the network uplink, registeration data quality, configuration of enrollment client and admin module of MOSIP
151	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.7	88 - 95	Lost card process	Need more clarity on this process, is it in the scope of MSI?		This requirement is dropped . Cards shall be issued by GoSL

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
152	Annexure-1A-As-Is Functional System	All	All	Complete Annexure	the current process flow of NIC issuance is same as the the requested in the RFP Annexure-1-High Level Process Flow. Do we need to consider the current as is system and migrate to the new setup ? Or need to implement a fresh. What about the data already in the current system. Any migration is required ?		It is fir information that e-NIC demographic legacy data for each applicant will be used in SLUDI MOSIP application for the purpose of pre-registration and validations of applicant's details. The applicant will be able to update, edit, append and add missing data. It is further confirmed that no integration will be made with the e-NIC system except for demographic data verification and updates.
153		General		MSI payment and Taxation related	As per RFP it has been stated payment will be made only in INR, as per Indian GST law transaction will be considered as zero rated (i.e. no tax charged considering export) only if payment for the services received in convertible foreign currency or in INR if permitted by Reserve Bank of India (RBI), we understand that Sri Lankan recipient of services or goods is permitted by RBI to make payment in INR and for making payment the procedures defined under RBI Circular No.10 (RBI/2022-2023/90 A.P. (DIR Series)) dated 11th July, 2022 required to be followed. We request to confirm whether payment from Sri Lanka will be made following the procedure defined in referred Circular ?		Already answered in S.No. 693
154	Volume 1 & 3	General		Export Control	Since this is a Government to Government project please confirm if there are any Transfer of Technology Agreement applicable for this contract. Request clarifications and details on the same.		No such transfer is envisaged
155	Volume 1 & 3	General		FEMA/Indian Contract Act	Please clarify if the FEMA/India Contract Act would be applicable to the RFP		Already answered in S.No. 694
156	Volume 1 & 3	General		Export Control/License Agreement	Is there list of Import control restrictions form Specific countries for HW/SW in Sri Lanka. If so request to please share the list. We also request GoSL to share Embargo list of countries.		Already answered in S.No. 695
157	Volume 1 & 3	General		Office Space for local delivery	Please clarify if MSI can use Sub-contractor's office space as Project office.		Yes MSI can use the space of sub-contractor
158	Volume 1 & 3	General		DC/DR Set up	We understand that the space for DC/DR would be provided by GoSL. Please confirm that Power, cooling, wiring and racks along with the necessary infrastructure for setup of DC/DR be provided by GoSL. Kindly provide the Tier specifications of the data centres been provided by GoSL.		(i) DC DR space is provided by GoSL (ii) DC DR facilities shall also be provided by GoSL (iii) DC / DR shall be Tier III certifed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
159	Volume 1 & 3	General		Payments, Taxes and Duties	Please confirm whether payment to Indian bidder will be paid by following RBI procedure i.e. payment will be made from Special Vostro account of foreign bank maintained in India ? Note: If we are expected to receive payment from Indian organization bank account then we need to charge Indian GST@18% on offshore services. Please elaborate on GST credits. And confirm If we will get exemption on the GST.		Payment for the project to MSI will be released in India by PIA i.e MoDE, GoSL (on the recommendation of JPMC) from their Indian Rupee Bank Account maintained in HDFC Bank in Worli, Mumbai.Further, the question of applicability of Withholding Tax in Sri Lanka doesn't arise, since payment is made in India. It may also be noted that export of goods is zero rated in GST. Therefore, items procured in India for export to Sri Lanka for the project would be exempted from GST.
160	Volume 1 & 3	General		Seating Space	Will GoSL provide space for the seating of the key personnel during the engagement.		GoSL will provide space for the seating of the key personnel during the engagement.
161	SL-UDI-Volume-02-of-03-Annexure-1A-As-Is Functional System.pdf and SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	All	All	Both the Annexures	During the site visit it was clarified that existing process flow will not be considered. Revised process flow will be discussed and decided by the customer during requirement gathering stage (Document Verification) and it will be implemented as an external stage in MOSIP. Please confirm of the understandng is correct, so that we will not consider the mentioned annexures		Yes the understanding is correct.
162	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.3	27	ECP-01 - Application form to be designed by DRP	Will DRP design and provide pdf forms, and should we host them on the website and make it available for citizens? Have seen some forms on the DRP website already.		MSI and GoSL shall design the form in consultation however this will be made available by MSI on the citizens portal
163	SL-UDI-Volume-02-of-03-Annexure-1-High Level Process Flow	1.4.4.3	33	ECP-21 - 21.1 - Scan and Tag additional documents	If the packet is not uploaded to the server then the changes can be made, however if the packet is uploaded to the server then it has to go through the process, which can either create the UIN or Reject the packet based on the information provided.		Please refer the reply Sr no 82
164	SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology	3.7 (d)	45	Mobile Application requirements - Point 14: My Profile - Digi Locker	Need more clarity in the requirement		Please refer Volume 02 of 03 - Annexure 3: Minimum Technical Specification Section 3.3.3.3 Mobile Application
165	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	4. Support for Multiple Pre-enrolment Data Sources	It is recommended to be managed via MOSIP- need more clarity		There is no multiple pre-enrolment data sources except the MOSIP and eNIC, which is required to be interfaced .

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
166	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	6.Ability to Capture Usage Metadata for Analysis	Need more clarity		Please refer 5.1.3 COTS Application and 5.1.3.1 Business Intelligence and Analytics Volume 2 of 3
167	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	8. Support for Audio Messaging (confirmations, instructions, etc.) in Languages in Sri Lanka	MOSIP does not have the feasibility for Audio messaging - need more clarity		This requirment is dropped
168	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	13. Ability to Integrate with Retina Scanner and Capture Retina Scans as per Specification	Mosip has the feasibility to capture, Finger, Face and Iris only, need more clarity on the requirement of retina scan		Retina scanner should be read as Iris Scanner
169	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	18. Automatic Audit of Forced Capture	Need more clarity- for now thresholds will be set to capture the biometrics, which if not accurate may highlight forced capture		Threshold parameter shall be set in consulation with GoSl for data quality purposes
170	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	16	20 &21. Biometric sample and Biometric bundle	Need more clarity		Biometrci bundle may be read as biometric packet . Biometric sample may be dropped
171	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	17	30. Ability to freeze client once a new version is available, after a certain cutoff date	Need more clarity		If MOSIP releases a new version client software then old verion should be frozen.
172	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	18	43. Ability to integrate a hardened VM through a dongle	Need more clarity		At times VM may be loaded on adongle , hence capacity to inegrate through a dongle. However MSI may plan accrodingly.
173	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	18	50. Ability to work in Online mode – where minutia + Demographic details can be sent to SL-UDI-DS through an online web-service and get **near real** time YES or NO confirmation that the citizen is successfully deduped and good for a UDI generation	ABIS solution will be used for dedupe check, however actual enrolment will have some manual verification and hence cannot be near real time.		Real time dedup is not envisaged and the ABIS should run in batch mode.
174	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	19	57. Ability to auto suggest fields such as names, locations etc. based on live fuzzy matching from a Local Location and Names Master data	Need more clarity		Fuzzy matching is not part of MOSIP, hence requirement to be removed.
175	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.2	19	54. Supporting local data validation using local master data stored.	Need more clarity		Validation has to be applied only for the location/address.
176	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.3	21	20. Capability to Dynamically allocate Biometric Deduplication requests to the Biometric Identification solution based on failure rates and response time	a dynamic biometric load-balancing mechanism that sends deduplication requests to the best-performing biometric engine based on accuracy and speed, ensuring efficient and reliable biometric identification.		This query will be answered during the next round of clarification.
177	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.2.3	24	67. Distributed processing with concurrent deduplication	Need more clarity		Requirement is dropped
178	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.9	51	8. Supporting Storage of UDI Fields for Optimal Analysis	As a best practice we should not store UDI related data in any other system except MOSIP		Bidder's understanding is correct.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
179	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.9	52	16. Process Session Data	We will not be maintaining any sessions, all sessions are stateless and token based		Agreed
180	SL-UDI-Volume-02-of-03-Annexure-15-Transition Framework	1.4	7	This annexure mentions about transitioning the existing DRP system including manpower by MSI	During the site visit it was clarified that the existing system will not be transitioned and SL UDI will be a greenfield implementation, please confirm.		Yes the understandng is correct.
181	SL-UDI-Volume-02-of-03-Annexure-13-Card Printing Personalization Technology	All	All	This annexure talks about Card Printing which has only machine and card related information	What is the scope of MSI w.r.t this annexure.		This is the responsibilty of GoSL
182	SL-UDI-Volume-02-of-03-Annexure-5-Demand-Capacity	5.1.4	5	Estimation of Foundational ID platform users and Supporting Application Users	As clarified during site visit the process will undergo a change and hence this section will have to be modified accordingly		Not clear
183	SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology	2.3.5	11	ii. ETL would be used for integration of all application data with the Data Warehouse, Business Intelligence, Analytics, , etc.	PII data will not be available for analytics or reporting, do we still need ETL?		This requirement i.of ETL is dropped
184	SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology	2.4.2	14	Integration Middleware	In MOSIP there is not integration middleware, please confirm on this requirement		Requirement is dropped
185	SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology	3.2	34	(viii) ETL/Data Acquisition System: This would include tools that would extract data from all the source systems into the BI Tool. This ensures data in BI is integrated with other parts of the system to ensure data is consistent with the rest of the system.	MOSIP has a reporting framework, please confirm if the same can be leveraged, if yes- do we still need consider this BI and anlytics requirement and supply of the respective COTS		Requirement of ETL is dropped, BI is required
186	SL-UDI-Vol-2-of-Vol-3	5.1.4.6	39	Single Sign On (SSO) Module	Do we have the consider e-signet module from MOSIP to meet this requirement, please confirm.		Bidder to provide solution as per requirement in vol 2 section 5.1.4.6.
187	Annexure-3	3.4.1.9. Network Core Router	97 of 361	Performance: 1) Minimum IP forwarding throughput of 190Gbps/higher. 130Gbps/higher IPSEC Bandwidth, 30Gbps/higher IMIX/EMIX encryption throughput. 2) 4000/more IPSEC tunnels. 3) 8000/more VRF segments. 4) Minimum 4M/more IPv4 & IPv6 routes. 5) 30M or more firewall sessions.	**Request to modify as : 250 IPsec tunnels & 1000 VRFs** Performance: 1) Minimum IP forwarding throughput of 190Gbps/higher. 130Gbps/higher IPSEC Bandwidth, 30Gbps/higher IMIX/EMIX encryption throughput. 2) 250/more IPSEC tunnels. 3) 1000/more VRF segments. 4) Minimum 4M/more IPv4 & IPv6 routes.		Original specs and the suggested specs, both are allowed and can be considered.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
188	Annexure-3	3.4.1.9. Network Core Router	97 of 361	Layer 2 , Layer 3 Security and other features: 1) static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling. 2) IKEv1, L2TP, IKEv2, GRE and IPSEC. 3) Router should support Zone Based Firewall feature. 4) Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided. 5) 802.1p class of service and marking, classification, policing and shaping. 6) AES-256 and AES-GCM. 7) Hierarchical QoS should be supported both at Physical and sub-interface level. 8) Support deep packet inspection to identify applications at layer-7 and 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. 9) IGMP v1/v2/v3 and PIM multicast routing.	**Please remove the highlighted.** Layer 2 , Layer 3 Security and other features: 1) static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling. 2) IKEv1, IKEv2, GRE and IPSEC. 4) Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided. 5) 802.1p class of service and marking, classification, policing and shaping. 6) AES-256 and AES-GCM. 7) Hierarchical QoS should be supported both at Physical and sub-interface level. 8) 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. 9) IGMP v1/v2/v3 and PIM multicast routing.		Already answered in S.No. 362
189	Annexure-3	3.4.1.9. Network Core Router	98 of 361	Manageability features: 1) SSHv2, SNMPv2c, SNMPv3 and NTP. 2) support AAA using RADIUS and TACACS+. 3) Support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1. 4) Support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	**Please remove the highlighted.** Manageability features: 1) SSHv2, SNMPv2c, SNMPv3 and NTP. 2) support AAA using RADIUS and TACACS+. 3) Support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1.		This feature is mainly for VoIP and its monitoring may not be required and hence should be dropped.
190	Annexure-3	3.4.1.10. Network Core Switch	98 of 361	Core Switch should meet/exceed following hardware features/capacity. 1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 80MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber modules should have duplex LC connector to work with multi-mode fiber supporting minimum 300 meters for 10Gbps link and 100 meters for 100Gbps link.	**Please change 80MB buffer to 32 MB dynami intelligent buffer** Core Switch should meet/exceed following hardware features/capacity. 1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 32MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber modules should have duplex LC connector to work with multi-mode fiber supporting minimum 300 meters for 10Gbps link and 100 meters for 100Gbps link.		Suggestion is accepted

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
191	Annexure-3	3.4.1.10. Network Core Switch	99 of 361	Core Switch should meet/exceed following performance parameters. 1) 80K MAC Addresses and 1K VLANs. 2) 25K ACLs, 30K Multicast and 80K IPv4, 80K IPv6 Routes. 3) Application visibility and traffic monitoring with minimum 60 K sflow/jflow/netFlow entries. 4) 200Gbps/more bidirectional stack throughput.	**Please change 25K ACLs to 7K ACLs and 60K sflows to 32K sflows.** Core Switch should meet/exceed following performance parameters. 1) 80K MAC Addresses and 1K VLANs. 2) 7K ACLs, 30K Multicast and 80K IPv4, 80K IPv6 Routes. 3) Application visibility and traffic monitoring with minimum 30 K sflow/jflow/netFlow entries. 4) 200Gbps/more bidirectional stack throughput.		Already answered in S.No. 365
192	Annexure-3	3.4.1.10. Network Core Switch	99 of 361	Core Switch should support following Layer 2 , Layer 3, Security and other features. 1) Virtual Switching/Stack/Equivalent features allows links that are physically connected to two different switch to appear as a single port channel. 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae (256-bit and 128-bit AES), 802.3x, 802.1p, 802.1Q, 1588v2. 3) AES-256 support with MACSEC-256 encryption algorithm on hardware. 3) BGP, MPLS, IS-IS, VRF, VXLAN, NAT, OSPF Routed Access, Policy-Based Routing (PBR), PIM SM, and Virtual Router Redundancy Protocol (VRRP). 4) 802.1p class of service, marking, classification, policing and shaping. Should support strict priority queuing. 5) port security, DHCP snooping, Spanning tree root guard, First Hop Security. 6) IPv6 support in hardware, providing wire rate forwarding for IPv6 network. 7) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment.	Please remove MACsec.		Already answered in 366

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
193	Annexure-3	3.4.1.11. Access Switch LAN	101 of 361	Access Switch should support following Layer 2 , Layer 3, Security and other features. 1) Switch should have dedicated slot for modular with dedicated stacking throughput and should support up to 8 switches in a stack 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q 3) AES-128 support with MACSEC-128 encryption algorithm on hardware all ports. 3) Static routing, RIP, REP PIM, OSPF, VRRP, PBR and QoS. 4) 802.1p class of service, marking, classification, policing and shaping and eight egress queues. 5) IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard. 6) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. 7) Should be SDN ready with VXLAN and VRF	**Allow virtual stacking throgh front panel ports. Please remove MACsec. Arista provides equivalenr features for the IPv6 security features.** Access Switch should support following Layer 2 , Layer 3, Security and other features. 1) Switch should have should support up to 8 switches in a stack 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q 3) Static routing, RIP, REP PIM, OSPF, VRRP, PBR and QoS. 4) 802.1p class of service, marking, classification, policing and shaping and eight egress queues. 5) IPv6 Binding Integrity Guard or equivalent, IPv6 Snooping or equivalent, IPv6 RA Guard, IPv6 DHCP Guard or equivalent, IPv6 Neighbor Discovery Inspection or equivalent and IPv6/IPv4 Source Guard. 6) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. 7) Should be SDN ready with VXLAN and VRF		Already answered in S.No. 367
194	Annexure-3	3.4.1.15. Data Center Leaf Switch	109 of 361	Performance & Scale: 1) Support non-blocking Layer 2 switching and Layer 3 routing. capable to function in line rate for all ports. 2) should be able to re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP). 3) Support minimum 1000 VRF instances with route leaking functionality, 1700K IPv4 LPM routes, minimum 3.6 TBPS of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) and should support intelligent buffer management with a minimum buffer of 40MB. 4) Should support minimum 90k of MAC addresses	**Please change 1000 VRFs to 500 VRFs. 1700K IPv4 LPM routes to 384K IPv4 LPM routes. 40MB buffer to 32 MB buffer.** Performance & Scale: 1) Support non-blocking Layer 2 switching and Layer 3 routing. capable to function in line rate for all ports. 2) should be able to re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP). 3) Support minimum 500 VRF instances with route leaking functionality, 384K IPv4 LPM routes, minimum 3.6 TBPS of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) and should support intelligent buffer management with a minimum buffer of 32MB. 4) Should support minimum 90k of MAC addresses		Already answered in S.No. 368

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
195	Annexure-3	3.4.1.15. Data Center Leaf Switch	111 of 361	Security: 1) Support control plane Protection from unnecessary or DoS traffic by control plane protection policy. 2) Support for external database for AAA using TACACS+ & RADIUS. 3) support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding. 4) VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware. 5) Support for Role Based access control (RBAC) for restricting host level network access as per policy defined. 6) support DHCP Snooping, dynamic ARP Inspection, IP Source Guard and unicast and/or multicast blocking on a switch port. 6) Support to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 7) Support broadcast, multicast and unknown unicast storm control. 8) LLDP, MAC Sec (802.1AE) in hardware and Spanning tree BPDU protection.	**Please remove MACsec. DAI to DAI or equivalent.** Security: 1) Support control plane Protection from unnecessary or DoS traffic by control plane protection policy. 2) Support for external database for AAA using TACACS+ & RADIUS. 3) support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding. 4) VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware. 5) Support for Role Based access control (RBAC) for restricting host level network access as per policy defined. 6) support DHCP Snooping, dynamic ARP Inspection or equivalent, IP Source Guard and unicast and/or multicast blocking on a switch port. 6) Support to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 7) Support broadcast, multicast and unknown unicast storm control. 8) LLDP, and Spanning tree BPDU protection.		Already answered in S.No. 369
196	Annexure-5-Demand-Capacity	5.1.4	7	Line items Security Operations Center, Network Operations Center and Administrators.	As per this clause SOC Agents, NOC Agents and Adminstrators coming under MSP. But in SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement clause 10.1 and SL-UDI-Volume-02-of-03-Annexure-12-Project-Sites-and-Sites clause 12.1, the same is coming under the responsibility of MSI. Please clarify ?		This is now the responsibility of GoSL and the same is dropped from the responsibility of MSI as mention id Annexure 10
197	Annexure-6-Exit-Management	6.2	143	Line item 14 Transition and Exit Management {Commence After T+ 44}	As per this requirement Exit Management period is 4 months, but in Annexure 6-Exit Management it is mentioned as 3 months. Which one is to be considered ?		Please consider as 3 months
198	Volume - 2	7	158, 159, 160	Items under IT Infrastructure, Field Infrastructure and Mobile Units.	In this section under IT Infrastructure, Field Infrastructure and Mobile Units, certain number of units are given agaist each component. Do we need to consider and supply the same number of quantity ? Confirm the exact quantity for field infrastructure and mobile units		Please see the revised RFP where correct number are mentioned
199	Volume - 2	3.1	15	Provisioning of the bandwidth and its commissioning and recurring charges shall be borne by GoSL during implementation and post-implementation phase. MSI will assist in establishing the connectivity between DC and DRC.	As per this clause, Provisioning of the bandwidth and its commissioning and recurring charges shall be borne by GoSL during implementation and post-implementation phase. But in Clause 7 under Network Connectivity, the same is requested from MSI. Who will bear the bandwidth charges ?		Provsioning of bandwidth is the responsbility of GoSL
200	Volume - 2	7	161	89. Internet Connectivity for mobile registration centers	Under Network Connectivity, Internet Connectivity for mobile registration centers is sought. Please clarify the same as dongle from telecom service provider for internet connectivity is also an ask from rfp.		Dongles are to provided by GoSL
201	Volume - 2	5.2.2	50	Service Creation - The necessary service creation environment for solution should be created in Primary Site as well as Disaster Recovery Site	What is Service Creation Environment in DC & DR ?		This requirement of service creation is dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
202	Volume - 2	5.2.2	50	The necessary testing & quality assurance environment for solution should be created in Primary Site as well as Disaster Recovery Site	Testing & QA environment is in DC and DR sites in Sri Lanka while development environment is in offshore (india). In this case, for testing and deploying the deliverables MSI need access to DC and DR (All the environments) from offshore till MSP takes over. Please confirm.		Yes this shall be provided . However the selected MSI shall discuss the modalites with GoSL
203		5	24	Identity Management System Identity and Access Management System	Identity Management system is being asked for MOSIP and also under COTS components. Do we need to supply and maintain 2 different Identity management systems or single Identity and access management is sufficient ? Please clarify.		No . It will come from MOSIP.
204	Annexure 10: Manpower Requirement	10.2	24	Track Lead – Data Centre Manager Note – This profile should be from the data center co-location provider in Sri Lanka.	Data center space is provided by GoSL. In this case GoSL appointed Data center provider only can fill this position. Please calrify if MSI has to bring in there own resource or the same would be provided by GoSL.		MSI may take call on this profile as the case may require.
205	Volume - 1	3.1.5	33	Local Presence of the Bidder The successful bidder should have a registered business presence in India and should agree to establish a project office with adequate staff and resources before the commencement of works in Sri Lanka, which should continue to be in operation for the duration of the contract for implementation, providing support for project management, providing technical support and maintenance of the system.	As per below Annexure 10 - Manpower Requirements, facility will be provided by GoSL for onsite position. In this case the purpose of Local presence by having project office is not clear and it is contradicting with the below requirements. **10.3.1 Guidelines for Staffing and Provisioning of Manpower** **i) Implementation of SL-UDI is envisaged offsite at SI's premises wherein, a dedicated** **core team shall be stationed at the Purchaser's premises while the development will** **take place in an offshore location.** **10.3.6 Role of GoSL and Responsibilities** **During project duration, GoSL shall have following roles and responsibilities:** **i) If onsite presence is required, GoSL will provide basic office amenities to the MSI's** **personnel at its office locations for performing their part of the obligations. MSI will** **not be entitled to any facilities beyond the contractual time frame.** **Please confirm that GoSL will provide the facility to depute MSI resources for entire duration of the project.**		Please refer to Annexure 10 section 10.3.6
206	Annexure 10: Manpower Requirement	10.3.1	48	vi) Key roles in the MSI's team should be held only by Permanent employees of the MSI	Please confirm the list of Key Roles.		Please refer to Volume 02 of 03 - Annexure 10: Manpower Requirements Table of Professional Staff and Engagement Approach . The table hads a col of Key Roles required. Please note that they have to be deployed as per the deployment plan of the MSI.
207	Annexure 10: Manpower Requirement	10.1	4	D. Engineers 3. CRM Engineer 4. BI & Analytics Engieer 5. Application Engineer	Only "Full Time" mentioned in the implementation phase. Please confirm whether they need to be in onsite or offshore. Application engineers may not be required during implementation phase as the support starts once the system go-live.		MSI has to deploy them accroding to its own deployment plan,.
208	Annexure 3: Minimum Technical Specification	3.3.3.14	61,62	SMS Gateway	SMS cost is the responsibility of GoSL as per Volume 2 requirements. In this case MSI to consider this section and is expected to find out and onboard SMS gateway services provider or GoSL will onboard them ?		Yes MSI has to onboard SMS gateway servcie provider . The SMS cost will be borne by GoSL.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
209	Annexure-5-Demand-Capacity	5.1.1 5.1.2	3	Total expected registrations	During site visit ICTA mentioned 30 million to be considered for MOSIP and Biometric ABIS sizing. Please confirm ?		Yes correct
210	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.2 Product Benchmarking	3	a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory.	We understand that the ask is to position all tools and technologies which are in the Leader's quadrant of Gartner.As discussed during SL visit, ICTA highlighted that they prefer Opensource products with Enterprise support. As all the Opensource Products with Enterprise support may not appear in the Gartner/IDC/Forester reports, we request to remove the requirement for Gartner/IDC/Forester reports. Please note that to integrate the various tools and to fast track the Implementation a technology aggegator which will also work as an accelerator will be beneficial to the project hence let us know if bidder is allowed to propose bidder's Pre existing IPR as a Technology aggregator and accelerator with proven credentials in variuous digital transformations in India Govt. implentations as well as with global customers.		Open source tool is accepatble with enterprise support
211	Volume-2	3.4.2.1 Virtualization Platform, point no 3	121	Provide the ability to hot-add CPU and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system).	Please remove this clause to avoid being locked into a specific vendor, since the Hot Add CPU feature is unique to Hyper-V and Vmware		Please read the clause as "The virtualization platform must support dynamic scaling of compute, storage, and network resources with minimal or no service interruption.”
212	Volume-2	5.8.2 Business Continuity and Disaster Recovery, Point No. - 7 (iii)	86	The Primary and Secondary sites will be configured in an Active-Active (for citizen facing applications, CRM, email, etc.) and Active-Passive mode (for other applications).	It is clear from the statement thet RPO/RTO will be "0" for citizen facing applications, CRM, email, etc. but what will be the RPO & RTO values for other applications configured in Active-Passive mode?		Please refer to Aneexure 16 for RPO and RTO values
213			115		"The solution shall have integration with Kubernetes Platforms and requisite controller/license/container plugin shall be provided with LB solution from day one. Controller/Plug-in should be from same make as LB. It should not be third party or opensource."		This query not clear
214	Annexure 3	3.4.1.17 Server Load Balancer, Point No 4	115	Solutions should support active-active and active-backup high availability from day 1	The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to acheive horizontal scaling.		This query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
215		3.4.1.17 Server Load Balancer, Point No 1	115	Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)	The proposed solution must handle high-capacity traffic, including L7 requests per second: 450K L4 connections per second:150K concurrent L4 connections:18M L4 throuput 20 Gbps on day 1 and scalable upto 25 Gbps		The SL UDI system does not host heavy public-facing web applications that require application acceleration or SSL offload. The platform already uses an API Gateway and standard L7 load balancing, which provide the necessary routing and security. An ADC like F5 or Citrix would duplicate these functions and add unnecessary cost and complexity. ***Therefore, a dedicated application delivery controller is not required for the UDI project.***
216	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	Proposed object storage should be able to consume storage capacity from the provisioned erasure coded storage nodes,block (SAN) storage, file (NAS) storage, public cloud storage or an S3 compatible storage.	This contradicts the appliance-based object storage requirement. As appliances have their own capacity and features, this compliance point should be removed.		Agreed. This requirement is not needed because the UDI platform only requires a reliable, scalable S3-compatible object storage, and it will already run on dedicated storage provisioned for the project. . Therefore, this multi-backend storage flexibility is not required for the UDI project
217	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	Object storage must support multiple replication topologies: active-active, active-passive, one-to-many, many-to-one, ring, and chain.	This contradicts the appliance-based object storage requirement. As appliances have their own capacity and features, this compliance point should be removed.		Agreed.
218	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	Erasure coding must provide protection against 6 or more disk failures and at least 1 node failure, with rebuilds occurring within the same site to preserve WAN bandwidth	This appears vendor-specific. NetApp supports up to 2 disk-drive failures per node. Clarification on business and technical use case is needed.		Agreed. . A standard, reliable S3-compatible object store with normal redundancy (e.g., 2- or 3-way replication or simple erasure coding) is sufficient for UDI workloads. Therefore, this high-level erasure-coding requirement is **not needed** for the UDI project.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
219	Annexure-3	3.4.1.1 Blade Servers &	79	Blade server should be proposed with the latest generation x86 Intel/AMD processors Should be quoted with minimum 2 x 16 Core processors with minimum 2.8Ghz of clock cycle	We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support.		Agreed. "Either Intel or AMD latest-generation processors" is sufficient to avoid architecture conflicts. Hence rwe do not mandate both CPU types for blade environments.
220	Annexure-3	3.4.1.2 Rack Servers	81	Blade server should be proposed with the latest generation x86 Intel/AMD processors Should be quoted with minimum 2 x 16 Core processors with minimum 2.8Ghz of clock cycle	We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support.		Agreed . Please refer to answer at Sr No 220
221	Volume 02 of 03	3.4.1.1 Blade Servers &	80	5. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade	Our latest blades do not provide a native converged NIC option delivering 100 Gbps per blade. However, with blade platforms achieve aggregated bandwidth through the interconnect modules with SDN capabilities (, which virtualize and pool uplink bandwidth across multiple blades. Furthermore, provisioning 100 Gbps per blade is not practically required when considering the switching specification requested below, as total bandwidth is determined by uplink capacity of the TOR/core switches and the aggregate design of the data center fabric. In typical deployments, per-blade bandwidth demand is well within 25–50 Gbps, with redundancy and aggregation handled at the interconnect/fabric level. Thus, the functional requirement for bandwidth resiliency and scalability is fully met without a native 100 Gbps converged NIC. We request amendment of the clause to recognize bandwidth aggregation via backend interconnect modules as meeting the requirement, at the interconnect/fabric layer, aligned with industry best practices.		Agreed. The functional requirement for bandwidth, failover, and scalability can be fully met without a native 100 Gbps converged NIC, and the MSI's suggestion to amend the clause is accepted.
222	Volume 02 of 03	3.4.1.3 Blade	83	2.Blade enclosure should support all x86 based Intel/AMD processor blade servers	As per the query shared for section 3.4.1.1. We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support. We therefore propose to comply with the latest generation of [Intel/AMD] processors validated for the blade family		Agreed . Please refer to answer at Sr No 220
223	Annexure-3	3.4.1.5-SAN Storage	87-88	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. In case of non-native/external component used, it should be supplied in redundant mode with no single point of failure.	This appears vendor-specific. Clarification on business and technical use case is needed.		Agreed. Because UDI will use its own dedicated storage and does not need to virtualize or aggregate old third-party arrays. The clause / or requirement is therefore dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
224	Volume 02 of 03	3.4.1.6 SAN S	92	11.The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model	Switches based on Brocade support frame-based trunking of up to 8 physical 64G FC ports per trunk, providing up to 512 Gbps aggregated bandwidth. This trunking is frame-based, ensuring even distribution of traffic across all trunked links, and does not require ports to be consecutive. While the RFP clause specifies 16 ports, OEM validation and industry standards in SAN fabrics currently limit the maximum aggregation to 8 ports per trunk. We request amendment of the clause to reflect up to 8 ports per trunk as per OEM design.		Agreed . The requirement for aggregating 16 FC ports is dropped.
225	Volume 02 of 03	3.6.2.1 Blade	346	1.Blade enclosure Should occupy a max of 8RU rack height, supporting a minimum 8 half height/4 Full height modular server per blade chassis	Most of the new blade enclosures supports up to 12 half-height or 6 full-height modular servers per chassis, exceeding the minimum capacity requirement. The enclosure occupies 10U rack height, which is slightly higher than the specified 8U. This is due to composable design, which integrates compute, storage, fabric interconnects, and management modules into a single frame, enabling higher density and scalability compared to traditional blade chassis. We request amendment of the clause to accept 10U rack height enclosures. Also this exceeds the required compute density (12 half-height vs. 8, 6 full-height vs. 4) while delivering additional composability and integration benefits.		Agreed. Accepting **10U enclosures** is fine as it aligns aligned with current industry standards.
226	Volume 02 of 03	3.6.2.2 Blade	349	5.The Blade server should support Converged Network Adapters. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade	Our latest blades do not provide a native converged NIC option delivering 100 Gbps per blade. However, with blade platforms achieve aggregated bandwidth through the interconnect modules with SDN capabilities (, which virtualize and pool uplink bandwidth across multiple blades. Furthermore, provisioning 100 Gbps per blade is not practically required when considering the switching specification requested below, as total bandwidth is determined by uplink capacity of the TOR/core switches and the aggregate design of the data center fabric. In typical deployments, per-blade bandwidth demand is well within 25–50 Gbps, with redundancy and aggregation handled at the interconnect/fabric level. Thus, the functional requirement for bandwidth resiliency and scalability is fully met without a native 100 Gbps converged NIC. We request amendment of the clause to recognize bandwidth aggregation via backend interconnect modules as meeting the requirement, at the interconnect/fabric layer, aligned with industry best practices.		Therefore, the MSI's request to amend the clause to 8 ports per trunk is technically accurate, aligned with OEM capabilities, and reflects real industry standards.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
227	Volume 02 of 03	3.6.2.3 Rack S	350	9.KVM Connector	Modern blade platforms, are designed with a composable architecture and integrated management systems. These provide full software-defined remote console access from hardware to operating system level, making physical KVM connectors unnecessary. All provisioning, troubleshooting, and lifecycle management can be performed via the embedded management platform which offers secure remote graphical console access equivalent to — and more efficient than — a physical KVM. We request amendment of this clause to accept software-defined management with integrated remote console as an alternative to physical KVM connectors. Physical KVM ports are no longer required in modern composable blade platforms, as full hardware-to-OS console access is natively available.		Agreed.Accepting software-defined remote console instead of a physical KVM port is correct and fully aligned with current industry standards.
228	Volume 02 of 03	3.6.2.3 Rack S	350	10.G200e video/graphics controller	Modern Blade compute modules do not include a discrete G200e graphics controller. Instead, they provide integrated video via management, which fully supports remote console, BIOS-level access, and OS deployment. This design aligns with composable, software-defined architecture, where physical VGA controllers are no longer required. If application-level graphics acceleration is needed, blades support via dedicated GPU modules (e.g., NVIDIA), which provide far greater performance than legacy G200e controllers. We request amendment of the clause to accept integrated onboard-based video and console access in place of a G200e controller. Modern blade compute nodes are designed for composable infrastructure and do not rely on legacy embedded VGA controllers.		Agreed. MSI request is accepted of onboard video and remote console instead.
229	Volume 02 of 03	3.6.2.5	359	42.The offered storage solution must be able to cater to file, block, and object workloads	"Block- and object-based enterprise storage platform. File protocols such as CIFS, NFS, FTP, HTTP, Telnet, and NDMP are not applicable to block storage arrays. These services are typically delivered via file servers, gateways, or archival/object storage platforms, which the RFP has separately requested. Implementing such protocols at the block-storage layer would not align with best practices, as they add unnecessary overhead and security exposure (e.g., telnet/FTP are legacy and insecure). Instead, access control and protocol support are handled at the application or file/object layer — in this case, the TCS application architecture will dictate integration with the file/archival solution. We request clarification and amendment of this clause to exclude block storage systems from requirements such as CIFS/NFS/telnet/http/https/ftp/ssh/NDMP. These protocols are supported in the file and archival platform requested separately in the RFP, and are not relevant to enterprise block storage platforms."		Agreed. the MSI's request to amend the clause and exclude file-protocol requirements from block storage is accepted

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
230	Volume 02 of 03	3.6.2.6 SAN	360	11.The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model.	"Switches based on Brocade support frame-based trunking of up to 8 physical 64G FC ports per trunk, providing up to 512 Gbps aggregated bandwidth. This trunking is frame-based, ensuring even distribution of traffic across all trunked links, and does not require ports to be consecutive. While the RFP clause specifies 16 ports, OEM validation and industry standards in SAN fabrics currently limit the maximum aggregation to 8 ports per trunk. We request amendment of the clause to reflect up to 8 ports per trunk as per OEM design. "		Agreed. MSI's request to amend the clause to **8 ports per trunk** is accepted
231	Volume 02 of 03	3.4.1.4 Stora	85	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.	Different software-defined object storage vendors have different scaling mechanisms for capacity and availability. For us a deployment can start with as few as 3 nodes (e.g. with 16×20 TB drives = 538 TB usable Day-1). By simply adding drives, the same 3-node cluster can scale to over 1 PB within the first year. The requirement for a minimum of 4 nodes is not necessary to achieve 500 TB Day-1 capacity or 1 PB scalability — we can provides this even with 3 nodes. Additionally, availability and fault tolerance are ensured: the platform can tolerate one node failure plus drive failures while continuing to serve data. The "pre-integrated appliance" condition is restrictive. Modern object storage is delivered as a software-defined platform, giving customers flexibility in hardware choice while still maintaining OEM validation and support. We request clarification and amendment of this clause: •Remove the "pre-integrated appliance" requirement. •Recognize that a 3-node starting configuration provides the required 500 TB Day-1 usable capacity and can scale to 1 PB within one year. •Confirm that availability requirements are met, as the solution provides tolerance against one node and multiple drive failures.		Agreed. Modern object storage platforms are software-defined and do not require a fixed "pre-integrated appliance" The ammendement is accepted.
232	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	Erasure coding must provide protection against 6 or more disk failures and at least 1 node failure, with rebuilds occurring within the same site to preserve WAN bandwidth	This appears vendor-specific. NetApp supports up to 2 disk-drive failures per node. Clarification on business and technical use case is needed.		Agreed. This requirement is dropped.
233	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	The proposed array must provide continuous monitoring and movement of sub-LUN data chunks to provide real-time performance improvements	This appears vendor-specific. Clarification on business and technical use case is needed.		Agreed. This requirment is drop
234	Annexure-3	3.4.1.6 SAN Switch	91-92	The switch(or director platform) must be able to provide up to 96 number - 64Gbps FC or 10-Gbps full line-rate autosensing Fibre Channel physical ports from day1. System should be scalable to support upto 384port or more.	Clarify the need for 384 ports. Director-level switches add significant cost and may not be necessary for the required capacity.		The MSI has to decide to scalibility, however the Systems should be scalable upto minimum 128

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
235	Annexure-3	3.6.2.5 SAN (in case separate hardware is required)	359	The offered storage solution must be able to cater to file, block, and object workloads	Object workloads, however, are fundamentally different from file and block storage. They are best handled by specialized platforms.Object may dilute performance of block/file if not on specialized engine Higher complexity to manage all 3 in one		Agreed. This requirment is drop
236	Annexure-3	3.4.1.7 TAPE	93	Tape Library	Request to remove this since back up can be achieved in VTL itself		Tape library is retained. VTL is dropped
237	Annexure-3	3.4.3.15 SSL V	232	SSL VPN / IPsec VPN with High Availability	This functionality can be achieved with the external firewall itself.		Requirement remains unchaged
238	Annexure-3	3.4.2.12 PROJECT MANAGEME NT TOOL	163		Request to remove the Gartner/Forrester/IDC rating for this as this is not available		Agreed
239	Annexure-3	3.4.2.2 Backu	127	Licensing: The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied having License for min. 250 VM's should be included and backup appliance should be provided with 500TB capacity from Day1.	The 500 TB capacity includes both virtual machine (VM) and Kubernetes (K8s) backups.		Agreed.
240	Annexure-3	3.4.2.11 ITSM		The solution should allow easy configuration of polling frequency till per second scenario.	Request to change this polling interval supported to 1 minute.		agreed . 30-second to 1-minute polling is acceptable
241	Annexure-3	3.4.2.11 ITSM		The solution should generate alarms based on what is currently mounted compared with what is configured on a defined compliant system.	Request to Eloborate more on this.		This is not mentioned in the specifcations.
242	Annexure-3	3.4.2.11 ITSM		The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: a. Event Filtering b. Event aggregation c. Event Masking	To Check		The query is not clear
243			116-117		"The device should support 'n' number DNS QPS"		Proper refrencing is required
244			116-117		"Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS and Must support resolution for A, AAAA, MX, and NS queries as External DNS"		Proper refrencing is required
245			232	Support for VRRP, QoS and full OSPF routing protocol.	"Support for VRRP or equivalent protocols"		Agreed - VRRP or Equivalent Protocol..
246			242	11. RAM 64 GB	"11. RAM 128 GB"		Agreed.
247	Annexure-3	3.4.2.2 Backup and Security	128		What is the selected hypervisor for running VMs		MSI should propose industry standard hypervisor with enterprise support

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
248	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Kubernetes distribution and version used to run containers		MSI to propose
249	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Total Kubernetes clusters:		MSI to propose
250	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Total worker nodes across all clusters		MSI to propose
251			53	The proposed solution shall provide API Lifecycle maintenance capabilities including definition, creation, security, monitoring and management	"The proposed solution shall provide API Lifecycle maintenance capabilities including definition, security monitoring and management."		The condition remains
252			53	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.	"The proposed solution shall have the capability to externalise APIs and should provide cataloguing capabilities with third party integrations."		Yes Agreed
253	Annexure-3	3.4.1.4-Object Storage Compliance	85-86	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.	Any distributed storage architecture starts with min 3Storage Nodes. Every storage OEM has its own architecture to ensure High Availability and Durability. NetApp can ensure the solution is optimized for availability. Number of active nodes should be left to storage OEM as per their best practices/guidelines.		Answered in S.No. 231

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
254	Annexure-3	3.4.1.6-SAN Storage	87-88	SAN Storage Capacity	No visibility on SAN Storage capacity requirements. Clarify if this is for single site or multi-site deployment.		Please refer to key sizinf=z parameter . Number of Copies (HDFS)3 Number of Copies (Archival)1 Number of Copies (HDFS + Archival)4 Enrolment Packet (MB)5 Enrolment Data Size Per Person (MB) - One Copy5 Enrolment Data Size Per Person (MB) - All Copies Population Size (in Million)30 Raw Storage with 30% Overheads Raw Storage with Head Room of 15% Storage (RAID 10) Multiplication Factor 1.50
255	Annexure-3	3.3.2.18 EMA	66		Pls provide No. of users/ Mailboxes/ Mailbox size and archive for how many time		This requirement is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
256	Volume 02 of 03	3.4.1.1	79	1.Blade server should be proposed with the latest generation x86 Intel/AMD processors	Blade platforms are engineered and validated around a specific CPU vendor (Intel or AMD) per generation. While both Intel and AMD are x86, OEM vendors (HPE, Dell, Lenovo, etc.) do not support mixing architectures across a blade family for the following reasons: 1.Chassis Compatibility – A blade chassis is designed with interconnect modules, backplane, and management firmware aligned to a single CPU architecture. Introducing a different CPU family would require separate validation and firmware paths, which vendors do not support. 2.Lifecycle Management – Firmware, BIOS, drivers, and system ROMs differ significantly between Intel and AMD. Running both architectures in the same enclosure would create dual update streams, increasing complexity and operational risk. 3.Resource Pooling & Interoperability – Blade environments rely on pooled resources (power, cooling, interconnects, management). Uniformity of CPU family ensures consistent performance and workload placement. Mixed CPU vendors break this design principle. 4.Industry Best Practice – Standardization on one CPU family within a blade environment is recommended to ensure stability, vendor support, and easier integration with hypervisors (VMware, Hyper-V, etc.), which have licensing and NUMA optimization differences per CPU vendor We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support. We therefore propose to comply with the latest generation of [Intel/AMD] processors validated for the blade family		The asnwer is provided earlier
257	Volume 02 of 03	3.4.1.1	80	4.Required Minimum 6 number of drives-	The specified minimum of 6 drives does not align with available blade configurations. Our platform supports either 4x SFF drives or 8x EDSFF drives. In blade environments, these internal drives are typically used only for operating system installation or boot partitions, while production workloads and data are hosted on external SAN/NAS storage. Therefore, the proposed configuration fully meets the functional requirement, while providing equivalent or greater performance and capacity. We request amendment of the clause to allow configurations of either 4x SFF or 8x EDSFF drives. These are OEM-validated configurations and are sufficient for OS installation and boot purposes, with production storage hosted externally as per best practice in blade server deployments and while aligning with RFP requirement as well		Answer is already provided

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
258	Volume 02 of 03	3.4.1.1	80	5. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade	Our latest blades do not provide a native converged NIC option delivering 100 Gbps per blade. However, with blade platforms achieve aggregated bandwidth through the interconnect modules with SDN capabilities (, which virtualize and pool uplink bandwidth across multiple blades. Furthermore, provisioning 100 Gbps per blade is not practically required when considering the switching specification requested below, as total bandwidth is determined by uplink capacity of the TOR/core switches and the aggregate design of the data center fabric. In typical deployments, per-blade bandwidth demand is well within 25–50 Gbps, with redundancy and aggregation handled at the interconnect/fabric level. Thus, the functional requirement for bandwidth resiliency and scalability is fully met without a native 100 Gbps converged NIC. We request amendment of the clause to recognize bandwidth aggregation via backend interconnect modules as meeting the requirement, at the interconnect/fabric layer, aligned with industry best practices.		Answer is given above.
259	Volume 02 of 03	3.4.1.2	82	8.Min 4 ports per storage controller.(not clear	We recommend to request m		Query is not clear
260	Volume 02 of 03	3.4.1.2	82	9.front KVM Connector	Modern blade platforms, are designed with a composable architecture and integrated management systems. These provide full software-defined remote console access from hardware to operating system level, making physical KVM connectors unnecessary. All provisioning, troubleshooting, and lifecycle management can be performed via the embedded management platform which offers secure remote graphical console access equivalent to — and more efficient than — a physical KVM. We request amendment of this clause to accept software-defined management with integrated remote console as an alternative to physical KVM connectors. Physical KVM ports are no longer required in modern composable blade platforms, as full hardware-to-OS console access is natively available.		Agreed
261	Volume 02 of 03	3.4.1.3	83	2.Blade enclosure should support all x86 based Intel/AMD processor blade servers	As per the query shared for section 3.4.1.1. We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support. We therefore propose to comply with the latest generation of [Intel/AMD] processors validated for the blade family		Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
262	Volume 02 of 03	3.4.1.3	84	6.The chassis cooling should be modular so that future enhancements can potentially handle open- or closed-loop liquid cooling to support higher-power processors	Current-generation blade platforms are designed with high-efficiency air-cooled modules that provide N+1 redundancy and scalable cooling for supported processors. The architecture does not support modular liquid cooling (open- or closed-loop) at the chassis level. OEM validation and long-term support are based on air cooling with optimized airflow and smart fan control. While liquid cooling is emerging in some rack-based HPC **systems where GPU processing is** required , it is not available or required for blade environments. We request amendment of the clause to accept high-efficiency air-cooled redundant modules as the validated and supported design for current blade platforms		Agreed
263	Volume 02 of 03	3.4.1.5	88	11.Storage should be supplied with Unlimited capacity of virtualization license for existing storage.-	We request to share the requirement of the virtualization license, since operational requirement is not clear.		Detailed solution will be designed and implemented by the MSI. The Storage should allow creation of as many virtual machines as would be required for successfully implementing the solution
264	Volume 02 of 03	3.4.1.6	92	11.The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model	Switches based on Brocade support frame-based trunking of up to 8 physical 64G FC ports per trunk, providing up to 512 Gbps aggregated bandwidth. This trunking is frame-based, ensuring even distribution of traffic across all trunked links, and does not require ports to be consecutive. While the RFP clause specifies 16 ports, OEM validation and industry standards in SAN fabrics currently limit the maximum aggregation to 8 ports per trunk. We request amendment of the clause to reflect up to 8 ports per trunk as per OEM design.		Already answered in S.No. 224
265	Volume 02 of 03	3.4.1.8	95	10.Must support point-in-time copies of a LUN or volumes with minimal performance impact	The term “point-in-time copies” is ambiguous and requires clarification. Industry best practice — is to use storage-based snapshots rather than full physical copies. Snapshots create lightweight, space-efficient point-in-time images that have minimal performance impact and also benefit from data reduction technologies (deduplication and compression). Full LUN/volume copies, by contrast, would introduce heavy I/O load and are not recommended for production environments. We request clarification whether “point-in-time copies” refers to snapshots. We recommend aligning with industry best practice and OEM guidance to use snapshot-based copies, which provide the same functionality with minimal performance impact, effective data reduction, faster recovery and **also to consider the ransomware protection and detection mechanisom of snapshots.**		VTL product is dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
266	Volume 02 of 03	3.4.1.8	95	11.Must supports communications and data transfers through 2x4GB/2x8GB FC SAN, 4 x 1 Gb/4x10Gb Ethernet LAN	The RFP references legacy data transfer standards (4/8 Gb FC, 1 GbE, 10 GbE). Modern blade and SAN platforms, have phased out these older speeds in favor of current industry standards such as 16G/32G FC and 10/25 GbE. These provide significantly higher throughput, lower latency, and future scalability, while maintaining backward compatibility with older environments through auto-negotiation. Supporting outdated interfaces would limit long-term performance and investment protection. We request amendment of the clause to accept 16G/32G Fibre Channel and 10/25 GbE Ethernet connectivity, which are the validated and supported options in current-generation SAN, and blade networking platforms. These interfaces ensure higher performance and longevity while remaining interoperable with existing infrastructure.		VTL product is dropped
267	Volume 02 of 03	3.4.1.8	96	24.Must support ACL for CIFS/NFS/telnet/http/https/ftp/ssh	Block- and object-based enterprise storage platform. File protocols such as CIFS, NFS, FTP, HTTP, Telnet, and NDMP are not applicable to block storage arrays. These services are typically delivered via file servers,		The product VTL is dropped
268	Volume 02 of 03	3.4.1.8	96	30.Should have inbuilt NDMP tape server.			The product VTL is dropped
269	Volume 02 of 03	3.6.2.1	346	1.Blade enclosure Should occupy a max of 8RU rack height, supporting a minimum 8 half height/4 Full height modular server per blade chassis	Most of the new blade enclosures supports up to 12 half-height or 6 full-height modular servers per chassis, exceeding the minimum capacity requirement. The enclosure occupies 10U rack height, which is slightly higher than the specified 8U. This is due to composable design, which integrates compute, storage, fabric interconnects, and management modules into a single frame, enabling higher density and scalability compared to traditional blade chassis. We request amendment of the clause to accept 10U rack height enclosures. Also this exceeds the required compute density (12 half-height vs. 8, 6 full-height vs. 4) while delivering additional composability and integration benefits.		Answered above in S.No. 225

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
270	Volume 02 of 03	3.6.2.1	346	2.Blade enclosure should support all x86 based Intel/AMD processor blade servers	Blade platforms are engineered and validated around a specific CPU vendor (Intel or AMD) per generation. While both Intel and AMD are x86, OEM vendors (HPE, Dell, Lenovo, etc.) do not support mixing architectures across a blade family for the following reasons: 1.Chassis Compatibility – A blade chassis is designed with interconnect modules, backplane, and management firmware aligned to a single CPU architecture. Introducing a different CPU family would require separate validation and firmware paths, which vendors do not support. 2.Lifecycle Management – Firmware, BIOS, drivers, and system ROMs differ significantly between Intel and AMD. Running both architectures in the same enclosure would create dual update streams, increasing complexity and operational risk. 3.Resource Pooling & Interoperability – Blade environments rely on pooled resources (power, cooling, interconnects, management). Uniformity of CPU family ensures consistent performance and workload placement. Mixed CPU vendors break this design principle. 4.Industry Best Practice – Standardization on one CPU family within a blade environment is recommended to ensure stability, vendor support, and easier integration with hypervisors (VMware, Hyper-V, etc.), which have licensing and NUMA optimization differences per CPU vendor We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support. We therefore propose to comply with the latest generation of [Intel/AMD] processors validated for the blade family		Agreed
271	Volume 02 of 03	3.6.2.1	347	6.The chassis cooling should be modular so that future enhancements can potentially handle open- or closed-loop liquid cooling to support higher-power processors	Current-generation blade platforms are designed with high-efficiency air-cooled modules that provide N+1 redundancy and scalable cooling for supported processors. The architecture does not support modular liquid cooling (open- or closed-loop) at the chassis level. OEM validation and long-term support are based on air cooling with optimized airflow and smart fan control. While liquid cooling is emerging in some rack-based HPC **systems where GPU processing is** required , it is not available or required for blade environments. We request amendment of the clause to accept high-efficiency air-cooled redundant modules as the validated and supported design for current blade platforms		Answered above in S.No. 262. Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
272	Volume 02 of 03	3.6.2.2	348	1.Latest generation x86 Intel/AMD processors	As per the query shared for section 3.4.1.1. We request amendment of this clause to state either Intel or AMD latest-generation processors. Blade server platforms are validated and supported by OEMs with a single CPU vendor architecture. Mixing Intel and AMD processors across the same blade platform is not recommended or supported, as it introduces risks in firmware management, interoperability, and lifecycle support. We therefore propose to comply with the latest generation of [Intel/AMD] processors validated for the blade family		Agreed
273	Volume 02 of 03	3.6.2.2	349	4.The blade server should support min 6 no's of SAS/SSD/NVMe disk drive	The specified minimum of 6 drives does not align with available blade configurations. Our platform supports either 4x SFF drives or 8x EDSFF drives. In blade environments, these internal drives are typically used only for operating system installation or boot partitions, while production workloads and data are hosted on external SAN/NAS storage. Therefore, the proposed configuration fully meets the functional requirement, while providing equivalent or greater performance and capacity. We request amendment of the clause to allow configurations of either 4x SFF or 8x EDSFF drives. These are OEM-validated configurations and are sufficient for OS installation and boot purposes, with production storage hosted externally as per best practice in blade server deployments and while aligning with RFP requirement as well		The amendment of the clause to allow configurations of either 4x SFF or 8x EDSFF drives is agreed and the earlier sepc of 6 nos of drives is dropped.
274	Volume 02 of 03	3.6.2.2	349	5.The Blade server should support Converged Network Adapters. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 100Gbs bandwidth per blade	Our latest blades do not provide a native converged NIC option delivering 100 Gbps per blade. However, with blade platforms achieve aggregated bandwidth through the interconnect modules with SDN capabilities (, which virtualize and pool uplink bandwidth across multiple blades. Furthermore, provisioning 100 Gbps per blade is not practically required when considering the switching specification requested below, as total bandwidth is determined by uplink capacity of the TOR/core switches and the aggregate design of the data center fabric. In typical deployments, per-blade bandwidth demand is well within 25–50 Gbps, with redundancy and aggregation handled at the interconnect/fabric level. Thus, the functional requirement for bandwidth resiliency and scalability is fully met without a native 100 Gbps converged NIC. We request amendment of the clause to recognize bandwidth aggregation via backend interconnect modules as meeting the requirement, at the interconnect/fabric layer, aligned with industry best practices.		The Blade server should support Converged Network Adapters. The Converged Network Adapters should aggregate both the Ethernet and FC connectivity on a single fabric providing 25 Gbps - 50 Gbps bandwidth per blade.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
275	Volume 02 of 03	3.6.2.3	350	9.KVM Connector	Modern blade platforms, are designed with a composable architecture and integrated management systems. These provide full software-defined remote console access from hardware to operating system level, making physical KVM connectors unnecessary. All provisioning, troubleshooting, and lifecycle management can be performed via the embedded management platform which offers secure remote graphical console access equivalent to — and more efficient than — a physical KVM. We request amendment of this clause to accept software-defined management with integrated remote console as an alternative to physical KVM connectors. Physical KVM ports are no longer required in modern composable blade platforms, as full hardware-to-OS console access is natively available.		KVM and software defined both are acceptable
276	Volume 02 of 03	3.6.2.3	350	10.G200e video/graphics controller	Modern Blade compute modules do not include a discrete G200e graphics controller. Instead, they provide integrated video via management, which fully supports remote console, BIOS-level access, and OS deployment. This design aligns with composable, software-defined architecture, where physical VGA controllers are no longer required. If application-level graphics acceleration is needed, blades support via dedicated GPU modules (e.g., NVIDIA), which provide far greater performance than legacy G200e controllers. We request amendment of the clause to accept integrated onboard-based video and console access in place of a G200e controller. Modern blade compute nodes are designed for composable infrastructure and do not rely on legacy embedded VGA controllers.		Agreed
277	Volume 02 of 03	3.6.2.5	355	11.Storage should be supplied with Unlimited capacity of virtualization license for existing storage	We request to share the requirement of the virtualization license, since operational requirement is not clear.		Detailed solution will be designed and implemented by the MSI. The Storage should allow creation of as many virtual machines as would be required for successfully implementing the solution

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
278	Volume 02 of 03	3.6.2.5	359	42.The offered storage solution must be able to cater to file, block, and object workloads	"Block- and object-based enterprise storage platform. File protocols such as CIFS, NFS, FTP, HTTP, Telnet, and NDMP are not applicable to block storage arrays. These services are typically delivered via file servers, gateways, or archival/object storage platforms, which the RFP has separately requested. Implementing such protocols at the block-storage layer would not align with best practices, as they add unnecessary overhead and security exposure (e.g., telnet/FTP are legacy and insecure). Instead, access control and protocol support are handled at the application or file/object layer — in this case, the TCS application architecture will dictate integration with the file/archival solution. We request clarification and amendment of this clause to exclude block storage systems from requirements such as CIFS/NFS/telnet/http/https/ftp/ssh/NDMP. These protocols are supported in the file and archival platform requested separately in the RFP, and are not relevant to enterprise block storage platforms."		Agreed. the MSI's request to amend the clause and exclude file-protocol requirements from block storage is accepted
279	Volume 02 of 03	3.6.2.6	360	11.The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model.	"Switches based on Brocade support frame-based trunking of up to 8 physical 64G FC ports per trunk, providing up to 512 Gbps aggregated bandwidth. This trunking is frame-based, ensuring even distribution of traffic across all trunked links, and does not require ports to be consecutive. While the RFP clause specifies 16 ports, OEM validation and industry standards in SAN fabrics currently limit the maximum aggregation to 8 ports per trunk. We request amendment of the clause to reflect up to 8 ports per trunk as per OEM design. "		Answered as above in S.No. 230
280	Volume 02 of 03	3.4.3.30	290	All the electromc deaces xn SKY wtll share the Foposed UPS. Sundarly. all the electromc devtces in NOC Will share the	Aurora 1000VA/600W (Reason: As per the requirement, the expected output is 455W; however, our product currently delivers 360W.)		Query is not clear please repeat

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
281	Volume 02 of 03	3.4.1.4	85	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.	Different software-defined object storage vendors have different scaling mechanisms for capacity and availability. For us a deployment can start with as few as 3 nodes (e.g. with 16×20 TB drives = 538 TB usable Day-1). By simply adding drives, the same 3-node cluster can scale to over 1 PB within the first year. The requirement for a minimum of 4 nodes is not necessary to achieve 500 TB Day-1 capacity or 1 PB scalability — we can provides this even with 3 nodes. Additionally, availability and fault tolerance are ensured: the platform can tolerate one node failure plus drive failures while continuing to serve data. The “pre-integrated appliance” condition is restrictive. Modern object storage is delivered as a software-defined platform, giving customers flexibility in hardware choice while still maintaining OEM validation and support. We request clarification and amendment of this clause: •Remove the “pre-integrated appliance” requirement. •Recognize that a 3-node starting configuration provides the required 500 TB Day-1 usable capacity and can scale to 1 PB within one year. •Confirm that availability requirements are met, as the solution provides tolerance against one node and multiple drive failures.		Agreed. 3 Nodes strating configuration or above is acceptable provindg 500 TB and scalable to 1PB is acceptablke.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
282	Volume 02 of 03	3.4.1.4	85	Proposed object storage should be able to consume storage capacity from the provisioned erasure coded storage nodes, block (SAN) storage, file (NAS) storage, public cloudstorage or an S3 compatible storage.	Block, file, and object storage are fundamentally different protocols and architectures for writing and storing data. For an object storage requirement, and considering the operational requirements of this RFP, the recommended approach is to use a native object storage platform where data is inherently treated as objects at the storage OS layer. Many vendors that claim to support block, file, and object in the same storage system are actually running a block-based underlying mechanism, with file/object services layered as software add-ons. This approach increases complexity, reduces efficiency, and does not provide the same resiliency or scalability as true software-defined object storage. With our approach, capacity consumption is handled directly via erasure-coded nodes with native S3 support, ensuring high availability, scalability, and alignment with modern object workloads. File/NAS and block requirements are best addressed in their respective dedicated platforms, which the RFP has already called for (archival/file systems separately). We request clarification on this clause. We recommend aligning the object storage requirement with native object storage (S3 protocol) only, as block and file storage are separate paradigms already covered by other components of the RFP. This ensures optimal scalability, performance, and resiliency, avoiding inefficiencies associated with block/file/object convergence on a block-native system.		Agreed with the suggestion

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
283	Volume 02 of 03	3.4.1.4		Solution shall be provided at least 4 nodes with Read Only allowed after losing: Single Node.	Different software-defined object storage vendors have different scaling mechanisms for capacity and availability. For us a deployment can start with as few as 3 nodes (e.g. with 16×20 TB drives = 538 TB usable Day-1). By simply adding drives, the same 3-node cluster can scale to over 1 PB within the first year. The requirement for a minimum of 4 nodes is not necessary to achieve 500 TB Day-1 capacity or 1 PB scalability — we can provides this even with 3 nodes. Additionally, availability and fault tolerance are ensured: the platform can tolerate one node failure plus drive failures while continuing to serve data. The “pre-integrated appliance” condition is restrictive. Modern object storage is delivered as a software-defined platform, giving customers flexibility in hardware choice while still maintaining OEM validation and support. We request clarification and amendment of this clause: •Remove the “pre-integrated appliance” requirement. •Recognize that a 3-node starting configuration provides the required 500 TB Day-1 usable capacity and can scale to 1 PB within one year. •Confirm that availability requirements are met, as the solution provides tolerance against one node and multiple drive failures.		Agreed. 3 Nodes strating configuration or above is acceptable provindg 500 TB and scalable to 1PB is acceptablke.
284	Volume 02 of 03	3.4.1.4	86	Special Note: Shall be in optimum throughput network 25GbE or higher (bidder shall calculate and propose network devices and speed accordingly)	While the RFP specifies 25 GbE or higher, it is important to note that throughput requirements can also be achieved on 10 GbE networks by leveraging Link Aggregation Control Protocol (LACP). Using LACP, multiple 10 GbE links can be combined to provide effective aggregated bandwidth, resiliency, and load balancing. We request clarification on whether link-aggregated 10 GbE uplinks (LACP) can be considered compliant under this clause, as they can deliver equivalent throughput and resiliency compared to individual 25 GbE links.		No Change
285	Annexure-3	3.4.1.4-Objec	85-86	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.	Any distributed storage architecture starts with min 3Storage Nodes. Every storage OEM has its own architecture to ensure High Availability and Durability. NetApp can ensure the solution is optimized for availability. Number of active nodes should be left to storage OEM as per their best practices/guidelines.		Agreed. 3 Nodes strating configuration or above is acceptable provindg 500 TB and scalable to 1PB is acceptablke.
286	Annexure-3	3.4.1.4-Objec	85-86	Proposed object storage should be able to consume storage capacity from the provisioned erasure coded storage nodes,block (SAN) storage, file (NAS) storage, public cloud storage or an S3 compatible storage.	This contradicts the appliance-based object storage requirement. As appliances have their own capacity and features, this compliance point should be removed.		Yes Agreed. This requirment is dropped.
287	Annexure-3	3.4.1.4-Objec	85-86	Object storage must support multiple replication topologies: active-active, active-passive, one-to-many, many-to-one, ring, and chain.	This contradicts the appliance-based object storage requirement. As appliances have their own capacity and features, this compliance point should be removed.		This requirment is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
288	Annexure-3	3.4.1.4-Objec	85-86	Erasure coding must provide protection against 6 or more disk failures and at least 1 node failure, with rebuilds occurring within the same site to preserve WAN bandwidth	This appears vendor-specific. NetApp supports up to 2 disk-drive failures per node. Clarification on business and technical use case is needed.		The requirment must be read as under "Erasure coding must provide protection against 1-2 or more disk failures and at least 1 node failure, with rebuilds occurring within the same site to preserve WAN bandwidth"
289	Annexure-3	3.4.1.5-SAN S	87-88	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. In case of non-native/external component used, it should be supplied in redundant mode with no single point of failure.	This appears vendor-specific. Clarification on business and technical use case is needed.		This requirment is dropped.
290	Annexure-3			The proposed array must provide continuous monitoring and movement of sub-LUN data chunks to provide real-time performance improvements	This appears vendor-specific. Clarification on business and technical use case is needed.		This requirment is dropped.
291	Annexure-3	3.4.1.6 SAN S	91-92	The switch(or director platform) must be able to provide up to 96 number - 64Gbps FC or 10-Gbps full line-rate autosensing Fibre Channel physical ports from day1. System should be scalable to support upto 384port or more.	Clarify the need for 384 ports. Director-level switches add significant cost and may not be necessary for the required capacity.		Already answered in S.No. 234
292	Annexure-3	3.4.1.6-SAN S	87-88	SAN Storage Capacity	No visibility on SAN Storage capacity requirements. Clarify if this is for single site or multi-site deployment.		Already answered in S.No. 254
293	Annexure-3	3.4.2.2 Backu	127		The 500 TB capacity includes both virtual machine (VM) and Kubernetes (K8s) backups.		Yes
294	Annexure-3	3.4.2.2 Backu	128		What is the selected hypervisor for running VMs		Thie biddere to propse to hypervsior with enterprise support
295	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Kubernetes distribution and version used to run containers		MSI to consider this and propose
296	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Total Kubernetes clusters:		MSI to consider this and propose

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
297	Annexure-3	3.4.2.3 Cloud Native Backup and Restore	131		Total worker nodes across all clusters		MSI to consider this and propose
298	Annexure-3	3.4.1.17 Serv	115		"The solution shall have integration with Kubernetes Platforms and requisite controller/license/container plugin shall be provided with LB solution from day one. Controller/Plug-in should be from same make as LB. It should not be third party or opensource."	Native integration with Kubernetes is essential due to the significant shift toward microservices architectures.	Bidder's suggestion is fine. Bidder is at liberty to propose native integration with Kubernetes
299	Annexure-3	3.4.1.17 Serv	115		"The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to acheive horizontal scaling"	Horizontal scaling is essential for future-proofing the system, ensuring it can efficiently handle increasing workloads as demand grows over time. By supporting N+1 architecture, the solution allows for the addition of more appliances to the HA cluster, enabling seamless traffic distribution and enhanced fault tolerance. While the current requirements may be met with an active-active or active-passive setup, the ability to scale horizontally ensures the system remains adaptable to future scalability needs and workload expansion.	Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
300	Annexure-3	3.4.1.17 Serv	115		"The proposed solution must handle high-capacity traffic, including L7 requests per second: 450K L4 connections per second:150K concurrent L4 connections:18M L4 throuput 20 Gbps on day 1 and scalable upto 25 Gbps"	There is currently insufficient clarity regarding the expected traffic requirements	The expected traffic requirements are as under, based on which MSI may size L7, L4 and throughput parameters. 1. The current user base is 2000 with 200 concurrent users. 2. The authentication requests per second is 14. 3. OTP request per second is 150 4. Packet size given in demand capacity annexure A5 , both for authentication and enrollment packet. 5. Connection lifespan at API is maximum 10 seconds The MSI should also refer to Demand Capacity Annexure 5 for further details.
301	Annexure-3	3.4.1.18 Glob	116-117		"The device should support 'n' number DNS QPS"	Clarity required on the number of expected DNS Request per second, which would help in sizing the appliacne	50,000 DNS QPS
302	Annexure-3	3.4.1.18 Glob	116-117		"Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS and Must support resolution for A, AAAA, MX, and NS queries as External DNS"	The requirement ensures comprehensive support for diverse DNS query types (A, AAAA, MX, etc.) critical for both internal service resolution within the data center and external citizen access. This guarantees seamless connectivity, scalability, and reliability for all services in a high-availability environment catering to large-scale public use.	Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
303	Annexure-3	3.4.3.15 SSL V	232	Support for VRRP, QoS and full OSPF routing protocol.	"Support for VRRP or equivalent protocols"	A SSL VPN solution does not inherently require support for VRRP (Virtual Router Redundancy Protocol), QoS (Quality of Service), or full OSPF (Open Shortest Path First) routing protocol. These features are not directly related to the core functionality of an SSL VPN, which primarily focuses on securely connecting users to a private network over an encrypted SSL/TLS tunnel	Agreed
304	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	242	11. RAM 64 GB	"11. RAM 128 GB"	To support 30 Gbps throughput, while preventing OWASP Top 10 and SANS Top 25 attacks, significant memory is required for packet inspection, state tracking, and rule processing. 64 GB RAM may cause bottlenecks under high traffic or attack scenarios. At least 128 GB RAM is essential to ensure performance, scalability, and reliable threat prevention.	Agreed
305	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	12. SSL TRANSACTION 10000 CPS/TPS	12. 60K TPS (2K SSL TPS) SCALABLE UPTO 100K TPS (RSA 2k keys) WITH LICENSE UPGRADE	While the expected L4/L7 throughput is 30 Gbps, the SSL CPS must be at least 60,000 to handle modern workloads with high connection rates, such as API traffic, short-lived sessions, or bursts of new connections. Higher SSL CPS ensures the appliance can manage high concurrency and rapid connection setups without becoming a bottleneck, even during peak demand.	Remains Unchanged

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
306	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	14. NETOWRK INTERFACE PORTS 24, 4*40	2 x 100G/40G QSFP28/QSFP+ ports 8 x 25G/10G SFP28/SFP+ ports	clarity required. In a modern spine-leaf network, the emphasis is on high-speed links (e.g., 10/25/100 Gbps) rather than a large number of ports. Efficient interconnections with aggregated uplinks reduce the need for devices with 24 ports. The architecture uses fewer, faster ports for scalability and performance, making excessive port counts unnecessary.	The requirement for "24, 4×40" ports is indicative, not strict. A modern port mix with higher-speed interfaces (such as 25G/100G uplinks) that meets or exceeds the switching capacity and performance requirements is acceptable. The intent is to ensure adequate bandwidth and scalability, not to mandate legacy port counts.
307	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	15. SSL THROUGHPUT 2 GBPS	35 Gbps bulk encryption scalable upto 50 Gbps bulk encryption with license upgradation	While the expected L4/L7 throughput is 30 Gbps, SSL throughput must exceed 2 Gbps to handle real-world workloads where most traffic is encrypted. Modern applications with high HTTPS usage and frequent key exchanges demand higher SSL capacity to prevent performance bottlenecks.	Yes, higher SSL throughput (e.g., 35–50 Gbps) is acceptable.
308	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243		The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the Application Security Top 10 attacks and also provide suggestions/shortcuts to address the compliances and configure policies for it.	The OWASP Compliance Dashboard is not just a feature—it is a critical tool for enhancing, monitoring, and ensuring the security of applications against modern threats. By incorporating it, the solution provides an efficient, scalable, and proactive approach to safeguarding applications, aligning with industry standards, and addressing the challenges of modern application security.	The OWASP Compliance Dashboard and tool is required.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
309	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243		Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	The requirement ensures a purpose-built, high-performance hardware platform designed specifically for application security and WAF, maximizing compatibility, stability, and performance. Avoiding virtual or white-labeled solutions ensures the platform leverages native OEM optimizations, unified support, and streamlined updates, reducing dependency on third-party hardware or software.	The requirement is retained.
310	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	sl no 2. Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	Should have 2 x 100G/40G QSFP+/QSFP28 ports8 x 25G/10G SFP28/SFP+ ports	The requirement for 2 x 100G/40G QSFP+/QSFP28 ports and 8 x 25G/10G SFP28/SFP+ ports ensures that the appliance can handle high-bandwidth demands and future scalability. The 100G/40G ports support environments with heavy traffic aggregation, ideal for data centers or high-performance networks, while the 8 x 25G/10G ports accommodate flexible connectivity for lower-speed links or incremental upgrades.	Anti-DDOS is being taken as a service by GoSL. This requirement is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
311	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	Sl No. 4. Present license should be for 1 Gbps throughput.	System should have 20 Gbps L4 througput sclable upto 25 Gbps with license upgrade without additional hardware	While the RFP specifies a 1 Gbps license, the expected L4/L7 traffic is up to 30 Gbps. For a robust DDoS solution, a minimum 20 Gbps throughput is essential to handle real-world attack scenarios effectively. DDoS attacks often involve massive volumes of traffic, requiring the solution to process and mitigate large-scale attacks while still maintaining legitimate traffic flows. A 1 Gbps license would be insufficient to address peak traffic requirements or volumetric attacks, leaving the network vulnerable. A minimum 20 Gbps ensures adequate capacity to protect critical infrastructure without compromising performance.	Anti-DDOS is being taken as a service by GoSL. This requirement is dropped.
312	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	Sl No. 5. Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	Point may please be dropped	The requirement for a fixed latency of <75 microseconds should be reconsidered, as latency is influenced by multiple factors beyond the hardware's capabilities, including network topology, connection quality, external routing, and environmental conditions	Anti-DDOS is being taken as a service by GoSL. This requirement is dropped.
313	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	"SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 7000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key from day 1 and scalable upto 15K TPS."	While Layer 3/4 DDoS solutions primarily focus on mitigating attacks based on packet headers, traffic patterns, and volumetric anomalies without decrypting encrypted traffic, the growing volume of encrypted traffic in modern networks can indirectly impact overall resource utilization during an attack. Hence looking at the future scalability we propose higher ssl tps .	Anti-DDOS is being taken as a service by GoSL. This requirement is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
314	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	The solution should support at least 2 million packets per second on each box from day 1.	"The solution should support at least 18M L4 Concurrent connections"	Calculating packets per second is impractical due to variable packet sizes. Connections per second (CPS) is a more reliable metric for measuring performance and capacity.	Anti-DDOS is being taken as a service by GoSL. This requirement is dropped.
315	Annexure-3	3.3.3.10 API (	53	The proposed solution shall provide API Lifecycle maintenance capabilities including definition, creation, security, monitoring and management	"The proposed solution shall provide API Lifecycle maintenance capabilities including definition, security monitoring and management."	The point "creation" can be removed because API creation typically involves the application logic and development process, which is outside the scope of an API management solution. The focus of the proposed solution should remain on API lifecycle maintenance, covering critical aspects like definition, security, monitoring, and management, which are essential for optimizing and governing APIs once they are developed, rather than including their initial creation.	The requirement of API creation is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
316	Annexure-3	3.3.3.10 API (	53	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.	"The proposed solution shall have the capability to externalise APIs and should provide cataloguing capabilities with third party integrations."	API cataloguing is not inherently a primary function of API gateway servers, as the core purpose of an API gateway is to manage, secure, and route API traffic. Their primary responsibility is to act as a central access point for APIs, handling authentication, load balancing, rate limiting, and request/response management. For advanced cataloguing capabilities such as detailed documentation, taxonomy management, or developer portal integration, leveraging third-party solutions is more appropriate. This ensures that the proposed solution remains focused on its core competencies while allowing seamless integration with external cataloguing tools to meet the requirement.	As above.
317	Annexure-3	compliance sheet point 6		The solution should include the proposal for the best diskless thin client for the solution.	what is the use case of disless thin client, will a thinclient with lockdown hardened Linux OS will work. This increase the lifespan of the device and better user experience when using heavy application, so please clarify.		The requirement of 3.4.3.7 VDI infrastructure is dropped.
318	Annexure-3	compliance sheet point 2		Virtual Desktop Infrastructure (VDI) must have native clients for Windows 8, Windows 10, Macintosh, Linux, Chrome OS, Blackberry OS, IOS, Android and HP WebOS	our solution provide support for Endpoints: Windows, macOS, Linux, Thin client OS, iOS, Android, Chromebook but doesn't support Blackbery or HP WebOS, how many devices in the current environment uses these 2 OS? Please clarify		Already answered in S.No. 317
319	Annexure-3	compliance sheet point 1		The solution should integrate and work with Backup solutions, Anti-virus solutions, Storage solutions, Network and Security solutions, SIEM Solution, PAM/PIM solution, IDAM solution, etc.	please clarify what all software or applications are used to support the listed components.		Already answered in S.No. 317
320	Annexure-3	compliance sheet point 1		Hardware should be sized for maximum 300 users.	Please clarify what is the total user count(named), and what is the actual concurrency at any given point of them.		Already answered in S.No. 317
321	Annexure-3	compliance sheet point 1		Proposed hardware solution should have blade center in both locations with FS SAN connectivity and High availability.	do we need to consider the DR in the solution, if yes, then what percentage need to be considered for user load? For example 100% users or 50%. Also can we consider active-passive DR or active-active DR?		Already answered in S.No. 317
322	Annexure-3	compliance sheet point 2		Proposed solution should be able to add more blade servers to expand to 300 users.	please specify what is the user CPU, RAM and OS disk requirement for each user and what version of OS windows and linux need to factored in?		Already answered in S.No. 317
323	Annexure-3	compliance sheet point 2		Proposed SAN should have minimum 5TB usable capacity (RAID 5) expandable to 50TB.	please specify what is the user profile and OS partion storage requirements for each user?		Already answered in S.No. 317

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
324	Annexure-3	DDI	S No 3	The solution shall be a scalable platform capable of managing an unlimited number of DNS/DHCP servers and IP addresses from a single management core.	Clarification Required : - Request you to please share the specification details, unlimited number of DNS / DHCP management is an open statement and it can lead to problematic situation during the time of implementation. 1. For DHCP how many lease per second required. 2 For DNS how many DNS query per second required.		2. Already answered in S.No. 301 1. Clarification required. The proposed solution should be scalable beyond these baselines.
325	Annexure-3	DDI	S No 4	The solution shall permit adding DNS/DHCP servers without the need to change the architecture or deploy additional management cores.	Clarification Required: - How many location DNS / DHCP Server department is looking to deploy and what is the future count Please clarify?		10 locations
326	Annexure-3	DDI	S No 10	The solution shall provide a pre-deployment data validation mechanism to prevent syntactical and logical configuration errors from being pushed to the managed DNS/DHCP servers.	Clarification Required:- The ask is related to UAT testing? Please clarify		This requirement refers to automated validation of DNS/DHCP configuration before it is applied to the production servers. It is not related to UAT. The intent is to ensure that invalid DNS/DHCP entries cannot be pushed by mistake
327	Annexure-3	DDI	S No 11	The solution shall support a referential data integrity model that will ensure that no configuration change will result in orphaned objects or incompatible data leading to outages.	Clarification Required:- Need some more details, please help with the use case to understand the requirement in a proper way to avoid any issues.		It is a standard integrity safeguard to prevent outages caused by inconsistent configuration states. The intent is to ensure the platform automatically enforces relational consistency before applying any change.
328	Annexure-3	DDI	S No 21	The solution shall provide high availability scheme that includes application layer clustering, database replication and failover to a secondary or tertiary server.	How many location HA is required please confirm? Also DNS & DHCP required on same appliance or it has to be separate appliances?		All 10 DNS deployment locations shall operate in High Availability mode, with a minimum of two DNS servers per site, configured for redundancy and continuous service availability.”
329	Annexure-3	DDI	S No 21	The solution shall provide high availability scheme that includes application layer clustering, database replication and failover to a secondary or tertiary server.	Clarification Required:- What is the no of user need to be considered each location wise? Please confirm		Indicative users are provided in Annexure 5: Demand Capacity. Actual number of users will be finalized during deployment in consultation with GoSL
330	Annexure-3	DDI	S No 24	The solution shall have the ability to manage both IPv4 and IPv6 blocks, networks and IP addresses.	Clarification Required :- How many IP addresses need to be managed? Please clarify		IP schema is to be prepared by MSI according to the solution design.
331		DDI	S No 34	The solution DNS Services should support both IPv4 and IPv6 with tracking of dual-stacked addresses.	Clarification Required:- Please share the IPv4 & IPv6 IP addresses count to factor the appropriate appliance for sizing		Already answered in S.No. 330

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
332	Infrastructure	3.4.1.5SAN (Storage Area Network	88	The storage system shall have a minimum of 256 GiB cache memory per system to ensure low latency performance. The proposed array must ensure cache data integrity during manual shutdowns or unexpected power outages by automatically destaging cached data to non-volatile media such as flash or disk.	From min 768 GiB cache to ensure sustained sub-ms latency, higher IOPS handling, future scalability, and enterprise-grade resiliency beyond the minimum requirement.		offering a larger cache than the 256 GiB minimum is acceptable and will not be viewed as non-compliant
333	3.4.1 Biometric Registration Kit	3.4.2.5SAN	357	The proposed storage array should support Three-Data- Center (3DC) replication, ensuring robust disaster recovery and high availability	If 3DC requires than increase the cache for 768GB for better performance		There is no requirement for 3DC. Only DC and DR will be configured in 1:1 configuration.
334	3.4.1 Biometric Registration Kit	3.4.2.5SAN	357	The proposed storage array should support Three-Data- Center (3DC) replication, ensuring robust disaster recovery and high availability			Already answered in S.No. 333
335	Infrastructure	3.4.1.1 SAN (Storage Area Network)	89	The proposed storage array should support Three-Data- Center (3DC) replication, ensuring robust disaster recovery and high availability	If 3DC requires than increase the cache for 768GB for better performance		Already answered in S.No. 333
336	Infrastructure	3.4.1.1 SAN (Storage Area Network)	89	The proposed storage array should support Three-Data- Center (3DC) replication, ensuring robust disaster recovery and high availability			Already answered in S.No. 333
337	Infrastructure	3.4.2.5SAN	359	The offered storage solution must be able to cater to file, block, and object workloads	Object workloads, however, are fundamentally different from file and block storage. They are best handled by specialized platforms.Object may dilute performance of block/file if not on specialized engine Higher complexity to manage all 3 in one		Already answered in S.No. 216
338	Infrastructure	3.4.1.1 Rack Server	350	Should support video using the Matrox G200e video/graphics controller Supports display resolutions up to 1920 x 1200 16bpp @ 60H	Specific to vendor on Graphic controller- we can provide same display resolution.		The requirement should be resolution-based, not chipset-specific. Any onboard graphics supporting 1920 × 1200 @ 60 Hz (16bpp) is acceptable. The requirement of Matrox G200e video/graphics controller is dropped.
339	Infrastructure	3.4.3.3		The proposed solution must offer a SDK or programming libraries for inclusion within the source code of internally developed software.	How many application servers are there in the environment for which SDKs are required?		The PAM/PIM solution does not require the use of an SDK for core functions such as privileged session management, password vaulting, session recording, or workflow-based access approvals.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
340	Infrastructure	3.4.3.3		The proposed solution must support zero information disclosure error messages to prevent logs from displaying sensitive information.	Pls help elaborating the requirement here.		This requirement ensures that PAM/PIM error messages and logs do not reveal any sensitive information (credentials, privileged account details or system internals) and only generate generic, non-disclosing messages to prevent information leakage.
341	Infrastructure	3.4.3.3		The proposed solution's account segregation hierarchy must support an inheritance model for resources and policies.	Pls help elaborating the requirement here.		Already answered in S.No. 340
342	Volume	4.5. Indicative Overall DC/DR Architecture	60	Fixed enrolment centers to be connected via DRP IPVPN network, DRP will extend exiting IPVPN network to DC, DR and NOC/SOC/IT helpdesk building,	We assume that DRP IPVPN is MPLS VPN, Please clarify the same ? Whether the single MPLS VRF of DRP IPVPN will be extened to DC, DR & NOC/SOC/IT Helpdesk locations by GoSL ?		DRP should be read as GoSL. Telecommunication networking is the responsibility of GoSL.
343					Whether NOC, SOC and IT Helpdesk's are at different locations or they all are located in the same location ?		NOC, SOC and IT Helpdesk location will be at different locations. However, IT helpdesk will be in primarcy DC manned by MSI
344					What is the Specification for Router to be deployed at NOC, SOC and IT Helpdesk		All networking equipmemt at NOC, SOC will be provided by GoSL. However, routing networking equipment will be provided by MSI.
345					From Annexure 5 - Demand capacity document we understand that Bandwidth at each Fixed Registration Centre is 4 Mbps. There are 340 Permanent Centers. So we assume to provision 1.5 Gbps at DC and DR to accommodate the traffic. Please confirm whether that's fine		The permanent center count now stands at 806 plus and 40 mobile centers. Please refer to section 5.1.3 of Annexure - Demand Capacity where bandwidth provisioning of registeration center is provided. The MSI is therefore requested to size the networking equiement accordingly considering the other parameters of packet size and peak volume in the annexure.
346					There are 466 Temporary Enrolment Clusters, whether 4 Mbps BW will be provided here aswell. If so do we have to consider aggregated BW at DC and DR as well ?		Already answered in S.No. 345

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
347				IT Helpdesk, SOC, NOC to be connected to DC and DR via p2p WAN links, bandwidth to be decided by MSI.	We assume MSI Should suggest the BW and GoSL will provide this BW. Please clarify ?		Yes
348	Annexure-11	4.5. Indicative Overall DC/DR Architecture	60	DC/DR Replication link to be implemented considering the RTT/latency requirement of applications.	Believe this should be a Fiber channel Link, please confirm? Whether this link to be provided by MSI ?		The backup and DC–DR replication architecture for the Sri Lanka UDI system is IP-based (Ethernet/IP replication), not Fibre Channel. MSI to provide the IP based replication.
349	Volume-2	SL-UDI Wide Area Network	55	Link : Data Centers (DC & DR) – NOC, Type : MPLS/SDWAN, Remark : MSI will be required to provide secure and reliable connectivity.	Request to clarify what MPLS/SDWAN Means ? Whether we are supposed to provide either MPLS or SDWAN over Internet underlay?		No. GoSL to provide.
350					If SDWAN to be provided, where should be the orchestration plane deployed ?		No
351					Is there any specification for Router to be Deployed at NOC?		No
352		SL-UDI Wide Area Network	55	Link : Data Centers (DC & DR) – SOC, Type : MPLS/SDWAN, Remark : MSI will be required to provide secure and reliable connectivity.	Request to clarify what MPLS/SDWAN Means ? Whether we are supposed to provide either MPLS or SDWAN over Internet underlay?		Already answered in 349
353					If SDWAN to be provided, where should be the orchestration plane deployed ?		Already answered in 350
354					Is there any specification for Router to be Deployed at SOC?		Already answered in 351
355					Whether NOC and SOC will be in same premises ?		SOC and NOC will be setup at the premises provided by GoSL in srilanka. Exact location will be shared with the successful bidder.
356		SL-UDI Wide Area Network	55	Link : Data Centers (DC & DR) – Contact center, Type : GoSL VPN , Remark : MSI will be required to provide secure and reliable connectivity.	IF the BW is going to be provided by GoSL then why the remark is mentioned as MSI responsibility ?		Bandwidth is not the responsibility of MSI
357		SL-UDI Wide Area Network	55	Link : Data Centers (DC & DR) – Technical helpdesk, Type : MPLS/SDWAN, Remark : MSI will be required to provide secure and reliable connectivity.	Please suggest whether Contact center and Technical helpdesks are in different locations or same building ?		Yes, Contact center and technical heldesk will be different location. Helpdesk will be in primary DC.
358					Can we propose a single MPLS VRF in which NOC, SOC, Contact center, Technical helpdesks are connected		NOC, SOC, Contact center, Technical helpdesk will be connected with single MPLS , to be provided by GoSL.
359				Link : Data Centers (DC & DR) – Hosting Infrastructure, Type : GoSL IPVPN, Remark : GoSL will provide secure and reliable connectivity, MSI shall work collaboratively with GoSL their network service provider	Hosting Infra will be inside the DC and DR and will be connected over LAN Network. What is that GoSL IPVPN here, needs more clarity ?		GoSL IPVPN is GoSL telecommunication network riding on MPLS.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
360		SL-UDI Wide Area Network	56	Internet Connectivity	Shall we consider 1 Gbps of Internet connectivity at DC & DR ? How many number of Public IP address space would be required ? Whether GoSL has its own APNIC pool ?		Regarding internet connectivity bandwith please refer to answer S.No. 300. Public IP Pool will provided by Telecom service provider.
361	Annexure-3	3.4.1.9. Network Core Router		Performance: 1) Minimum IP forwarding throughput of 190Gbps/higher. 130Gbps/higher IPSEC Bandwidth, 30Gbps/higher IMIX/EMIX encryption throughput. 2) 4000/more IPSEC tunnels. 3) 8000/more VRF segments. 4) Minimum 4M/more IPv4 & IPv6 routes. 5) 30M or more firewall sessions.	Request to modify as : 250 IPsec tunnels & 1000 VRFs	For a Core Network Router, the primary function is high-speed IP routing and secure site-to-site connectivity, not large-scale firewalling or IPsec termination. The requested 4000+ IPsec tunnels and 30M firewall sessions represent firewall-class workloads, which are not applicable to core routing functions. Adjusting the requirement to 250 IPsec tunnels and 1000 VRFs aligns with realistic operational needs for inter-site or DCI encryption while maintaining full multi-tenancy support. Core routers in a modern L3 Leaf-Spine or SDN fabric typically delegate large-scale IPsec and session handling to dedicated security gateways, ensuring optimal routing performance and scalability.	To ensure technical accuracy and alignment with operational needs, the requirement stands modified to: 250 IPsec tunnels, and 1000 VRF segments, which reflect realistic and appropriate performance expectations for Core Routing functions while still supporting secure inter-site connectivity and multi-tenancy.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
362	Annexure-3	3.4.1.9. Network Core Router		Layer 2 , Layer 3 Security and other features: 1) static Routes, OSPFv2, OSPFv3, BGP4, MBGP, BFD, Policy based routing, IPv4 and IPv6 tunnelling. 2) IKEv1, L2TP, IKEv2, GRE and IPSEC. 3) Router should support Zone Based Firewall feature. 4) Support Traffic Optimization feature built in the router operating system or an external appliance for the same functionality can be provided. 5) 802.1p class of service and marking, classification, policing and shaping. 6) AES-256 and AES-GCM. 7) Hierarchical QoS should be supported both at Physical and sub-interface level. 8) Support deep packet inspection to identify applications at layer-7 and 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. 9) IGMP v1/v2/v3 and PIM multicast routing.	Please remove the highlighted.	The requested features — L2TP, Zone-Based Firewall, and Deep Packet Inspection (DPI) — are typically associated with security gateways or WAN edge devices, not core or aggregation routers. In a modern L3 Leaf-Spine or SDN-based data center or core network, the router's role focuses on high-performance Layer 3 routing, segmentation, QoS, and encryption (IPsec) rather than session-based or application-layer security functions. L2TP is primarily used for legacy remote access VPNs and is not relevant for data center or core routing. Zone-Based Firewall and DPI/application identification introduce unnecessary processing overhead and are better handled by dedicated firewalls or security appliances. Therefore, it is recommended to	Agreed. The highlighted features—L2TP, Zone-Based Firewall, and Deep Packet Inspection—are security-gateway functions and not applicable to a Core Network Router. Therefore, these requirements are dropped.
363	Annexure-3	3.4.1.9. Network Core Router		Manageability features: 1) SSHv2, SNMPv2c, SNMPv3 and NTP. 2) support AAA using RADIUS and TACACS+. 3) Support for IP SLA or equivalent and best path selection for metrics like delay, latency, jitter, packet loss to assure business-critical IP applications from Day1. 4) Support monitoring of network traffic with application-level insight with deep packet visibility into web traffic, RTP-Based VoIP traffic.	Please remove the highlighted.	Application-level traffic visibility and deep packet inspection (DPI) are security or analytics platform functions, not core router requirements. In modern architectures, such capabilities are typically handled by dedicated NPM/APM or firewall solutions, while the router focuses on high-performance forwarding, telemetry, and routing control.	Agreed. The requirement is dro

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
364	Annexure-3	3.4.1.10. Network Core Switch		Core Switch should meet/exceed following hardware features/capacity. 1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 80MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber modules should have duplex LC connector to work with multi-mode fiber supporting minimum 300 meters for 10Gbps link and 100 meters for 100Gbps link.	Please change 80MB buffer to 32 MB dynami intelligent buffer	Modern data center and campus switches employ dynamic or intelligent buffer allocation, where memory is shared across all ports and allocated on demand. This approach offers superior real-world performance compared to large fixed (static) buffers, as it optimizes utilization during congestion and adapts to varying traffic patterns. An intelligent 32 MB dynamic buffer can handle microbursts and mixed traffic flows more efficiently than a larger static buffer, while also reducing latency and packet loss. It aligns with the latest merchant silicon architectures (e.g., Broadcom Trident3 / Trident4), which focus on smart congestion management rather than raw buffer size. Therefore, a 32 MB dynamic shared buffer delivers equal or better performance than an 80 MB static buffer under realistic network conditions, ensuring	Yes, agreed. A 32 MB dynamic shared buffer can be provisioned as per modern switching architectures.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
365	Annexure-3	3.4.1.10. Network Core Switch		Core Switch should meet/exceed following performance parameters. 1) 80K MAC Addresses and 1K VLANs. 2) 25K ACLs, 30K Multicast and 80K IPv4, 80K IPv6 Routes. 3) Application visibility and traffic monitoring with minimum 60 K sflow/jflow/netFlow entries. 4) 200Gbps/more bidirectional stack throughput.	Please change 25K ACLs to 7K ACLs and 60K sflows to 32K sflows.	Modern data center and campus networks rely heavily on segmentation through VRFs, VLANs, and EVPN overlays, which significantly reduce the number of ACL entries required per device. A capacity of 7K ACL entries is more than adequate for large-scale enterprise or campus environments, supporting thousands of flows and granular security policies per interface. The requirement for 60K sFlow/jFlow/netFlow entries is significantly above typical operational requirements. In practical deployments, 32K sFlow entries are more than sufficient for comprehensive application visibility and traffic analytics across all active interfaces and VLANs. sFlow operates via sampling, not per-flow state tracking; hence, increasing entries beyond 32K does not meaningfully improve visibility	MSI's proposed revision to 7K ACLs and 32K sFlow entries is Accepted.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
366	Annexure-3	3.4.1.10. Network Core Switch		Core Switch should support following Layer 2 , Layer 3, Security and other features. 1) Virtual Switching/Stack/Equivalent features allows links that are physically connected to two different switch to appear as a single port channel. 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.1ae (256-bit and 128-bit AES), 802.3x, 802.1p, 802.1Q, 1588v2. 3) AES-256 support with MACSEC-256 encryption algorithm on hardware. 3) BGP, MPLS, IS-IS, VRF, VXLAN, NAT, OSPF Routed Access, Policy-Based Routing (PBR), PIM SM, and Virtual Router Redundancy Protocol (VRRP). 4) 802.1p class of service, marking, classification, policing and shaping. Should support strict priority queuing. 5) port security, DHCP snooping, Spanning tree root guard, First Hop Security. 6) IPv6 support in hardware, providing wire rate forwarding for IPv6 network. 7) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment.	Please remove MACsec.	Limited Use in DCs: MACsec is best suited for DCI links where traffic leaves the data center's physical boundary, protecting against wiretapping and inter-site risks. Within a secured data center, existing physical and network controls make it largely unnecessary. Operational Overhead: As a Layer 2 hop-by-hop protocol, MACsec adds latency, CPU load, and management complexity—particularly in L3LS fabrics, where it hinders automation and scalability. Performance Impact: MACsec adds a 32-byte header and integrity field, reducing effective MTU and throughput. In VXLAN/EVPN environments, this leads to measurable performance loss, especially on high-speed (100G/400G) links.	MSI's request to remove MACsec support from the Core Switch specification is accepted.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
367	Annexure-3	3.4.1.11. Access Switch LAN		Access Switch should support following Layer 2 , Layer 3, Security and other features. 1) Switch should have dedicated slot for modular with dedicated stacking throughput and should support up to 8 switches in a stack 2) IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q 3) AES-128 support with MACSEC-128 encryption algorithm on hardware all ports. 3) Static routing, RIP, REP PIM, OSPF, VRRP, PBR and QoS. 4) 802.1p class of service, marking, classification, policing and shaping and eight egress queues. 5) IPv6 Binding Integrity Guard, IPv6 Snooping, IPv6 RA Guard, IPv6 DHCP Guard, IPv6 Neighbor Discovery Inspection and IPv6 Source Guard. 6) 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment. 7) Should be SDN ready with VXLAN and VRF	Allow virtual stacking throgh front panel ports. Please remove MACsec. Arista provides equivalenr features for the IPv6 security features.	Limited Use in DCs: MACsec is best suited for DCI links where traffic leaves the data center's physical boundary, protecting against wiretapping and inter-site risks. Within a secured data center, existing physical and network controls make it largely unnecessary. Operational Overhead: As a Layer 2 hop-by-hop protocol, MACsec adds latency, CPU load, and management complexity—particularly in L3LS fabrics, where it hinders automation and scalability. Performance Impact: MACsec adds a 32-byte header and integrity field, reducing effective MTU and throughput. In VXLAN/EVPN environments, this leads to measurable performance loss, especially on high-speed (100G/400G) links. The proposed switch supports high-performance stacking through front-panel ports using standard	The request to remove MACsec (AES-128/MACsec-128) support from Access Switch requirements is Accepted. allowing virtual stacking through front-panel ports is consistent with modern switching architecture is also accepted.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
368	Annexure-3	3.4.1.15. Data Center Leaf Switch		Performance & Scale: 1) Support non-blocking Layer 2 switching and Layer 3 routing. capable to function in line rate for all ports. 2) should be able to re-converge all dynamic routing protocol at the time of routing update changes i.e. Graceful restart for fast re-convergence of routing protocols (OSPF, IS-IS, BGP). 3) Support minimum 1000 VRF instances with route leaking functionality, 1700K IPv4 LPM routes, minimum 3.6 TBPS of switching capacity (or as per specifications of the switch if quantity of switches are more, but should be non blocking capacity) and should support intelligent buffer management with a minimum buffer of 40MB. 4) Should support minimum 90k of MAC addresses	Please change 1000 VRFs to 500 VRFs. 1700K IPv4 LPM routes to 384K IPv4 LPM routes. 40MB buffer to 32 MB buffer.	1. VRF Instances: Requesting a minimum of 500 VRFs is sufficient for large-scale campus or data center segmentation requirements. Each VRF can isolate tenants, departments, or services without impacting routing performance. 2. IPv4 Route Scale: For a leaf switch, a scale of 384K IPv4 LPM routes is adequate. In a Leaf-Spine (VXLAN EVPN) architecture, Spine switches handle the majority of Layer 3 routing, while leafs primarily manage local subnet reachability. The original 1.7M route requirement aligns more with a core or border role, not a leaf. And the IPv4 LPM asked for Spine switch is 500K. 3. Buffer Capacity: Modern Arista switches employ dynamic intelligent buffering that adapts to traffic patterns, minimizing congestion even under bursty workloads. A 32 MB dynamic buffer provides	requested changes (500 VRFs, 384K LPM routes, and 32 MB dynamic buffer) are technically justified and accepted

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
369	Annexure-3	3.4.1.15. Data Center Leaf Switch		Security: 1) Support control plane Protection from unnecessary or DoS traffic by control plane protection policy. 2) Support for external database for AAA using TACACS+ & RADIUS. 3) support to restrict end hosts in the network. Secures the access to an access or trunk port based on MAC address. It limits the number of learned MAC addresses to deny MAC address flooding. 4) VXLAN and other tunnel encapsulation/decapsulation should be performed in single pass in Hardware. 5) Support for Role Based access control (RBAC) for restricting host level network access as per policy defined. 6) support DHCP Snooping, dynamic ARP Inspection, IP Source Guard and unicast and/or multicast blocking on a switch port. 6) Support to suppress the flooding of frames destined for an unknown unicast or multicast MAC address out of that port. 7) Support broadcast, multicast and unknown unicast storm control. 8) LLDP, MAC Sec (802.1AE) in hardware and Spanning tree BPDU protection.	Please remove MACsec. DAI to DAI or equivalent.	Limited Use in DCs: MACsec is best suited for DCI links where traffic leaves the data center's physical boundary, protecting against wiretapping and inter-site risks. Within a secured data center, existing physical and network controls make it largely unnecessary. Operational Overhead: As a Layer 2 hop-by-hop protocol, MACsec adds latency, CPU load, and management complexity—particularly in L3LS fabrics, where it hinders automation and scalability. Performance Impact: MACsec adds a 32-byte header and integrity field, reducing effective MTU and throughput. In VXLAN/EVPN environments, this leads to measurable performance loss, especially on high-speed (100G/400G) links. The requirement for Dynamic ARP Inspection (DAI) can be met through Arista's Static ARP	MACsec is dropped. In Interest of vendor neutrality, DAI or DAI equivalent is allowed.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
370	Annexure-3	3.4.1.19. Network Access Control		The hardware appliance should come with minimum 4 x 10G SFP interfaces, 64GB RAM and 1TB Disk. Each appliance should have redundant hot swappable power supply and fan module/tray.	Please remove the highlighted	AGNI is provided as a purpose-built appliance with a predefined and optimized hardware configuration. Each AGNI appliance is designed to support up to 50,000 clients while ensuring reliable performance and scalability. The appliance includes redundant, hot-swappable power and fan modules for high availability and operational resilience. Storage and compute resources are optimized to retain data for 30 days, meeting the functional and performance requirements of large-scale NAC deployments. As AGNI is delivered as a validated turnkey solution, its configuration cannot be altered, but it fully meets the performance, redundancy, and reliability expectations defined in the requirement.	The requirement is retained. However, The bidder may choose to provide NAC as per the specifications or equivalent. Either solution can be accepted based on the overall network architecture and interoperability needs.
371	Annexure-3	3.4.2.9 ENTERPRISE MONITORING SYSTEM		The solution should allow easy configuration of polling frequency till per second scenario.	Request to modify this as 1 minute.		Agreed. Please refer to S.No. 240
372	Annexure-3	3.4.2.9 ENTERPRISE MONITORING SYSTEM		The system should provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity.	Request to modify this point as discovery / manual mapping of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity.		Agreed. Manual and automated mapping in EMS is allowed.
373	SL-UDI-Vol-2-of-Vol-3	5.8.5 IT Helpdesk	102	IT Helpdesk	What field hardware (biometric devices, scanners, etc.) needs to be installed at new sites?		Query not clear.
374	SL-UDI-Vol-2-of-Vol-3	5.8.5 IT Helpdesk	102	IT Helpdesk	What are the preventive maintenance procedures to be followed?		As per ITIL V4 protocol.
375	SL-UDI-Vol-2-of-Vol-3	5.8.5 IT Helpdesk	102	IT Helpdesk	What baseline performance metrics should be tracked post-deployment?		Already answered in S.No. 374
376	SL-UDI-Vol-2-of-Vol-3	5.8.5 IT Helpdesk	102	IT Helpdesk	How is installation scheduled and coordinated?		MSI to follow its project plan

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
377	SL-UDI-Vol-2-of-Vol-3	5.8.5 IT Helpdesk	102	IT Helpdesk	What Escalation Matrix to be followed in case of any hardware failures ?		Escalation Matrix in case of hardware failure is internal to bidder as per defined SLAs. Ths MSI will inform GoSL regarding any failures/replacement/destruction.
378	SL-UDI-Vol-2-of-Vol-3	5.8.5.1 Helpdesk Setup and Operations	102	Helpdesk Setup and Operations	What mechanisms will the helpdesk implement to ensure effective coordination and collaboration with the application, infrastructure, and field teams?		MSI to follow ITIL V4.
379	SL-UDI-Vol-2-of-Vol-3	5.8.5.1 Helpdesk Setup and Operations	102	Helpdesk Setup and Operations	What specific roles and permissions will be assigned to each user within the CRM/Incident Management module of the EMS system?		To be defined at the stage of implementation and O&M phase in consultation with GoSL
380	SL-UDI-Vol-2-of-Vol-3	5.8.5.1 Helpdesk Setup and Operations	102	Helpdesk Setup and Operations	What processes will the helpdesk follow to coordinate with third-party vendors in cases where external support is required?		MSI to follow ITIL V4.
381	SL-UDI-Vol-2-of-Vol-3	5.8.5.2 Deployment of Infrastructure for IT helpdesk	103		What escalation procedures will be established between GoSL and MSI to address unresolved support requests?		MSI to follow ITIL V4.
382	SL-UDI-Vol-2-of-Vol-3	5.8.5.2 Deployment of Infrastructure for IT helpdesk	103		What redundancy measures to be implemented to mitigate risks associated with power outages, connectivity disruptions, and hardware failures?		MSI to follow ITIL V4.
383	Volume-2	3.2 SL-UDI Op	16	SL-UDI Support arrangement	What is a definition of all other components?		All other components will exclude bandwidth, network connectivity and non IT component of DC-DR NOC and SOC.
384	Volume-2	5.1.3.2 Custo	34	4. The MSI shall be responsible for integrating the CRM with the technical Help Desk.	Overall CRM system will deployed and manage by MSI. Pl. confirm.		yes
385	Volume-2	1.8 Key Consi	11	**Enrolment (Field Aspects)** 7. Registration Kit (other than Biometric Capture Devices) 11. Registration related issue identification and resolution	Tickets will be placed on MSI's technical helpdesk. 1st level remote support by MSI Next-level remote support by BSP 1st level On-site support by MSI Next-level on-site support by concerned agency. Kindly confirm scope & the defined process in filed support activities for a seamless alignments with local filled support partners.		All field support tickets will be generated by contact center on MSI CRM. First level remort support will beby CRM resources. In case of escalation, all tickets will be transferred to MSI helpdesk for resolution by respective resources including BSP resources.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
386	Volume-2	5.3 Field Infrastructure 5.4 Enrolment Centers	60~65	5.3.2.4 Installation and Commissioning	Kindly help us to understand if any role in Field infra & enrolment centers commissioning activities.		yes, the MSI has to monitor the commissioning activities and provide a Go-Live status of each enrollment center before the actual enrollment of citizen is undertaken.
387	Volume-2	5.8.4 Support (Contact Center and Helpdesk)	97-101	Contact Center & Helpdesk Setup and Administration. Contact Center will be facilitated by GoSL. (v) MSI will be responsible for supplying and implementing Customer Relationship Management (CRM) software to support Contact Center Agents / GoSL Officials at the Contact Center. The GoSL will provide necessary manpower i.e., supervisors and contact center agents to run the Contact Center. The MSI will be responsible to train the aforementioned manpower for the resolution of citizen and partner queries. The contact center will provide support in Sinhalese, Tamil, and English languages.	This will be in scope of MSI & GoSL. Design, Build, Operate & Transfer to MSP.		Please refer to S.No. 32 Annexure 16 - RACI matrix. The effective date for transfer to MSP will be decided by GoSL.
388	Volume-2	5.8.5 IT Helpd	102	handle end user (can be internal users of SL-UDI or external users) queries and service requests, which may be in the form of an omnichannel interface (call, email, online ticket, paper, etc.).	What is a definition & method to differentiate between internal and external users in this environment to support. SOPs to be provided by GoSL/MSI for supporting internal and external users.		Internal users here refer to team of MSI , MSP , ICTA (or its sucessor). External users, for example refers to enrollment officers, citizen using portal etc. SOP for resolution will have to provided by the bidder as part of the project delivery plan.
389				(i) Staff the service desk with technically qualified **system admin, application, IT infra and Biometric specialists** in two shifts 24*7.	IT Helpdesk staff (i.e. L1,L2,L3) will be working in **three shifts 24*7**. Does it require to have a language proficiency of Sinhalese, Tamil, and English languages for the staff members in IT Helpdesk support?		IT helpdesk primarily will be working in two shifts. However, a nominal third shift has to be planned by MSI for any emergency pertaining to data center emergency. Language should be english.
390		5.9.1.2 SOC S	107	SOC administration services will provide L1, L2 and L3 support services for security monitoring of the infrastructure. L1 services will comprise of monitoring, L2 services will comprise of validation of incidents and SIEM management and L3 activities will cover supervision of the SOC team.	Both NoC/SoC services to be operational for 24*7. deploy appropriate manpower at the site specified by GoSL to selected bidder for the contract period of 3Y with MSI. L1,L2 & L3 service resources allocation should be in a reference of Manpower annexure. After 3Y MSI should transform the services to MSP selected by GoSL. Kindly add your inputs to highlight specific pointer for seamless operation of services as expected.		Please read demand capacity Annexure 5 for man management of NOC and SOC. Please refer to Annexure 16 - RACI matrix S.No. 19,20,21,22 for operational responsibility

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
391		5.9.2.2 NOC S	109	NOC administration services will provide L1, L2 and L3 support services for network monitoring of the infrastructure. L1 services will comprise of monitoring, L2 services will comprise of validation of incidents and network monitoring tools management and L3 activities will cover supervision of the NOC team.			Already answered in S.No. 390
392	Annexure-10	10.1 Professi	4	(D) Engineers For Example, Infrastructure Engineer Implementation Phase : Full-Time Onsite O&M Phase : Offsite	During O&M phase is it allowed for these engineers to access remotely for supporting any change/configuration request?		Yes, remote access would be provided under the supervision of MSP and GoSL.
393	Annexure-10	10.3 Resourc	48	Guidelines for Staffing and Provisioning of Manpower	What corrective actions will be applicable in the event of non-compliance with the staffing guidelines outlined in the contract?		Please refer to section 10.3.1 Guidelines for Staffing and Provisioning of Manpower
394	Annexure-3			The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform:	need clarity on this. Some thing related to Device Control means, request to remove / factor 3rd party integration for wider participation		External event ingestion is required and is technically necessary for achieving true correlation and root-cause visibility. Requriement of Third party event correlation tools is maintained.
395	Volume-2	5.8	74	Alternatively, MSI can bring in own digital signature issuance infrastructure as a part of the solution.	What is the purpose of this?, is this for Internal Certificate Authority for DC assets and Infra Management Users Authentication and Authorization?		For Establishing trust in SLUDI components
396	Volume-2	5.8	74	The MSI should ensure that all the components can be accessible only within Sri Lanka and not accessible outside.	As per RFP if Development allowed from offshore location, access needs to be provided to some components over Secure connection.		Yes, this will be allowed under the supervision of MSP and GoSL.
397	Volume-2	5.8.1.2	74	It is essential that SL-UDI collects, periodically reviews, and securely archives the security log data, including encryption logs (i.e., logs from HSM and other cryptographic processes, where applicable), for a defined period of time. MSI shall develop logging and auditing processes ensuring security and retention of security logs.	What is the log retention period?		No data will be deleted . Live logs will be retained for 1 year and thereafter it will be archived.
398	Volume-2	5.8.1.2	74	Risk assessment and treatment process: MSI shall develop and implement processes for identification, estimation, assessment, and treatment of security risks in SL-UDI's applications, systems, office, and DC/DR locations, etc. basis SL-UDI's risk management framework.	Do we need to provide GRC solution. This would require consultancy work to ensure policies and compliance processes are in place in addition to the solution.		GRC solution is not required to be implement by MSI. Only GRC framework will be provided by MSI.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
399	Volume-2	5.8.1.3	75	An indicative list of the security components and tools considered for security solution is given below. The MSI shall be responsible for procurement, deployment as well as daily operations of all security tools and technologies in SL-UDI environment.	Can we provide UTM functality to combining security services? Ex, NIPS with External Firewall and HIPS part of EDR solution or separate physical component required for each functionality?		Not agreed.
400	Volume-2	5.8.1.3	75	Security Components for Implementation	For solutions, where personal data may be processed (DLP and Email Security), can cloud based options be used. Gartner quadrant products are cloud based for these solutions		No
401	Volume-2	5.8.1.3	75	Security Components for Implementation	For solutions, where no personal data is processed (EDR and NDR solutions), can cloud based options be used. Gartner quadrant products are cloud based for these solutions or any mandate to maintain all the security products only on-Prem DC?		No
402	Volume-2	5.8.1.3	75	Security Components for Implementation	For directory services and IAM, can we use a non-Gartner, local solution (WSO2) being used in other key projects as the understanding is to Manage the Infra Management User identity and related RBAC and SSO with MFA.		Not agreed.
403	Volume-2	5.8.1.3	75	Security Components for Implementation	Can we combine SIEM and SOAR on same OEM Bundle if the Specifications requirements fit in?		SOAR is not required. MSI to propose the solution accordingly.
404	Volume-2	5.8.1.3	76	Server hosting the centralized EDR console (In DC and DR)	Anayst Leader products are SaaS based, do we need to look strictly On prem EDR solution?		No. On prem EDR solution is required.
405	Volume-2	5.8.1.3	76	Server hosting the 2FA tool (DC + DR)	How many user license required for this MFA?, can we consider Cloud solution for this?		No. Cloud solution is not acceptable. 15 licenses required for MFA.
406	Volume-2	5.8.1.3	77	Privileged Access Management (PAM) / Privileged Identity Management (PIM):	How many privillaged accounts expected for licensing?		15 licenses
407			243	14. NETOWRK INTERFACE PORTS 24, 4*40	2 x 100G/40G QSFP28/QSFP+ ports 8 x 25G/10G SFP28/SFP+ ports		Already answered in S.No. 306
408			204	sl no 2. Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	Should have 2 x 100G/40G QSFP+/QSFP28 ports8 x 25G/10G SFP28/SFP+ ports		Already answered in S.No. 310
409			204	Sl No. 5. Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	Point may please be dropped		Already answered in S.No. 314
410	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability. 14. NETOWRK INTERFACE PORTS 24, 4*40	243	2 x 100G/40G QSFP28/QSFP+ ports 8 x 25G/10G SFP28/SFP+ ports	clarity required. In a modern spine-leaf network, the emphasis is on high-speed links (e.g., 10/25/100 Gbps) rather than a large number of ports. Efficient interconnections with aggregated uplinks reduce the need for devices with 24 ports. The architecture uses fewer, faster ports for scalability and performance, making excessive port counts unnecessary.		Already answered in S.No. 306

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
411		3.4.3.17 Internal Firewall (Next-Gen) with High Availability		17. Firewall should have 8*10Gbps SFP integrated data ports, 8 x 100Gbps ports. Fiber interfaces should be populated with multi-mode transceiver modules.	If the customer agrees to reduce the 8 x 100Gbps ports to 6 x 100Gbps ports, a more cost-effective and optimized model can be recommended.		6 x 100 Gbps ports is acceptable.
412		3.4.31		Solution should have Ability to exclude by application process name in removable storage device rules	Need clarity on this. Some thing related to Device Control means, request to remove / factor 3rd party integration for wider participation		Most leading DLP solutions support this natively; removing it would weaken endpoint security. Therefore, the requirement remains unchanged.
413		3.4.31		Solution should support device control for endpoints	Device control is not the DLP Function. Hence request to modify the spec as " The Solution shoud support Whitelist / Black List the Removable Media Devices based on the Device Serial Number		The requirement is retained.
414				The solution should allow encryption using strong algorithms as per industry best practices of the complete hard drive sector by sector.	its a OEM Specific one. Hence request to remove the same for wider participation or the bidder should plan for the dedicated encryption solution to deliver the same.		Either of the solution can be provided.
415				The solution should support encryption of extended partitions. The configuration for full disk encryption is controlled from the management console by selecting the drive letter that you intend to encrypt regardless of the partition type.	its a OEM Specific one. Hence request to remove the same for wider participation or the bidder should plan for the dedicated encryption solution to deliver the same.		Requirement is dropped provided the product benchmarking guidelines as mentioned in Annexure 3 are complied to.
416				The solution should record the encryption status of each hard drive	its a OEM Specific one. Hence request to remove the same for wider participation or the bidder should plan for the dedicated encryption solution to deliver the same.		Answered in S.No. 415
417				The solution should have achieved at least EAL 2. The solution should be FIPS 140-2 Compliant.	Its a OEM Specific, Hence request to change the spec as "The Solution should have Achieved at least EAL 2 or FIPS 140-2 Compliant.		Requirement remains unchanged.
418				The Patch Management solution should support the heterogeneous environment i.e. multiple version of operating systems including but not limited to Microsoft, Unix, Linux, Mac OS, Sun Solaris etc.	Our Patch Management solution supports Windows, Linux & Mac only.		Solution should support multiple versions of OS proposed as part of the SLUDI solution.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
419		3.4.3.19 Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) with High Availability - TrendMicro TippingPoint		The solution should include the following capabilities at a minimum: •-the ability to analyse network traffic to detect intrusions, store data on attacks, block and modify malicious traffic; •-the ability to create custom intrusion policies; the ability to detect sensitive data such as identity number or credit card or personal information in ASCII text; •-traffic anomaly detection and event impact analysis to prevent zero-day attacks; •-capture traffic for evidence analysis in TCPDUMP-supported format for attack reproduction; •-signature categorization based on MITRE ATT&CK TTPs with incidents viewable on the dashboard based on MITRE ATT&CK mapping to comprehend attack stages; •-dynamic, real-time analysis to create a monitored network map, including parameters such as Host, Application, Protocols, IOCs, OS, and Vulnerabilities	**Request to remove the point related to DLP as DLP is not a functionality of NIPS		•-the ability to create custom intrusion policies; the ability to detect sensitive data such as identity number or credit card or personal information in ASCII text; The requirement should be read as "the ability to create custom intrusion policies;"
420		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		2. Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	Considering point 3 and 4 where appliance is required with license of 1Gbps throughput and support scalable inspection throughput of 5 Gbps scalable to 10 Gbps respectively, 4 x 40Gbps SFP interfaces may not be required or utilized. So, we request to consider changing the interface counts as follows: Should have 4X10Gbps and 2X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.		The requirement is dropped
421		3.4.3.15	235	Support for VRRP, QoS and full OSPF routing protocol.	VRRP is an open standard protocol used to provide high availability and fault tolerance for the solution. If the proposed solution includes it's own method to provide high availablity clustering (active/passive, active/active), is it necessary to include support for VRRP protocol?		Already answered in S.No. 303
422		3.4.3.17	241	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated environment without any need to connect with the Internet.	Threat protection functions such as IPS/vulnerability protection, Antivirus, C&C protection etc., require updates to be received on the firewall through the Internet to provide effective protection. Therefore, Is it acceptable to for the firewall to receive these updates through the Internet?		MSI should support offline update packages through internal distribution servers, or controlled DMZ proxies to ensure signature updates in isolated environments. Therefore, the requirement for the solution to operate without direct Internet dependency is retained, while permitting offline or proxy-based update mechanisms.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
423		3.4.3.17 Internal Firewall (Next-Gen) with High Availability		17. Firewall should have 8*10Gbps SFP integrated data ports, 8 x 100Gbps ports. Fiber interfaces should be populated with multi-mode transceiver modules.	If the customer agrees to reduce the 8 x 100Gbps ports to 6 x 100Gbps ports, a more cost-effective and optimized model can be recommended.		Answered in S.No. 411
424		3.4.3.26 Network Detection and Response (NDR)			What's the expected throughput?		The expected throughput should be minimum 45 Gbps
425					What's the required sensor count?		The MSI to calculate the sensor count based on the parameter provided.
426		3.4.3.21 Security Orchestration Automation and Response (SOAR) with High Availability			What is the required number of analyst licenses?(Concurrent)		6
427		3.4.3.13 Email Gateway with High Availability			What’s the expected mailbox count?		Please refer to demand capacity - Annexure 5. However, the minimum mailbox should be 2000.
428					What's the number of Email Routing (per hour)?		MSI to size the solution.
429		3.4.3.11 Security Information and Event Monitoring (SIEM) with High Availability			What's the number of servers which required FIM features & communication without depending WMI?		MSI to size the solution.
430					What's the number of endpoints which requires UEBA features?		2000 endpoints required UEBA features
431		3.4.3.5 Web Gateway with High Availability			What’s the expected user count?		2000 users for endpoints

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
432		3.4.3.2 Anti-Advanced Persistent Threat (APT) with High Availability			What's the required Nested VM count for & what are are the required windows & office licenses?		MSI to size the solution.
433		3.4.31		Solution should have Ability to exclude by application process name in removable storage device rules	Need clarity on this. Some thing related to Device Control means, request to remove / factor 3rd party integration for wider participation		Already answered in S.No. 412
434		3.4.31		Solution should support device control for endpoints	Device control is not the DLP Function. Hence request to modify the spec as " The Solution shoud support Whitelist / Black List the Removable Media Devices based on the Device Serial Number		Already answered in S.No. 413
435		3.4.31		The solution should allow encryption using strong algorithms as per industry best practices of the complete hard drive sector by sector.	its a OEM Specific one. Hence request to remove the same for wider participation or the bidder should plan for the dedicated encryption solution to deliver the same.		Already answered in S.No. 414
436		3.4.31		The solution should support encryption of extended partitions. The configuration for full disk encryption is controlled from the management console by selecting the drive letter that you intend to encrypt regardless of the partition type.			Already answered in S.No. 414
437		3.4.31		The solution should record the encryption status of each hard drive			Already answered in S.No. 414
438		3.4.31		The solution should have achieved at least EAL 2. The solution should be FIPS 140-2 Compliant.	Its a OEM Specific, Hence request to change the spec as "The Solution should have Achieved at least EAL 2 or FIPS 140-2 Compliant.		Alreadt answered in S.No. 417
439		3.4.3.5		The solution should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page and creation of custom URL categories for allowing/blocking specific destinations as required by the	Request to change the Spec as " The solution should support following actions like Permite, Block, Confirm , time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page and creation of custom URL categories for allowing/blocking specific destinations as required by the		Functionally if "monitor" is equivalent to "confirm" then suggestion is fine.
440	Annexure-3	3.4.1.17 Serv	115		"The solution shall have integration with Kubernetes Platforms and requisite controller/license/container plugin shall be provided with LB solution from day one. Controller/Plug-in should be from same make as LB. It should not be third party or opensource."	Native integration with Kubernetes is essential due to the significant shift toward microservices architectures.	Bidder's suggestion is fine. Bidder is at liberty to propose native integration with Kubernetes

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
441	Annexure-3	3.4.1.17 Serv	115		"The solution shall be provided in High Availability in Active-Active and Active-Passive Mode configuration, when deployed in dual mode and should have seamless takeover in-case if one device fails. It should also support in transparent failover between the devices, and support session mirroring, SSL mirroring, persistence mirroring, connection mirroring and heartbeat check. The solution must support N+1 architecture to provision more than 2 appliances in a HA cluster to acheive horizontal scaling"	Horizontal scaling is essential for future-proofing the system, ensuring it can efficiently handle increasing workloads as demand grows over time. By supporting N+1 architecture, the solution allows for the addition of more appliances to the HA cluster, enabling seamless traffic distribution and enhanced fault tolerance. While the current requirements may be met with an active-active or active-passive setup, the ability to scale horizontally ensures the system remains adaptable to future scalability needs and workload expansion.	Suggestion is accepted.
442	Annexure-3	3.4.1.17 Serv	115		"The proposed solution must handle high-capacity traffic, including L7 requests per second: 450K L4 connections per second:150K concurrent L4 connections:18M L4 throuput 20 Gbps on day 1 and scalable upto 25 Gbps"	There is currently insufficient clarity regarding the expected traffic requirements	Already answered in S.No. 300
443	Annexure-3	3.4.1.18 Glob	116-117		"The device should support 'n' number DNS QPS"	Clarity required on the number of expected DNS Request per second, which would help in sizing the appliacne	Already answered in S.No. 301
444	Annexure-3	3.4.1.18 Glob	116-117		"Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS and Must support resolution for A, AAAA, MX, and NS queries as External DNS"	The requirement ensures comprehensive support for diverse DNS query types (A, AAAA, MX, etc.) critical for both internal service resolution within the data center and external citizen access. This guarantees seamless connectivity, scalability, and reliability for all services in a high-availability environment catering to large-scale public use.	Already Answered in S.No. 302

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
445	Annexure-3	3.4.3.15 SSL V	232	Support for VRRP, QoS and full OSPF routing protocol.	"Support for VRRP or equivalent protocols"	A SSL VPN solution does not inherently require support for VRRP (Virtual Router Redundancy Protocol), QoS (Quality of Service), or full OSPF (Open Shortest Path First) routing protocol. These features are not directly related to the core functionality of an SSL VPN, which primarily focuses on securely connecting users to a private network over an encrypted SSL/TLS tunnel	Already answered in S.No. 303
446	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	242	11. RAM 64 GB	"11. RAM 128 GB"	To support 30 Gbps throughput, while preventing OWASP Top 10 and SANS Top 25 attacks, significant memory is required for packet inspection, state tracking, and rule processing. 64 GB RAM may cause bottlenecks under high traffic or attack scenarios. At least 128 GB RAM is essential to ensure performance, scalability, and reliable threat prevention.	Already answered in S.No. 304
447	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	12. SSL TRANSACTION 10000 CPS/TPS	12. 60K TPS (2K SSL TPS) SCALABLE UPTO 100K TPS (RSA 2k keys) WITH LICENSE UPGRADE	While the expected L4/L7 throughput is 30 Gbps, the SSL CPS must be at least 60,000 to handle modern workloads with high connection rates, such as API traffic, short-lived sessions, or bursts of new connections. Higher SSL CPS ensures the appliance can manage high concurrency and rapid connection setups without becoming a bottleneck, even during peak demand.	Already answered in S.No. 305

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
448	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	14. NETOWRK INTERFACE PORTS 24, 4*40	2 x 100G/40G QSFP28/QSFP+ ports 8 x 25G/10G SFP28/SFP+ ports	clarity required. In a modern spine-leaf network, the emphasis is on high-speed links (e.g., 10/25/100 Gbps) rather than a large number of ports. Efficient interconnections with aggregated uplinks reduce the need for devices with 24 ports. The architecture uses fewer, faster ports for scalability and performance, making excessive port counts unnecessary.	Already answered in S.No. 306
449	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	15. SSL THROUGHPUT 2 GBPS	35 Gbps bulk encryption scalable upto 50 Gbps bulk encryption with license upgradation	While the expected L4/L7 throughput is 30 Gbps, SSL throughput must exceed 2 Gbps to handle real-world workloads where most traffic is encrypted. Modern applications with high HTTPS usage and frequent key exchanges demand higher SSL capacity to prevent performance bottlenecks.	Already answered in S.No. 307
450	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243		The solution should provide OWASP Compliance Dashboard which provides holistic and interactive interface that clearly measures app's compliancy against the Application Security Top 10 attacks and also provide suggestions/shortcuts to address the compliances and configure policies for it.	The OWASP Compliance Dashboard is not just a feature—it is a critical tool for enhancing, monitoring, and ensuring the security of applications against modern threats. By incorporating it, the solution provides an efficient, scalable, and proactive approach to safeguarding applications, aligning with industry standards, and addressing the challenges of modern application security.	Already answered in S.No. 308

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
451	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243		Proposed hardware platform should be of high performance, highly scalable, and purpose-built next Generation platform for application security and Web Application Firewall (WAF) from same OEM running on same OEM OS version and platform; Web Application solution should not be virtual WAF and it should not white labeled WAF running on third party hardware.	The requirement ensures a purpose-built, high-performance hardware platform designed specifically for application security and WAF, maximizing compatibility, stability, and performance. Avoiding virtual or white-labeled solutions ensures the platform leverages native OEM optimizations, unified support, and streamlined updates, reducing dependency on third-party hardware or software.	Already answered in S.No. 309
452	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	sl no 2. Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	Should have 2 x 100G/40G QSFP+/QSFP28 ports8 x 25G/10G SFP28/SFP+ ports	The requirement for 2 x 100G/40G QSFP+/QSFP28 ports and 8 x 25G/10G SFP28/SFP+ ports ensures that the appliance can handle high-bandwidth demands and future scalability. The 100G/40G ports support environments with heavy traffic aggregation, ideal for data centers or high-performance networks, while the 8 x 25G/10G ports accommodate flexible connectivity for lower-speed links or incremental upgrades.	Already answered in S.No. 310

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
453	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	Sl No. 4. Present license should be for 1 Gbps throughput.	System should have 20 Gbps L4 througput sclable upto 25 Gbps with license upgrade without additional hardware	While the RFP specifies a 1 Gbps license, the expected L4/L7 traffic is up to 30 Gbps. For a robust DDoS solution, a minimum 20 Gbps throughput is essential to handle real-world attack scenarios effectively. DDoS attacks often involve massive volumes of traffic, requiring the solution to process and mitigate large-scale attacks while still maintaining legitimate traffic flows. A 1 Gbps license would be insufficient to address peak traffic requirements or volumetric attacks, leaving the network vulnerable. A minimum 20 Gbps ensures adequate capacity to protect critical infrastructure without compromising performance.	Already answered in S.No. 311
454	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	Sl No. 5. Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	Point may please be dropped	The requirement for a fixed latency of <75 microseconds should be reconsidered, as latency is influenced by multiple factors beyond the hardware's capabilities, including network topology, connection quality, external routing, and environmental conditions	Already answered in S.No. 314
455	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	"SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 7000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key from day 1 and scalable upto 15K TPS."	While Layer 3/4 DDoS solutions primarily focus on mitigating attacks based on packet headers, traffic patterns, and volumetric anomalies without decrypting encrypted traffic, the growing volume of encrypted traffic in modern networks can indirectly impact overall resource utilization during an attack. Hence looking at the future scalability we propose higher ssl tps .	Already answered in S.No. 313

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
456	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	The solution should support at least 2 million packets per second on each box from day 1.	"The solution should support at least 18M L4 Concurrent connections"	Calculating packets per second is impractical due to variable packet sizes. Connections per second (CPS) is a more reliable metric for measuring performance and capacity.	Already answered in S.No. 314
457	Annexure-3	3.3.3.10 API (	53	The proposed solution shall provide API Lifecycle maintenance capabilities including definition, creation, security, monitoring and management	"The proposed solution shall provide API Lifecycle maintenance capabilities including definition, security monitoring and management."	The point "creation" can be removed because API creation typically involves the application logic and development process, which is outside the scope of an API management solution. The focus of the proposed solution should remain on API lifecycle maintenance, covering critical aspects like definition, security, monitoring, and management, which are essential for optimizing and governing APIs once they are developed, rather than including their initial creation.	Already answered in S.No. 315

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
458	Annexure-3	3.3.3.10 API (	53	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.	"The proposed solution shall have the capability to externalise APIs and should provide cataloguing capabilities with third party integrations."	API cataloguing is not inherently a primary function of API gateway servers, as the core purpose of an API gateway is to manage, secure, and route API traffic. Their primary responsibility is to act as a central access point for APIs, handling authentication, load balancing, rate limiting, and request/response management. For advanced cataloguing capabilities such as detailed documentation, taxonomy management, or developer portal integration, leveraging third-party solutions is more appropriate. This ensures that the proposed solution remains focused on its core competencies while allowing seamless integration with external cataloguing tools to meet the requirement.	Already answered in S.No. 316
459		Patch Management Solu		The Patch Management solution should be Agent based/Agentless	The solution is completely agent based. Request you to consider changing it to agent based		Clause remains unchanged. The Patch Management solution shall support agent-based deployment, agentless deployment, or a combination thereof. The solution shall ensure complete patch coverage, compliance reporting, and secure operations across all supported endpoints
460		Patch Management Solu		The offered solution should have the capability to discover the Assets operational across SL-UDI's locations i.e. Scan the network to produce a full inventory of IT assets, and provide flexible ways to group and classify these assets.	The scanning of all the IT assets shall be done by the vulnerability tool i.e Tenable Security Center. As our VM & PM solutions can be bi-directionally integrated , the scannned assets for which patches are available & the potential impact are showcased on the PM console as well.		The requirement remains unchanged.
461		Patch Management Solu		The Patch Management solution should support the heterogeneous environment i.e. multiple version of operating systems including but not limited to Microsoft, Unix, Linux, Mac OS, Sun Solaris etc.	Our Patch Management solution supports Windows, Linux & Mac only.		Solution should support multiple versions of OS proposed as part of the SLUDI solution.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
462		Patch Management Solu		The Patch Management solution should have the ability to manage PCs, Laptops, Servers, Routers, and Printers etc. on the network.	Our Patch Management solution is purely agent based solution and doesn't support network devices currently		Clause remains unchanged.
463		Patch Management Solu		The solution should be able to remove and create network shares at any time.	Please provide more info on why is this required in a PM solution		Clause remains unchanged.
464	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.9 Hardware Security Module (HSM) with High Availability	202	Hardware Security Module (HSM) with High Avai	Total Number of HSM (Count)		Total Three - 1 HSM that can be partitioned. 1 backup HSM. 1 for the authentication
465	SCHEDULE OF REQUIREMENTS Volume 02 of 03 Two Stage Bidding Procedure	5.8.2.3 HSM I	89	(iii) In the event of a catastrophe, such as a flood or fire, it might lose both your working HSMs and locally stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote location.	Total Number of Back-Up HSM (Count)		1 backup HSM
466	SCHEDULE OF REQUIREMENTS Volume 02 of 03 Two Stage Bidding Procedure	3.4.3.19 Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) with High Availability - TrendMicro TippingPoint		Management: a. Should support SNMP V1 to V3 b. Should support HTTPS c. Should support SSH/TELNET d. Should support Console	We do not support SNMP V1, only SNMP V2 and SNMP V3 are supported.		Agreed.
467	SCHEDULE OF REQUIREMENTS Volume 02 of 03 Two Stage Bidding Procedure	3.4.3.19 Intrusion Detection System/ Intrusion Prevention System (IDS/IPS) with High Availability - TrendMicro TippingPoint		The solution should include the following capabilities at a minimum:	**Request to remove the point related to DLP as DLP is not a functionality of NIPS		Already answered in S.No. 419

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
468		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		2. Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	Considering point 3 and 4 where appliance is required with license of 1Gbps throughput and support scalable inspection throughput of 5 Gbps scalable to 10 Gbps respectively, 4 x 40Gbps SFP interfaces may not be required or utilized. So, we request to consider changing the interface counts as follows: Should have 4X10Gbps and 2X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.		Already answered in S.No. 310
469		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		3. System should have scalable inspection throughput of 5 Gbps scalable to 10 Gbps without additional hardware.	Please confirm if 5 Gbps scalable to 10Gbps is the Mitigation/Attack traffic expected to be dropped/blocked by the Appliance.		Item is dropped
470		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		4. Present license should be for 1 Gbps throughput	Please confirm if 1Gbps is the Clean/Legitimate traffic expected to be passed by the Appliance.		Item is dropped
471		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		5. Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	We request to change the latency parameter from 75 microseconds to 80 microseconds.		Item is dropped
472		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		9. The solution should support at least 2 million packets per second on each box from day 1.	Considering point 3 where appliance is required to support scalable inspection throughput scalable to 10 Gbps, a DDoS attack launched in both inbound and outbound direction using smallest packet of 64 bytes will require appliance to support atleast 30 million packets per second. Packets per second values have to be built in to the appliance from Day 1 and cannot be increased without changing the hardware. So we request to change this point as follows: The solution should support at least 30 million packets per second on each box from day 1.		Item is dropped
473		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		23. Inspection and prevention is to be done in hardware.	The proposed Anti-DDoS appliances are built for DDoS inspection and prevention using dedicated, purpose built software architecture that runs on a dedicated hardware, this allows flexibility to incorporate quick changes, feature enhancements, product improvements, etc., hope this approach is acceptable.		Item is dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
474		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		36. System provides behavioral-DoS protection using real-time signatures.	Behavioral DoS protection using signatures is prone to false positives and overblocking (legitimate traffic blocked), there are other better methods for behavioral DoS protection that are more accurate, so we request to change this point as follows: System provides behavioral-DoS protection using any of the methods like real-time signatures, host behavioral protection, anti-spoofing, TCP authentication, DNS authentication, etc.		Item is dropped
475		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		40. Should support IP defragmentation, TCP stream reassembly.	Our understanding is that the solution is expected to detect and mitigate fragmented packet attacks, please confirm.		Item is dropped
476				47. System should support anti-evasion mechanisms.	Our understanding is that the solution is expected to detect and mitigate evasion mechanisms using methods like Behavioral Analysis, Challenge-Response Mechanisms, Protocol Deviation Detection, etc., please confirm.		Item is dropped
477				56. System supports HTTP Challenge Response authentication without Scripts.	Our understanding is that the solution is expected to detect and mitigate HTTP based attacks that can be done using many other methods, in fact modern day botnets are capable of bypassing http challenge response authentication. So, we suggest to modify this point as follows: System supports HTTP-based attack protection without scripts using any of the methods like Challenge Response authentication,HTTP Regex. Malformed HTTP filtering, Botnet Prevention, Threat Intelligence, etc.		Item is dropped
478		3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability			What is the Support duration required for the Anti-DDoS appliance ?		Item is dropped
479		3.4.3.26 Network Detection and Response (NDR)		7. Automatically discovers and classifies device and set up device groups based (critical assets, workstation..etc)	Request to change this as follows: Automatically or manually discovers and classifies device and set up device groups based (critical assets, workstation..etc)		The clause remains unchanged
480		3.4.3.26 Network Detection and Response (NDR)		14. The solution should leverage both packet capture and flow based technologies	NDR utilizes either packet or flow data not both. Secondly, this point contradicts with point # 1 that states "Analyze raw network packet traffic in real time or near real time.", so we request to change this point as follows: The solution should leverage both packet capture or flow based technologies		The clause remains unchanged

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
481		3.4.3.26 Network Detection and Response (NDR)		21. Even if the license exceeded, the NDR platform must work normally from technical perspective	The proposed solution uses license to enforce the number of monitored elements, traffic/data from any monitored elements in excess of the purchased license are not processed. Hope this approach is acceptable.		The clause remains unchanged
482		3.4.3.26 Network Detection and Response (NDR)		23. The solution should provide ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.	The proposed solution is packet based as required in point # 1, so analysis is using packet and not flow. So, we request to change this as follows: The solution should provide ability to establish “normal” traffic baselines through flow or packet analysis techniques and the ability to detect deviations from normal baselines.		The clause remains unchanged
483		3.4.3.26 Network Detection and Response (NDR)		24. Unsupervised and supervised machine learning along with probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.	The proposed solution uses deterministic ML techniques to detect threats as this method minimize false positives, hope this approach is acceptable.		The clause remains unchanged
484		3.4.3.26 Network Detection and Response (NDR)		26. The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall/endpoints/NAT gateway that are associated with a single conversation and present them as a single bi-directional flow record including traffic traversing NAT devices.	Flow record stitching is a NetFlow feature and does not apply to packet based solution. So, we request to delete this point.		The solution shall be capable of correlating and presenting a single logical bi-directional conversation by stitching flow/session information derived from packets, flow records, or equivalent mechanisms, including across NAT devices
485		3.4.3.26 Network Detection and Response (NDR)		29. The solution must be able to consume flow information from the network in the form such as Netflow V5, Netflow V9, IPFIX, sFlow, Jflow, cFlowd, NSEL as well as port-mirrored traffic to perform behavioural analysis.	This point is specific to NetFlow and does not apply to packet based solutio, so we request to delete this point.		The requirement mandates the ability to consume flow and packet inputs where available; it does not restrict the solution to NetFlow-only architectures. Therefore, the clause remains applicable
486		3.4.3.26 Network Detection and Response (NDR)		35. The solution should have the ability to state fully reassemble unidirectional flows into bi-directional conversations; handling deduplication of data and asymmetry and eliminate redudant telemetry to improve system performance.	This point is specific to NetFlow and does not apply to packet based solutio, so we request to delete this point.		The clause remains unchanged
487		3.4.3.8 1			What are the other custom applications that are being deployed, what technologies are they, are they thick client or thin client?		No custom applications from GoSL side. Entire SL-UDI system will be implemented by the MSI. There is a data interfacing requirement with eNIC system.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
488		3.4.3.8 2			LDAPv3 compliant is looking for our Data store being LDAPv3 compliant or the customer wants to integrate their LDAPv3 compliant data store with us?		There are no legacy LDAPv3 compliant from GoSL side.
489		3.4.3.8 3-6			Customer is looking for on-prem solution or SAAS solution? If on-prem, our solution is self managed deployed in customer premise, and these parameters are not applicable		On-prem. Our IDAM is on-prem solution hence any SAAS parameters should be ignored.
490		3.4.3.8 14			What is the usecase of SNMP protocol? Is it an application talking that protocol needs to be integrated?		No application-layer protocol integration via SNMP is needed.
491		3.4.3.8 36			What type of legacy applications are there? Are they web based or thick client?		None.
492		3.4.3.4 22			Is MDM capability being looked or the Ping solution is expected to integrate with an MDM solution?		MDM capability and solution is not required.
493		3.4.3.3 (whole PAM requirements)			Are the requirements only for privileged accounts or normal accounts are also being looked at here?		The requirement is only for privileged accounts.
494					Please confirm whether the implementation scope covers internal users, external customers, or both. Kindly describe all user types expected to be onboarded.		It is only for internal users
495					Confirm the total number of applications planned for integration within the current scope of work.		This is internal to MSI based on solution required may provision necessary privilege accounts, which would be later transferred to MSP.
496					Provide a breakdown of how many applications are on-premises, hybrid, and cloud-based.		Entire solution is on-premise.
497					Clarify whether all applications to be integrated are currently available, or if some will be developed or acquired as part of this RFP.		No legacy applications are required to be integerated or acquired for maintainence.
498					Identify the golden repository or authoritative source of user identities (e.g., AD, HRMS, CRM).		Query is not clear
499					Confirm the number of environments required to be set up, including Disaster Recovery (DR).		Refer to Volume 02 section 5.2.2
500					What is the preferred deployment model — On-Premises, Hybrid, or Private Cloud?		On-premise only
501					Should the setup be deployed on Virtual Machines (VMs) or through a containerized environment (e.g., Docker/OpenShift)?		Deployment strategy to be decided by MSI and detailed out in the technical proposal
502					Specify which SIEM or logging solution is currently being used by the customer.		There is no legacy SIEM or logging solution
503					Confirm whether the customer is open to a hybrid execution model		Query is not clear
504					Indicate if the customer requires any post-production support / 24/7 support or managed services following implementation.		O&M requirements are clearly specified in volume 02

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
505		3.4.3.3		The proposed solution must offer a SDK or programming libraries for inclusion within the source code of internally developed software.	How many application servers are there in the environment for which SDKs are required?		Already answered in S.No. 339
506		3.4.3.3		The proposed solution must support zero information disclosure error messages to prevent logs from displaying sensitive information.	Pls help elaborating the requirement here.		Already answered in S.No. 340
507		3.4.3.3		The proposed solution's account segregation hierarchy must support an inheritance model for resources and policies.	Pls help elaborating the requirement here.		Already answered in S.No. 341
508	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	What are the exact locations and addresses of the Primary Data Center (PDC) and Disaster Recovery (DR) sites?		Will be shared later with the selected MSI.
509	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	What will be the distance between from DC to DR location		Already answered in S.No. 21
510	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	Are these data centers owned by GoSL or hosted by a third-party provider?		GoSL
511	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	What is the tier level or certification of these data centers (e.g., Tier III, Tier IV, ISO 27001)?		Tier III ISO 27001 compliant. However, this information will be issued upon confirmation from GoSL

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
512	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	Will the data centers provide existing racks, power, cooling, and network connectivity, or should MSI include these in the scope?		Racks to be supplied by MSI. Power and coolling to be provided by data center service provider. Telecom to be provided by GoSL. Space for 20 racks is available in the DC. 3,5 and 7 KVA of racks can be configured and 4 high density racks can be configured.
513	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	Can GoSL provide existing site diagrams and rack layouts for reference?		GoSL will provide the Co-location space for the DC-DR . The MSI to propose the solution as per the RFP meeting the SLAs .
514	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	Can you please confirm the the space be provided in a ready-to-use condition (flooring, false ceiling, lighting, etc.), or should the MSI include civil work in the scope if any ..		Space will be provided in ready-to-use condition
515	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	Will power supply and backup (UPS, DG sets) be provided by GoSL, or should MSI provision these		Non-IT (UPS, DG sets) to be provided by Data Centre Serv Provider
516	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	What will be the load bearing capacity to place rack in both DC and DR location		Data center is Tier III compliant.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
517	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	Please confirm whether GoSL will be responsible for obtaining all necessary approvals and clearances from relevant government authorities for site setup, ensuring there are no delays or showstoppers in the implementation process		Yes
518	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	Are these sites Tier III certified, and what physical facilities (power, cooling, fire suppression, access control) are already provisioned?		Non-IT (power, cooling, fire suppression, access controlled) to be provided by Data Center Serv Provider .
519	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	a. Clear floor-to-ceiling height and load-bearing capacity (both point load and uniformly distributed load). b. Available space (in square feet) for in-building facilities for staging area c. Availability of service lifts along with their load-bearing capacity. d. Availability of mains power supply (HT or LT line) and approved power load in kW.		Will be shared later with the downselected MSI.
520	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation with GoSL for setting up of site,	a. For HT lines, specify the KV rating (eg. 11 KV / 33 KV / 66 KV) and number of lines. b. For LT lines, specify input voltage (e.g., 415 Volts) and number of inputs. c. Availability of DG power, including capacity and redundancy details.		Query is not relevant
521	Vol-2	5.2.1	49	5.2.1.1 Data Center Strategy of Project GoSL shall utilize its data center for hosting IT Infrastructure in Primary Data Center and Disaster Recovery. The Primary Data Center and Disaster Recovery sites will be in two separate data centers. MSI shall undertake assessment of the data centers, prepare a site plan and rack plan.	How will fiber-based connectivity for DC–DR replication be provisioned and tested?		Connectivity between DC and DR will be provided by telecom service provider, selected by GoSL. The bidder shall specify the bandwidth requirement.
522	Vol-2	5.2.2	50	5.2.2 Hosting Environments a. Development b. Quality Assurance c. Service Creation d.Staging	As per the RFP, the bidder is required to provision Development, Quality Assurance, Service Creation, and Staging environments. Could you please confirm the expected downscale ratio for these environments compared to the Production environment (for example, 50%, 25%)?		As per Industry standard. Bidder to decide.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
523	Vol-2	5.2.3	56	5.2.3 Installation, Configuration and Testing Internet Connectivity Internet for mobile registration centers MSI will be required to provide secure and reliable internet dongles for connectivity of mobile registration centers with the DC and DR	Could you please confirm the total number of Mobile Registration Centers, so that the bidder can plan for the corresponding number of dongles? This information is critical as it will have a direct impact on the commercial proposal.		40. Internet dongle is the responsibility of GoSL.
524	vol-2	5.3.3.	64	5.3.3 Service Centers and Spares In order to ensure uninterrupted enrolment services, the MSI for enrolment kits would be responsible. The MSI will be responsible for monitoring of the spares and maintenance activity of the enrolment kits and report deviations to the expected performance levels to GoSL.	Could you please clarify whether the bidder is required to maintain spare devices at all registration locations, or if there are specific guidelines to meet the RFP requirements? This clarification is important as maintaining spares across all locations could have a significant commercial impact.		Bidder has to plan appropriate provisioning of spares to meet the SLAs.
525	Vol-2	5.4	65	5.4 Enrolment Centers GoSL is setting up a wide network of registration centers across the country. The citizens can do their biometric registration (and updates) in these registration centers. These centers will be located in identified premises and will have the government staff to undertake the registrations under the SL-UDI program. The civil and electrical setup in these centers will be managed by the GoSL. In addition, the seating arrangements for citizens as well as government staff (including furniture) will also be made by the GoSL. GoSL needs to facilitate requirements from the MSI for monitoring. The MSI needs to do the following: • Network Connectivity: Monitor and support the network connectivity from enrolment center to DC/DR (refer Section 5.2.6)	Could you please clarify and confirm the number of locations that will be connected through the WAN network and the number of locations that will require dongle-based connectivity? This information is essential for the bidder to design the architecture appropriately.		The responsibility of providing bandwidth connectivity rests with GoSL. The bidder is requested to suggest the appropriate bandwidth size. For mobile registeration centers, Internet dongles will be provided by GoSL.
526	Vol-2	5.8.1.3	77	5.8.1.3 Security Components for Implementation 18. Virtual Desktop Infrastructure (VDI) VDI licensing is generally per user. In SL-UDI only certain internal users will be requiring VDI capabilities as per business requirement (Exact number can be decided once the manpower strength is estimated)	Please share the expected number of VDI users so that the bidder can factor this into the solution design. This information is critical as it will have a significant commercial impact.		VDI Solution is not required
527	Vol-2	5.8.1.7	80	5.8.1.7 Security Requirements – Security Operations 2. Implement SOC infrastructure, security tools and integrate with the SL-UDI network.	Please confirm whether the Security Operations Center (SOC) is required to be set up at the bidder's premises or at GoSL's premises. If it is to be established at GoSL's premises, kindly provide the location details along with seating capacity and any other infrastructure requirements that need to be considered for planning.		SOC and NOC will be setup at the premises provided by GoSL in srilanka. Exact location will be shared with the successful bidder.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
528	Vol-2	5.8.2	85	5.8.2 Business Continuity and Disaster Recovery (ii) MSI shall endeavor **zero data loss while switching from Primary Site to Disaster Recovery site** by maintaining a very high level of RTO and RPO.	The RFP requires zero data loss during failover between Primary and DR sites by maintaining stringent RTO and RPO objectives. Industry best practices recommend Near-DC and Near-DR sites within approximately 25 km of the respective primary and secondary data centers to achieve synchronous replication and near-zero data loss. Please confirm if this guideline applies to the SL-UDI project or if GoSL has defined specific requirements for DC and DR site proximity.		RTO and RPO will be as per RFP, which is 1 and 4 hours respectively. The distance between DC and DR will be within 25Kms. Only DC and DR are envisaged in this RFP.
529	Vol-2	5.8.2.2	87	5.8.2.2 Data Backup d. Tapes shall be moved by MSI to offsite location on Daily basis at a geographically separate location with appropriate physical security controls, at par with banking regulator of Sri Lanka for such secure transfer, arranged by MSI.	The RFP states that tapes must be moved by the MSI to an offsite location on a daily basis, at a geographically separate site, with appropriate physical security controls in line with the standards of the banking regulator of Sri Lanka. Please clarify: a. Does GoSL have any specific guidelines or approved vendors for secure tape transportation and offsite storage? b. Is the bidder expected to arrange and manage the offsite facility independently, or will GoSL provide any designated location? c. What is the minimum distance or geographic separation required between the primary data center and the offsite tape storage location?		MSI is responsible to take backup in the tape library and hand it over to GoSL. It will be the responsibility of GoSL or its nominated agency to ship it to a remote location.
530	Vol-2	5.8.2.4	89	5.8.2.4 VPN Access (i) MSI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible	The RFP specifies that MSI shall enable remote working for Data Center staff via VPN in case the sites are physically inaccessible, keep VPN facilities enabled for key staff, and allow operations from locations designated by GoSL during such scenarios. Please clarify: a. How many key staff members are expected to have VPN access for remote operations? b. Are there any bandwidth or performance benchmarks defined for VPN connectivity to ensure smooth operations?		MSI needs to solution this as per their assessment of the requirements asked in RFP for implementation/O&M phase.
531	Vol-2	5.8.2.3	89	5.8.2.4 HSM Recovery (iv)Execute recovery plan at least semi-annually (every six months) to ensure that fully recover key material.	The RFP specifies that encryption keys for HSM Backup and Recovery to be Offsite location (other than DC and DR) in fireproof safe and biometric enabled locker. Please clarify: a.What are the Offsite location for stroage of keys? b.Does offsite location's fireproof and biometric enable locker in place?		a. Offsite location details will be shared later. b. To be supplied by GoSL
532	Vol-2	5.8.2.6	91	5.8.2.6 Retention (iii) Daily Backup: Core data shall be backed up on a daily basis and shall be maintained for two weeks along with version history on unique media. No tape shall be overwritten for two weeks, including daily incremental.	RFP specifies that Backup is done to tape. For short tem Disk to disk backup is preferred for faster recovery. For Archival of data, Tape can be used as per Archival policy.		Back up must be taken for Tape. For short term , disk to disk backup may be proposed by the bidder.
533	Vol-2	5.8.1	73	The security solution of SL-UDI Information System should comply with the international security standard ISO 27001	whether ISO 27001 Certification of the Sytem and infrastucture is in the MSI scope ?		The processes and controls adopted by MSI as per statement of applicability should be compliant to ISO27001 (latest release).
534	Vol-2	5.8.1.7	80	8. Support SL-UDI during external certification and other security audits – such as ISO 22301, ISO 27001, etc.	Whether ISO Certification of the Certification of the Sytem and infrastucture is in the MSI scope or is it to support during Audits? What other certifications in addition to ISO 27001 and ISO 22301 are expected to be supported		MSI shall support these certification process.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
535	Vol-2	5.8.1.8	81	6.MSI shall develop and implement processes and response procedures for business continuity and disaster recovery. MSI shall ensure compliance to ISO 22301 standard.	whether ISO 22301 Certification of the Sytem and infrastucture is in the MSI scope ?		MSI shall support these certification process.
536	Vol-2	5.8.3	91	Review / Augment the information security policy and privacy policy that will provide the baseline controls to be implemented across SL-UDI ecosystem.	Please provide the data privacy Requirement		Compliant to PDPA act of Srilanka
537	Vol-2	5.8.2	86	(iv) Both RPO and RTO will be discussed and agreed between SL-UDI and MSI during the design phase. MSI shall indicate the RTO and RPO of their solution in the technical response to the RFP.	Please provide Indicative range for RTO and RPO		Answered in 528
538	Vol-2	4.1.5	9	Changes in the application as an outcome of UAT shall not be considered as a Change Request. The MSI will need to rectify the observations raised.	Its is assumed that it will be on the basis of the size of the change request. Change request having architectural impact or having high implementation efforts will have an impact on plan and schedule. We assume the defination of change and its impact considerations will be agreed at the start of the project		No
539	Vol-2	4.1.3	4	4.1.3 Design - Point iii - subpoint b & c	Will there be a assigned member from goSL to approve the high and low level designs ?		Project Governance structure will be in place.
540	Vol-1	4.12.4	86	HW Payment Milestones: 1. Advance Payment - 10% of P1 2. On Supply - 60% of P1 3. On Acceptance of HW system - 10% of P1 4. Go Live - 5% of P1 5. Operational Stabilization of Iteration 2 - 15% of P1	All capex payment should be paid upfront and not linked to Go Live or operational stabilization. Request you to change payment milestones as below. 1. Advance Payment - 10% of P1 2. On Supply - 80% of P1 3. On Acceptance of HW system - 10% of P1		No change
541	Vol-1	4.12.4	86	SW Payment Milestones: 1. Advance Payment - 10% of P2 2. On Supply - 60% of P2 3. On Acceptance of SW system - 10% of P2 4. Go Live - 5% of P2 5. Operational Stabilization of Iteration 2 - 15% of P2	All capex payment should be paid upfront and not linked to Go Live or operational stabilization. Request you to change payment milestones as below. 1. Advance Payment - 10% of P2 2. On Supply - 80% of P2 3. On Acceptance of HW system - 10% of P2		No change
542	Vol-1	4.12.4	86	Registration kits, including the cost of Fingerprint Scanner and Iris Scanner Payment Milestones: 1. Advance Payment - 10% of P4 2. On Supply - 60% of P4 3. On Acceptance of Kits - 10% of P4 4. Go Live - 5% of P4 5. Operational Stabilization of Iteration 2 - 15% of P4	All capex payment should be paid upfront and not linked to Go Live or operational stabilization. Request you to change payment milestones as below. 1. Advance Payment - 10% of P4 2. On Supply - 80% of P4 3. On Acceptance of HW system - 10% of P4		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
543	Vol-1	4.12.4	87	Software ABIS with manual adjudication, SDKs (Fingerprint, Iris and Facial), Operating System, Database Cost of license of SDKS for registration and Authenticator Systems required Cost of Authentication devices - Payment Milestones: 1. Advance Payment - 10% of P5 2. On Supply - 60% of P5 3. On Acceptance of SDK Licences - 10% of P5 4. Go Live - 5% of P5 5. Operational Stabilization of Iteration 2 - 15% of P5	All capex payment should be paid upfront and not linked to Go Live or operational stabilization. Request you to change payment milestones as below. 1. Advance Payment - 10% of P5 2. On Supply - 80% of P5 3. On Acceptance of HW system - 10% of P5		No change
544	Vol-1	4.12.4	87	P7 - For IT hardware, software and registration kits, three years of annual technical support (ATS) and annual maintenance cost (AMC) are required. - Quarterly Invoice	Request you to change the payment to Annual Invoice in advance against the receipt of ATS / AMC support being extended		No change
545	Vol-1	4.12.5 TABLE 1 for P1; 4.12.6 TABLE 2 for P2; 4.12.8 TABLE 4 for P4: 4.12.8.1 TABLE 5 for P5:	88	***Price Bid table as per RFP*** ***Prices in INR*** Total Quantity (F) Price INR E X F = (G) Taxes INR (H) Total Price (I) = F+G+H	Total price formula I = F+G+H where as F stands for total quantity. The formaula need to be changed to Total Price (I) =G + H. Please clarify if this understanding is correct. **Request to share the Xls format of Price Bid coprising of all tables with formula**		Can be shared on request
546	Vol-1	4.12.7 TABLE 3 for P3 4.12.9 TABLE 6 for P6:	92	***Price Bid table as per RFP*** ***1. (c)*** ***The unit of measurement (column number E) should be in person-month numbers*** ***2. Total Price in INR T=C+D***	1. Incorrect coulmn reference given 2. The total price formula as per the RFP mentioned as T=C+D whrere as C denotes Base Rate Per Person Per Month. Request to correct the formula and amend suitaby.		Column of Total Base Price should be read as D=B x C. Total Price in INR should be read as F=D+E
547	Vol-1	C. Submission and Opening of Bids	27	Employer/NISG reserves the right to vary the quantities in Section VI (Schedule of Requirements) of Volume 2 by increasing or decreasing them by up to 25%	Please clarify how such variations will impact the overall contract value or who will bear the financial implication of such changes. In the event of change in quantities, will the contract value be adjusted proportionately based on the unit rates quoted in the financial bid?		Yes, contract value will be adjusted proportionately.
548	Vol-1	3.1.2.5	31	D1 Qualification, certification and experience of the MSI's team D1.1 Leadership D1.2 Architects D1.3 Engineers D1.4 Track Leads D1.5 BSP engineers	Please clarify how many resumes are required to be submitted to get full marks under secion D1		Lead and alternate for each position.
549	Vol-1	4.4.2 Key Personnel Details	66	General qualifications	Please clarify what are the General Qualifications should be mentined for this ask in RFP CV format		Please refer to annexure 10 manpower requirement.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
550	Volume-1	19.5 b)	15	Locally supplied Products: Unit prices of Products offered from within the Employer's Country shall be quoted on a CIF basis.	Locally supplied products should be quoted on a DDP basis ?		Agreed.
551	Volume-1	ITB 6.1 Status of Sub-Contractors	25	Sub-Contractors' qualifications under "a," "b," and "c" shall be taken into account when assessing the Bidder's overall qualifications. a) Biometric Devices b) Automated Biometric Identification System Solution c) Systems Integration	Can sub contract additional items not only following? A) COTS Hardware delivery B)Islandwide support for Biometric devices Because it is required a local party to import hardware to Sri Lanka and there must be a local party to provide islandwide support to Biometric devices.		Agreed. But the entire responsibility is with the MSI.
552	Volume-1	Conflict of Interest	33		Conflict of Interest ITB 3.3 is applicable for sub-contractors as well? There is a contradiction with ITB 6.2 because it is clearly mentioned there, one sub-contractor can work with multiple bids if it is not a JV partner or lead bidder in another bid.		No change
553	Volume-1	4.12.7	93	These resources can be made available during migration to New Data Center and Disaster Recovery site if required	Is this valid? Because there is no migration in this scope.		Solution will be deployed in GoSL provided DC and DR
554	Annexure-1	1.3	6	Connectivity between two Data Centers	Will GoSL provide the sufficient connectivity between two DCs or bidder has to provide that?		Connectivity between DC and DR will be provided by telecom service provider, selected by GoSL. The bidder shall specify the bandwidth requirement.
555	Annexure-2	2.2	16	Hence to have high availability, the applications must have low downtime and low recovery time.	Please define the allowed down time and recovery time		Clause is self explainatory
556	Annexure-3	3.2	3	a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023	There were reports published in 2024 and 2025 as well, in that case bidder has to refer 2021,2022,2023 reports or 2023,2024,2025 reports?		2022-2025
557	Annexure-3	3.2	3	the Vendor has to mandatorily provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023.	Can bidder consider case studies in 2024, 2025 as well?		Revised to 2024, 2025.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
558	Annexure-3	3.4.1.1	79	Blade Servers	Is it mandatory to propose Blade Servers?		Bidder has to design and implement the solution. It is not mandatory to propose blade servers. The bidder has the liberty to design the solution using server types and its composition.
559	Annexure-3	3.4.1.5	89	The Proposed storage system should support Active-Active Storage configuration across two sites replicating to each other for same LUN/volume for zero RPO/zero RTO configuration.	Achieving zero RTO,RPO is not practically possible, specially considering the latency between two sites. Therefore please propose practically achievable RPO/RTO values.		No change
560	Annexure-3	3.4.1.5	89	The proposed storage array should support Three-Data-Center (3DC) replication, ensuring robust disaster recovery and high availability	Is this mandatory? Because the solution will be deployed in two Data centers		Not mandatory and the requirement is dropped.
561	Annexure-3	3.3.3.10	53-56	The proposed solution shall be on premise solution and not a cloud-based solution.	Are cloud services such as those provided through cloud service providers, however delivered as on-premise deployments such as AWS Outposts, Azure Stack etc. acceptable. They can operate in complete isolation or managed via the cloud service provider. If the infrastructure is on-premise yet management and control plan in a public cloud is acceptable?		No. The solution will be deployed in GoSL provided DC and DR. Public cloud management is not acceptable.
562					If the infrastructure is on-premise yet management and control plan in a public cloud is acceptable?		No
563	Annexure-3				Is a hybrid model where the control plane of the API Gateway is hosted in cloud and data plane (gateways) are hosted on premise, acceptablable?		No
564	Annexure-3	3.3.3.10	53-56	The proposed solution shall have capabilities for Mobile Integration	Requirement is unclear. Typically Mobile applications will consume APIs (REST/AsyncAPI, GraphQL, WebSocket) published by the API gateway. In addition to making available such mobile friendly API's, is there anything else expected here?		The clause is self explainatory
565	Annexure-3	3.3.3.15	62-63	The SL-UDI services preferably be integrated using open source/standard version of Enterprise Service Integration platforms	For open source versions of such platforms - would you require enterprise support, or would community support be acceptable?		Enterprise support is required.
566	Annexure-3	3.3.3.19	76-78	N/A (General)	Will the application servers / web servers be deployed on containers / Kubernetes or on traditional Virtual Machine environments?		MSI to decide the details of the solution.
567	Annexure-3	3.4.2.15	168-169	N/A (General)	Are cloud based tools, where the necessary application endpoints need to be exposed to the tool via the internet, acceptable?		No.
568	Annexure-3	3.4.2.15	168-169	The tool should support testing of all kinds of mobile apps such as Native, Hybrid, Web and Secure applications.	Typically, performance testing tools focus on testing back-end applications or APIs. When it comes to mobile apps, most of the focus of the testing tools will be on the backing APIs of the mobile application. Is this the intention of this requirement, or are mobile specific client-side aspects such as memory consumption, battery drainage etc also expected?		Clause is self explainatory
569	Annexure-3	3.4.2.8	141-158	N/A (General)	Is a Sofware-as-a-Service acceptable, where the metrics data only (no PII data or otherwise sensitive data) will be transported to a cloud-based service?		No

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
570	Annexure-3	3.3.3.16	63-66	Relational Database Management System/Non - Relational Database Management System	Only the PostgreSQL is listed as the supported RDBMS for MOSIP in their web site. Hence all specifications/requirements should be limited to the PostgreSQL or it's commercial version EDB		PostgreSQL is preferred with enterprise support
571	Annexure-3	3.4.1.1	79-80	Blade Servers	Requested blade server configuration can be provided. But considering the global trends (Large failure domain, high cost, vendor locking etc), rack mount serers would be the best optimal server solution		Bidder has to design and implement the solution. It is not mandatory to propose blade servers. The bidder has the liberty to design the solution using server types and its composition.
572	Annexure-3	3.4.1.2		Rack servers			NA
573	Annexure-3	3.4.1.2	81-82	Server should be quoted with latest generation x86 Intel/AMD processor Server should be configured with minium of 2 x 32 Cores 2.8GHz latest generation Intel/AMD processors	Better to request a new CPU model with higher core count to reduce the physical server quantity for optimal cost		No change
574	Annexure-3	3.4.1.2	81-82	Server should support 64Gbps FC ports. Min 4 ports per storage controller	Standard HBA comes with dual ports only. Configuring 2 x dual ports HBAs will provide adiquate performance and high availability.		No change
575	Annexure-3	3.4.1.2	81-82	Graphics controller: Supports display resolutions up to 1920 x 1200 16bpp @ 60H	Graphic controller performance will not contribute to the UID solution, but this point may limit the compatible server options where it could drive to cost increase		No change
576	Annexure-3	3.4.1.3	83-85	Blade Chassis	Please refer comments for 3.4.1.1 - Blade servers		Refer answer at 3.4.1.1
577	Annexure-3	3.4.1.4	85-86	Enterprise Grade Object Storage Solution	Only MinilO is listed as the MOSIP compatible Objet storage. Hence we might have to stick to the same product and available featues		Enterprise license of MinilO should be used.
578	Annexure-3	3.4.1.4	85-86	Object storage must support multiple replication topologies: active-active, active-passive, one-to-many, many-to-one, ring, and chain.	Market available Object Storage product support some of these features, but difficult to find a single product supporting all those.		Requirement is dropped
579	Annexure-3	3.4.1.5	87-91	SAN (Storage Area Network)	Userable capacity requirement is not clearly indicated		Already responded in S.No. 254
580	Annexure-3	3.4.1.5	87-91	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage. In case of non-native/external component used, it should be supplied in redundant mode with no single point of failure.	What does mean by "Existing Storage"		There are no existing storage with GoSL.
581	Annexure-3	3.4.1.5	87-91	The Proposed storage system should support Active-Active Storage configuration across two sites replicating to each other for same LUN/volume for zero RPO/zero RTO configuration.	Technicaly this can be complied. But network latency will be a key consideration		Bidder to propose bandwidth requirement which GoSL will provide.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
582	Annexure-3	3.4.1.5	87-91	Storage management software should be able to send notifications for alerts generated in the end to end infrastructure i.e. virtual machines, Host OS, hypervisors, SAN devices, Storage devices	Can not fully comply. Will be able to notify up to host level only		No change
583	Annexure-3	3.4.1.6	91-93	SAN Switch	Overall specs given will drive to a high cost SAN director, but there may not be such work load or performance requirement		No change
584	Annexure-3	3.4.1.6	91-93	The switch(or director platform) must be able to provide up to 96 number - 64Gbps FC or 10-Gbps full line-rate autosensing Fibre Channel physical ports from day1. System should be scalable to support upto 384port or more.	This will lead to a high cost SAN director model instead actually required mid range SAN switch		Already responded in S.No. 291.
585	Annexure-3	3.4.1.6	91-93	With the combination of 64-Gbps Fibre Channel switching module and supervisor switching modules it should be capable of enabling up to 4 terabits per second (Tbps) at the aggregate level	Requested 4Tbps is a very high figure		Minimum 1-2 Tbps and scalable upto 4Tbps
586	Annexure-3	3.4.1.6	91-93	The switch must support port aggregation of up to 16 physical Fibre Channel ports into a single aggregated link. The aggregated ports must NOT be consecutive ports on a line card and should support distributed model.	This is a very high performance requirement compaired to similar workloads.		Please refer to answer at S.No. 24
587	Annexure-3	3.4.1.7	93-94	Tape Library	Tape solutions are already obsolete. Better proopse a disk based backup solution		No change
588	Annexure-3	3.4.1.8	94-96	VTL	Tape solutions are already obsolete. Better proopse a disk based backup solution. VTLs mostly used by lagacy applications, not required for modern apps like MOSIP However some disk based backup appliances support VTLs (Eg.Dell DataDoain)		VTL is dropped.
589	Annexure-3	3.4.2.1	123-126	*Virtualization Platform*			NA
590	Annexure-3	3.4.2.1	123-126	*Provide a highly-available administrative console for management of the virtual data center platform…*	The term “highly-available” is vague. Does it mean: Active-Active clustering for the management console? Or just failover capability?		Please consider Failover capability
591	Annexure-3	3.4.2.1	123-126	*Provide the ability to hot-add CPU and memory and hot-plug disks and NICs…*	Is this mandatory for all workloads, or only for critical workloads? Can downtime be allowed for non-critical workloads?		Downtime may be allowed for non critical workloads with prior approval from GoSL.
592	Annexure-3	3.4.2.1	123-126	*Enable consolidation of VMs on fewer hosts and automatically power down unused capacity… leverage deep process power state of the CPU…*	Deep process power state” is vendor-specific terminology.In that case Accept equivalent CPU power management features from other platforms as well ?		Agreed. Equivalent CPU power management feautre is acceptable.
593	Annexure-3	3.4.2.1	123-126	*Provide the ability to boot from iSCSI, FCoE, Fibre Channel SAN, locally attached USB storage and network PXE boot.*	Are all boot options mandatory, or can alternatives (like iSCSI + PXE) suffice?		Alternatives such as PXE, iSCSI, and FC SAN are acceptable

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
594	Annexure-3	3.4.2.1	123-126	*Provide continuous availability for critical application workloads… live shadow instance… zero downtime.*	Will high availability clustering (with minimal downtime failover) be acceptable instead of FT?		High Availability (HA) clustering with minimal downtime failover is acceptable. Minimal down shall be acceptable as defined in the SLAs. Fault-tolerant (FT) hardware platforms or zero-downtime live-shadow systems are not required.
595	Annexure-3	3.4.2.1	123-126	Solution shall provide zero downtime hosts patching with maintenance mode…	Is live migration acceptable as an alternative?		Live migration mechanism is an acceptable.
596	Annexure-3	3.4.2.1	123-126	Support AES-128 and AES-256 encryption (in conjunction with any KMIP 1.1 compliant KMS server)…	Will other standards-based KMS solutions be acceptable?		KMIP 1.1 compliance is not mandatory. Any standards-based KMS solution that supports AES-128/256 encryption and secure key management is acceptable.
597	Annexure-3	3.4.2.1	123-126	Solution must intelligently learn the environment behavior… preemptively rebalances workloads…	Is policy-based load balancing acceptable instead of AI-driven predictive balancing?		No change. AI driven predictive balancing is not required.
598	Annexure-3	3.4.2.2	127-130	Backup and Security			Query below
599	Annexure-3	3.4.2.2	127-130	Licensing: The proposed Backup software must offer instance based licenses with no restrictions on type of arrays (protecting heterogenous storage technologies), front end production capacity or backup to disk target capacity restrictions. Licenses and associated hardware should be supplied having License for min. 250 VM's should be included and backup appliance should be provided with 500TB capacity from Day1.	500TB capacity is requested, but there is no clear indication whether it is raw, useable or efective capacity.		500 TB Usable
600	Annexure-3	3.4.2.3	130-131	Cloud Native Backup and Restore			NA
601	Annexure-3	3.4.2.3	130-131	Solution shall provide volume snapshots and App consistent backup and application cloning	Snapshot and cloning capabilities should be provided by the CSI driver–enabled storage solution, not by the backup software.		Clause remain unchanged. CNBR solution shall orchestrate volume snapshots using CSI driver–enabled storage and provide application-consistent backup, restore, and application cloning workflows.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
602	Annexure-3	3.4.2.3	130-131	Solution shall provide logging integration capabilities	A centralized log management solution should be in place to support comprehensive log integration.		The CNBR solution shall generate comprehensive operational and audit logs and support integration with log management & SIEM platforms for monitoring and compliance.
603	Annexure-3	3.4.2.4	131	Disaster Recovery	Recovery point objective (RPO) and Recovery time objective (RTO) information is not given. But those are the most important considerations for designing DR solution		1 hr: 4Hr
604	Annexure-3	3.4.2.5	132-134	Enterprise Container Application Platform			NA
605	Annexure-3	3.4.2.13	165-166	Container Orchestration Platform			NA
606	Annexure-3	3.4.2.13	165-166	Deploy most up-to-date, stable and enterprise ready release with relevant tools and should allow workloads to be moved between environments like Dev , testing , Pre-Prod Prod etc.	What is meant by “workload movement between clusters”?		The term “workload movement between clusters” refers to the capability of the proposed solution to migrate or transfer application workloads—such as virtual machines, containers, or application packages—across different environments including Development, Testing, Pre-Production, and Production. This involves the ability to move workloads between physically or logically separate clusters without requiring redesign, reinstallation, or compatibility adjustments.
607	Annexure-3	3.4.2.13	165-166	Setup multiple Kubernetes clusters for different environments i.e. Production /Dev/Test as per the requirement. Each cluster should support multi-tenancy and would have multiple tenant applications.	Deploying multiple clusters will result in higher costs. This requirement can be met through namespace isolation and by assigning dedicated nodes to each environment		No change
608	Annexure-3	3.4.2.13	165-166	Persistant Volume	This section does not clearly indicate how the persistent volumes are expected to be provided. Should this requirement be addressed through the storage solution described in Section 3.4.1.5?		Cloud native backup and restore (solution) is dropped.
609	Annexure-3	3.6.2.1		Blade Chassis	Please refer previous comments under 3.4.1.1, 3.4.1.2, 3.4.1.3,3.4.1.4, 3.4.1.5		Already answered
610	Annexure-3	3.6.2.2		Blade Server			Already answered
611	Annexure-3	3.6.2.3		Rack Server			Already answered
612	Annexure-3	3.6.2.5		SAN (in case separate hardware is required)			Already answered
613	Annexure-3	3.6.2.6		SAN Switch (in case separate hardware is required)			Already answered

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
614	Annexure-3	3.3.3.8	48	Document Management System should allow inputting files through following sources:	Are you expecting document scanning capability also? If yes, pl. specify the number of users for scanning / indexing and the avg. no. of pages to be scanned daily.		Document would be scanned by the Document Scanner cum printer. These scanned documents would be inputted in the DMS
615	Annexure-3	3.3.3.8	49	OCR in different language	what are the languages to be supported for OCR		Sinhala, English & Tamil
616	Annexure-3	3.3.3.8	50	Inbuilt Document Editors for various file types	what are the file types expected?		Illustrative list of file types: DOC, DOCX, XLS, XLSX, PPT, PPTX, ODT, ODS, ODP, PDF, PDF-A, RTF, TXT, JPG, JPEG, PNG, TIFF, CSV, JSON, XML.
617	Annexure-3	3.3.3.8	49	Revise Documents	What is meant by 'Revise documents'? Pl. explain		Requirement is dropped
618	Annexure-3	3.3.3.8	49	Create Documents using Templates	what are the document types expected to be created by the DMS?		Requirement is dropped
619	Annexure-3	3.3.3.8	50	Business Process Modeling with Customized Windows, Re- ports	what is meant by customized windows?		Requirement is dropped
620	Annexure-3	3.3.3.8	51	Follow-ups and Chat	Are you expecting a chat facility within DMS?		Requirement is dropped
621	Annexure-3	3.3.3.8	51	Inbuilt Calendar, Email, SMS	It is assumed the requirement is to integrated the DMS with calendar, email and SMS; but not to implement these features within DMS. Pl. confirm		Requirement is dropped
622	Annexure-3	3.3.3.8	N/A		Pl. spcciify the following volumetric details - Total number of users for DMS - Approx. number of concurrent users for DMS - Approx. no. of new documents that will be added to the DMS daily - Approx. no. of documents viewed / processd daily -Avg. document size (MB) and pages per file - Avg. retention period per document - Expected annual growth rate of documents or storage		Volumetric details are provided as follows: • Total users: 250–300 • Concurrent users: 30–50 • New documents/day: 100-125 • Documents viewed/day: 200 • Avg size: 1-2 MB • Retention: As per GoSL policy. • Annual growth in new documents: 5-10% DMS will be preferrably an open source with an enterprise support.
623	Annexure-3	3.3.3.8	N/A		Are you expecitng migration of existing documents in to DMS? If so pl. specify the following - Pl. provide total volume (no. of documents, total size, avg. file size) - Pl. specify the source repositories and data formats. - Confirm availability and format of metadata. - Clarify if document versions, permissions, or folder structures must be retained. - It is assumed that required metadata will be provided in a standard database or exportable format, and that no data enrichment /indexing or cleansing activities are expected as part of the migration. Pl. confirm		No migration is expected.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
624	Annexure-3	3.3.3.11	56	The solution shall support Phreak & Reteoo algorithm	Pl. confirm whether it is mandaotry to use Drools rule engine, or if equivalent rule inference algorithms are acceptable		Drool rule engine is required but it needs to be implemented as dedicated rule service for SLUDI and not as a BRMS.
625	Annexure-3	3.3.3.11	56	The Rules Engine must be able to submit business rules to an external repository at such time as the repository exists.	What is meant by 'external repository'?. Does it refer to a centralized business rule repository or a source control system (e.g., Git)?		External repository refers to a centralized business rule repository where rule definitions can be exported or synchronized. This may be implemented using centralized rule repository.
626	Annexure-3	3.3.3.11	56	Support both embedded and stand-alone services. Other requirements beyond java compatible.	Can you pl. explain this requirement? Does it mean the support for non-Java access via REST APIs ?		Yes, the requirement applies. In a MOSIP environment, the service must support both embedded usage and stand-alone microservice deployment. Non-Java access via REST APIs is required to ensure interoperability with other MOSIP modules and external partner systems.
627	Annexure-3	3.3.3.11	N/A		Pl. specify the following -expected daily and peak decision request volumes. -number of business rule authors and technical users. -Indicate number and complexity of decision services (avg. rules per service). -expected concurrent rule executions or transactions per second		Please refer to Annexure 5 - Demand capacity where volume analysis is provided both for enrollment, authentication users. Rules per service and concurremt rule execution shall be determined by the MSI during solution design.
628	Annexure-3	3.3.3.12	N/A		Pl. specify the following -total no. of named users for BPMS -Approx. no. of concurrent users -No. of process authors and administrators -Avg. no. of process requests initiated daily -Ratio of straight-through vs. human-centric -Avg. no. of process definitions -Avg. no. of workflow steps per workflow -Avg. process duration -Avg. no. of attachments per workflow and avg. attachment size		As Above
629	Annexure-3	3.3.3.12	N/A		Please confirm whether external or public users will initiate workflows through the BPM system. If so how such external users to be authenticated?		A separate enterprise BPM is not required.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
630	Annexure-3	3.3.3.4	39-41	The CRM solution shall be integrated with IVR/Voice, SMS Gateway, USSD Gateway, Email, messaging platforms, social media platforms, Live Chat and FAX for both inbound and outbound communication.	Other than the intergration to these systems ,should the solution provider also provide solutions to cater these systems-E.g IVR/Voice,USSD…etc		The requirement specifies that the CRM solution must be capable of integrating with IVR/Voice, SMS Gateway, USSD Gateway, Email, messaging platforms, social media platforms, Live Chat, and FAX for inbound and outbound communication.
631	Annexure-3	3.3.3.4	39-41	Support languages in Sri Lanka as per the need	Need more details as to what extend the local langauge support is needed in the CRM system		Sinhala, English & Tamil
632	Annexure-3	3.3.3.4	39-41	General	Can we propose a cloud or on Prep CRM solution		On Prem based
633	Annexure-3	3.4.2.10	159-160	The solution must provide a flexible framework for collecting and managing service level templates including Service Definition, Service Level Metrics, Penalties and other performance indicators.	Confirm if API-based template management is required		API-based template management is not required. The system only needs to provide UI-based configuration and management of SLA templates, including definitions, metrics, penalties, and KPIs..
634	Annexure-3	3.4.2.10	159-160	Ability to define and calculate key performance indicators from an End-to-End Business Service delivery perspective.	Does this require real-time KPI calculation or periodic batch processing? Should the tool integrate with external monitoring systems for KPI data? Define calculation frequency and integration expectations.		Periodic batch processing. No, the tool do not need to integrate with external monitoring system.
635	Annexure-3	3.4.2.10	159-160	Support for Defining and Calculating service Credit and Penalty… service Bonuses…	Should calculations be automated based on SLA breaches, or manual entry allowed? Should the system integrate with financial systems for credit issuance?		Requirement is dropped
636	Annexure-3	3.4.2.10	159-160	Make it possible to find underlying events that cause SLA failure.	Does this require root cause analysis (RCA) capability or just correlation reporting?		The solution will provide correlation reporting to link SLA failures to underlying events, along with root cause analysis capability to identify and address primary causes, ensuring proactive service reliability.
637	Annexure-3	3.4.2.10	159-160	Supports dynamic service level targets to reflect obligations importance and priority over time.	Should dynamic targets be rule-based or AI-driven predictive adjustments?		SLA targets are rule based and configurable dyanimically with approval of GoSL. AI drive predictive adjustment are not envisaged.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
638	Annexure-3	3.4.1.10	98	Core Switch should meet/exceed following hardware features/capacity. 1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 80MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber modules should have duplex LC connector to work with multi-mode fiber supporting minimum 300 meters for 10Gbps link and 100 meters for 100Gbps link.	Considering the transceiver quantity, is it possible to go ahead with 48 ports? Is that port requirement sufficient? Should the port bandwidth be 1/10G or 1/10/25G? Are dedicated stacking ports required, or can we use the service ports for stacking?		Please note following 1) Minimum 48 ports are required. For any scalability purpose, MSI will be responsible. 2) Port bandwidth 1/10/25G is required 3) Both are acceptable depending upon the model or OEM that MSI proposes.
639	Annexure-3	3.4.1.12	101	The NMS will be hosted on-premises. NMS solution to provide a single pane of glass to discover, configure, provision, monitor, manage, analyze and troubleshoot the network using the features and functionalities defined below.	Do we need to consider traffic flow analysis?		The NMS requirement specifies capabilities for discovery, configuration, provisioning, monitoring, management, analysis, and troubleshooting of the network. Traffic flow analysis (e.g., NetFlow, sFlow) is not required in the stated features;
640	Annexure-3	3.4.1.13	104	Fabric Definition: 1) Proposed fabric must be the CLOS network topology architecture defined using Spine, Leaf switches with VXLAN overlay. 2) Fabric Should allow workload mobility anywhere in the DC, across the Data Center sites. 3) fabric should be able to sustain multiple link and device (Leaf & Spine), Controller failures. 4) fabric should be able with use full cross sectional bandwidth (any-to-any) across all provisioned uplink ports using equal cost multi pathing. 5) Solution should provide latency and drop analysis between end points connected to fabric with reason of drop. 6) The proposed architecture should provide a single pane for provisioning, monitoring, and management to deploy stretched policies across DC and DR.	Should the datacenter network follow the stretched DC network architecture or multi-site DC network architecture? If the customer requires a stretched DC network architecture, we need to ensure the maximum latency is 50 msec RTT between datacenters.		This is not required.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
641	Annexure-3	3.4.3.3	182	The proposed solution must support the automatic recording of sessions with and without notification to the user.	Time period the recording should be stored for (eg - number of years or months)		Provide configurable options for **notification** and **retention period**, ensuring flexibility, compliance, and operational control. It should be available for 15 months.
642	Annexure-3	3.4.3.2	183	The solution should support selective analysis of files which are deemed suspicious based on internal capability. Entire solution and all its components should be on-premises with no data including meta data leaving the buyers data centre	IS the on-preme requiremnt a strict rule or can we poropose a hybrid solution.		ON Prem only
643	Annexure-3	3.4.3.18	242	Supported application optimization modules such as compression, caching, connection multiplexing, SSL offloading, TCP optimization.	will the customer be providing the SSL certifications		MSI to provide SSL certifications
644	Annexure-3	3.4.3.6	194		Can the soution be a cloud SAAS offering.		No
645	Additinal queries				Mosip has a java 21 migration and release planned this year. Need a clarification whether this would be part of scope		Yes, the latest version of MOSIP should be used.
646	Additinal queries				Mosip has a committed LTS support till Feb 2027 (https://docs.mosip.io/1.2.0/setup/upgrade/adopting-lts-1.2.0#whats-new-in-lts-1.2.0) - need a clarification on the upgrade path to next LTS version.		Upgrade path and relevant documentation shall be made available by MOSIP. However, remote support can also be provided on case to case basis, if required.
647	Additinal queries				Clarification regarding responsibility of the MSI if security patches are not available from MOSIP on Core MOSIP modules.		For the MOSIP code, security patches will made available universally and MSI will have to apply thoise patches. For open source components of Core MOSIP modules, MSI will get enterprise support and it would be the responsibility of MSI to update all the patches including security patches for core MOSIP modules. However, MOSIP will also issue advisory to partner countries for new updates.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
648	Additinal queries				Clarification of face auth as there are no mosip certified face auth devices available right now, a few are undergoing compliance tests though.		Yes. MOSIP is currently evaluating devices for face authentication. However, in the absence of MOSIP certified devices, MSI can come up with face authentication solution , which is based on international standards. In due course, if MOSIP comes up with face authentication devices or standards, MSI can adopt those.
649	**Vol-2**	Section VI, Clause 5.1.3.1	33	Business Intelligence and Analytics	As per discussions during Srilanka VIsit, it was stated by the Employer that BI & Analytics is out of scope. Kindly confirm whether BI & Analytics is included or excluded in the final scope.		BI and Analytics is included in the final scope. Please refer to Volume 2 section 5.1.3.1 for details.
650	**Vol-2**	Section VI, Clause 5.1.4.1	36	The SL-UDI Citizen Portal would be available to all stakeholders (residents, internal users, contact center agents, TSPs, Administrators, etc. vi)Implement a “Content Management” framework and solution to allow authorized users of GoSL to manage publication of new content on the portal. The proposed content management solution should meet the minimum technical specifications given in the RFP. As part of this, MSI shall provide training to users identified by GoSL on the following:	As per discussions during Srilanka VIsit, it was stated by the Employer that Citizen Portal is meant only for citizens. Kindly confirm and revise the scope accordingly.		Understanding is correct.
651	**Vol-2**	Section VI, Clause 5.1.4.5	39	Service Billing System	The RFP indicates about Service Billing System requiremnt. Since authentication services are initially free, please clarify whether MSI is required to provide the same.		Service billing system is required.
652	**Vol-2**	Section VI, Clause 5.2.1.1	49	GoSL has decided to utilize a two-way setup containing DC and DR sites. The DC and DR sites will be in 1:1 configuration i.e., exact replica of each other. For the entire duration, a mechanism for storage and safekeeping of backup tapes, a remote site will be utilized.	The RFP specifies Virtual tape libraries (VTL) as well. Kindly confirm whether Tape Library or VTL is required.		VTL is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
653	**Vol-2**	Section VI, Clause 5.3.1	60	8. Web camera 13. Enrolment – Microphone 16. Auth – Facial Scanner 17. Auth – Iris Capture Device 18. Auth- Fingerprint	Microphone is not required for enrolment. Web camera is an enrolment device and must be MOSIP-compliant. - Authentication devices (Facial, Iris, Fingerprint) are not required as part of the biometric registration kit. Kindly confirm and correct the scope accordingly		Microphone is not required. Authentication devices (Facial, Iris, Fingerprint) as part of biometric registeration kit are not required. However, 100 pieces each of Facial, iris and Fingerprint Auth devices are required. Please refer to Section 7 Volume 02 for details
654	**Vol-2**	Section VI, Clause * and 5.3.2	61 and 62	* Authentication software could be from 3 different OEMs. Registration software could be from a single OEM to ensure interoperability, reusability and reduce complexity as it may have time and cost implications. 5.3.2 (iii) It is expected that the enrolment software developed by the MOSIP shall be compatible/interoperable with biometric capture devices (fingerprint, iris, and photograph) of at least three leading and reputed OEMs. In order to ensure this, MSI is expected to provide each type of biometric capture devices (fingerprint, iris, and photograph) from three different OEMs.	Please confirm from how many vendors the authentication and registration devices need to be provided.		Authentication software to be read as Authentication devices. Authentication devices shall be from 3 different OEMs. Please referfoot note page 61 Section 5.3.1 from Volume 02. Registeration softwares would be supplied from MOSIP and not from a other OEMs.
655	**Vol-2**	Section VI, Clsue 5.1.7.2 and 5.8.1.9	48 & 82	5.1.7.2 (viii)(a) Integration of Enrolment Software with FTP servers for upload of completed enrolment packets. 5.8.1.9 (VIII)(9) Secure channels such as HTTPS shall be used to transmit the enrolment packer to SL-UDI DS.	The two statements conflict. One mandates HTTPS, while another asks for FTP integration. MOSIP supports HTTPS only. Kinldy clarify.		MOSIP only supports HTTPS. Hence, MSI will use HTTPS as a secure channel.
656	**Vol-2**	Section VI, Clause 5.1.5	40	5.1.5 (v) BSP shall supply perpetual server licenses and desktop licenses for multi-modal SDK. The SDK licensing should be: (a) Unrestricted, unlimited right to uses, but not machine specific licenses and the right to deploy the solution anytime anywhere. (b) Enrolment SDK licenses must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID)	The licences need to be tied up with the kits else there is a chance of misuse. Kindly confirm.		No. The licences shall not be tied up to the Kits and they will be transferable from one machine to another. However, misuse shall be preveneted by restricting the overall count of the licences and through licencing process.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
657	**Vol-2**	Section VI, Clause 20	13	Card Activation - At the time of issuance, the card is in inactive state and before usage of card, it needs to be activated. MSI needs to build and provide the functionality to activate the cards in both online and offline manner.	Request clarification on the following points: •Where will the card details be stored and accessed? •What is the expected impact on MOSIP when a card is activated or deactivated? •How should physical cards be activated in offline mode, given that only the UID can be activated for authentication? •For the online activation process, MSI is expected to build components for card activation and integrate with web/mobile/SMS channels, as well as update status in the personalization workflow. We Request more clarity on these integration requirements.		This reuirement is dropped
658	**Vol-2**	Generic	NA	Legacy UID issued only based on demographics; migration not required. - Integration needed to fetch demographics from legacy system. - Verification mechanism needed to ensure correct ID mapping. - Potential integration with other data sources such as Passport and Driving License.	Please confirm whether these requirements apply to both the Pre-Registration Portal and the Registration Client. The Pre-Registration Portal also collects the applicant's demographic details as per the ID schema before an appointment is booked, so integration will be required here as well—not only in the Registration Client. Additionally, if integration is expected, the Registration Clients must operate in online mode.		Yes - Integration needed to fetch demographics from legacy system. Verification mechanism needed to ensure correct ID mapping (eNIC mapping). Potential integration with other data sources such as passport and driving license is not envisaged at this stage.
659	**Vol-2**	Generic	NA	Access, CI/CD & Environments	All vendors will require secure access to the Production environment even after the system is live for trouble shooting and monitoring purpose.		Agreed. Under the supervision of GoSL.
660	**Vol-2**	Generic	NA	Performance testing environment	Kindly confirm whether a separate performance testing environment is required or whether Production can be used, and whether recertification will be needed.		Performance testing environment is required.
661	**Vol-2**	Section VI, Clause 7	160	68. Auth - Facial Scanner 69. Auth - Iris Capture Device	SBI 2.0 Compliant successful face & iris devices are not available. It is requested to either change it to SBI 1.0 devices or remove such requirement?		SBI 1.0 and above is acceptable
662	**Vol-2**	Annexure-3, Clause No. 3.5.2.4 and 3.5.2.6	317 and 320	3.5.2.4(19) FTM** : SBI 2.0 – FTM supported security 3.5.2.6 (11) FTM** : SBI 2.0 – FTM supported security	SBI 2.0 Compliant successful face & iris devices are not available. It is requested to either change it to SBI 1.0 devices or remove such requirement?		SBI 1.0 and above is acceptable

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
663	**Vol-2**	Annexure-3, clause No. 3.5.1.7	304	(3) Size: Should be able to accommodate items in the enrolment kit (4) Cushion: Should have sufficient cushions for all the equipment from Top, Bottom and all sides (5) Space: Separate enclosures should be built for the items of enrolment kit	Multiple devices in field infrastructure are in GoSL scope. Kindly share Make model, datasheet & dimensions of the components to be provided by GoSL		Exsiting devices with GoSL. MSI to assess the compatibility of these devices with MOSIP required compliances : 1. Finger Print Scanner - Kojak, KJ220DA-EOO. FBI Appnedix F, FAP 60 2. Signature Pad - Kojak, KJ220DA-EOO Signotec, Gamma 3. Finger Print Auth Scanner - Signotec, Gamma 4. Dual Display Monitor - Eizo, Duravision FDF2182WT 5. Flash Light 6. Background Screen 7. Web Camera - Sandberg, Proelite 134-39 8. USB Hub - Lindy, 43128
664	**Vol-2**	Section VI, Clause 5.3 and 7	60 and 160	5.3 (1) Desktop PC and other components: GoSL 7. (71) Laptop for registration kits: 860	Field infrastructure scope on page 60mentions Desktops under GoSL scope. Whereas schedule of requirement mentions Laptops under MSI scope. Please clarify.		MSI scope.
665	**Vol-2**	Annexure-3, Clause 3.5.2.7	324	3.5.2.7 (8) Printer: • Resolution - 600 x 600 dpi • Paper Size - A4 • PPM - Black (A4) - >8 ppm • Duty Cycle - 5000 pages • Media Used - Ink tank for low cost running with additional 2 in tank refills of 150 ml • Monochrome – Yes (Black) • Connectivity - USB • Compatibility – Operating system of the laptop	Ink Tank printers are not suitable for mobile registration kits as they are bulky & it is also not suitable for transportatiion as inkTank would spill Can this changed to Thermal Receipt printer? if no, Can this be changed to AP thermal Printer?		Yes. Please refer to specification of Thermal printers in revised annexure 3 .
666	**Vol-2**	Annexure-3, Clause 3.5.2.8	328	Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of SLUDI.	Number of devices are very less a dedicated Deviice Management Server in Sri Lanka would be very costly. Can the device manegement server be at overseas location? Can it be shared between other MOSIP implementation with dedicated partition and channel for SLUDI?		1. Device management server has to be in srilanka and dedicated for SLUDI
667	**Vol-2**	Section VI, Clause 7	160	81. UPS : 40	Requirement of UPS will be bulky for Mobile registration kits. it will affect the Mobility. Can a heavy duty batttery of +50,000 MAH can be used to support 7-8 hours of operation?		Agreed. (Field infrastructure section mobile Kit - replace UPS with +50000 MAH battery)

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
668	**Vol-2**	Annexure-3, Clause 3.5.1.1	300	7. Ports: Two x USB 3.2 Port One x USB 2.0 One x Gigabit LAN (RJ 45), One x HDMI Port (v1.4b), One x VGA Port, One x Headphone / MicrophoneTwo x USB 3.2 Port One x USB 2.0 One x Gigabit LAN (RJ 45), One x HDMI Port (v1.4b), One x VGA Port, One x Headphone / Microphone	Is it acceptable to meet the VGA port requirement using an HDMI to VGA adapter? Lately VGA port is obsolete with major laptop brands.		Agreed.
669	**Vol-2**	Annexure-3, Clause 3.5.1.1	300	14. Battery Minimum 4 Cell lithium-ion or lithium polymer battery with minimum 10 hours as battery backup	Mostly Laptops have 5-6 hourss of battery back-up. Can the 10 hours be relaxed. Also these kits are part of Field infrastructure where stable power supply would be available		5 to 6 hours of battery backup is acceptable
670	**Vol-2**	Annexure-3, Clause 3.5.1.13	310	Speaker: (11) Memory Card Supported up to 32 GB	Can Speaker with BT based connection be accepted? Speakers with SD cards are obsolete now		No change
671	**Vol-2**	Annexure-3, Clause 3.5.1.7	304	1. Material High-Quality Fibre	Is 'High-Quality Fibre' a mandatory material specification, or are alternatives like ABS or PP also permissible under the tender?		Agreed.
672	**Vol-2**	Annexure-3, Clause 3.5.1.9	305	6. Safety: Water Resistant	As per our understanding the Dongle is under GoSL scope. If not, kindly confirm if water resistance a mandatory requirement for the internet dongle? As the dongle would be part of the water resistant kit, we propose to modify this requirement.		Internet Dongle is under GoSL scope.
673	**Vol-2**	Annexure-3, Clause 3.5.2.7	321	(2) Laptop: Processor: Latest Generation, min 2 GHz Base Frequency, 8MB cache, turbo boost- 4 cores- 16 GB RAM or more- OS: Windows 10 Pro 64-bit installed on SSD- Storage: Hybrid (512 GB SSD M.2 PCIe + 1 TB HDD)- Screen: Full HD, 14-14.1 inches- Power Supply: AC adapter for 220V, 60Hz- Battery: 6 hours continuous usage- Network: Ethernet RJ45, Wi-Fi (802.11 b/g/n)- Ports: 2x USB 3.0, 1x USB 2.0, 1x USB Type C, HDMI port- Mouse: 1 wired- Touchpad: Below keyboard- Accessories: Charging cable/adapter- Anti-virus: Third-party pre-installed with updates; 3-year license- Chip: TPM 2.0 or higher	1. The "Latest Generation" is a generic term. Kindly clarify more about the Generation of required processor. 2. laptops with HDD are obsolete now. Is it acceptable to meet the storage requirement with a 512 GB SSD alone, or is inclusion of a 1 TB HDD mandatory under the tender specifications?		1. Latest generation should be read as not later than 12 months in field deployment. Processor i7 or higher or AMD equivalent. 2. No change
674	**Vol-2**	Annexure-3, Clause 3.5.2.5	318	10. Operating Temperature* 0 to °50 C	Considering standard webcams do not typically carry official operating temperature ratings. Kindly confirm if this requirement is mandatory?		Refer to MOSIP website for latest values.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
675	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS 19 ABIS Log	Page 336 of 361	e. Percentage of automated identification vs. manual intervention rate.	If re-templatization required during production, necessary additional infra should be provided by Employer to MSI to support re-templatization without disturbing production system. Kindly confirm.		Agreed. re-templatization would arise in extreme cause of force majure or only of the direction of GoSL. Necessary infratructure can be provided but time and speed calculations will have to be provided by MSI. However, all efforts would be made to deploy the existing hardware and infrastructure in the DC and deployed for BSP solution.
676	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS 29 Re-template	Page 338 of 361	The ABIS should support re-template creation i.e. re-creation of biometric gallery from raw images based on latest algorithm with zero or minimal downtime during this re-template exercise.	If re-templatization required after Go-Live of production , then necessary additional infra should be provided by Employer to MSI to support re-templatization without disturbing production system.		As Above
677	**Vol-2**	Annexure 9, Clause 9.5 Service Levels for Biometric Solution in Annexure-5, Clause 5.1.8 Other Performanc e Measures	page 13 of 34 , 14 of 34 Page 10 of 11	As per Clause 9.5: 1. False Positive Identification Rate (FPIR) <= 1% measured per month 2. False Negative Identification Rate (FNIR) <=1% measured per month 3. False Match Rate (FMR) <=0.01% for all levels of verification measured per month 4. False Non-Match Rate (FNMR) <=2% for all levels of verification measured per month As per Clause 5.1.8: 4. FPIR <= 0.1% and FNIR <=1% 5. • For Fingerprint: FMR <= 0.01% and FNMR <= 2% • For Iris: FMR <= 0.001% and FNMR <= 0.5% • For Face: FMR <= 0.01% and FNMR <= 2%	As per Annexure 9: SLA, the accuracy numbers are specified. However, in the Annexure – 5 , the accuracy numbers are mentioned differently. Kindly confirm which one should be used for SLA?		The accuracy parameters given in Annexure 5 shall be used in SLA
678	**Vol-2**	Annexure - 5, Clause 5.16 Infrastructur e	Page 8 of 11	1. CPU utilization upper limits - 60%	Kindly clarify the statement. As per design, the ABIS is expected to utilize available HW resources to the fullest optimization level with minimum wastage. We suggest to modify this requirement to avoid under utilization of CPU and to optimizing the server sizing.		This is applicable to Non-ABIS resources.
679	**Vol-2**	Annexure-5, Clause 5.16 Infrastructur e	Page 8 of 11	2. Re-size/ headroom (Virtual Cores, Memory, and Storage Seamlessly) - 25% of the base capacity	Kindly clarify the statement. As per design, the ABIS is expected to utilize available HW resources to the fullest optimization level with minimum wastage.		This is applicable to Non-ABIS resources.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
680	**Vol-2**	Annexure-5, Clause 5.1.5 Data Size	Page 8 of 11	Size of Enrolment Packet: Demographic, 10-Fingerprint, 2 Iris, Photograph and Documents	ABIS expected to store only templates and basic Demographics (Age, Gender) to optimizing the server sizing, images & Document stroage is outside ABIS system requirment, please confirm.		ABIS is expected to only store templates and no demographic data.
681	**Vol-2**	Annexure-5, Clause 3.6.1.1 ABIS MOSIP Compliance	Page 330 of 361	1. Compliance to MOSIP specification https://docs.mosip.io/1.1.5/biometrics/automated-biometric-identification-system-abis	Is this the MOSIP docs version to be used for MOSIP integration, considering there is a 1.2.0 version of MOSIP documentation available in MOSIP website? Kindly confirm.		Refer to response in Sr 645
682	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS	Page 331 of 361	4. Use to remove an ID from the reference database. The removal need could arise for a variety of reasons. All such incidents should be automatically brought to the notice of DRP on an immediate basis. The DELETE functionality of the ABIS should be disabled by the BSP.	Kindly clarify how DELETE function will be used if ABIS will have to disable DELETE function?		Delete Function has to be disabled.
683	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS 12 Verify	Page 333 of 361	12. A scaled comparison score and a "match/non- match" decision is always returned.	Usually ABIS will return the score based on which MOSIP / GoSL should make a decision of match/non-match. If ABIS is expected to return the match/Non-match decision, then the threshold value should be defined by GoSL		Yes, threshold value shall be defined by GoSL based on which ABIS will reutrn match non-matched decisions.
684	**Vol-2**	Section VI, Clause 5.1.5 Biometric Solution Implementation	Page 40 of 164	(v) BSP shall supply perpetual server licenses and desktop licenses for multi-modal SDK. The SDK licensing should be: a) Unrestricted, unlimited right to uses, but not machine specific licenses and the right to deploy the solution anytime anywhere. b) Enrolment SDK licenses must not use hardware license key or keyed to ID (such as CPU, serial number, Ethernet ID)	If SDK license should not use client machine details, then how SL-UDI planning to prevent the SDK license usuage outside the intended scope ?		GoSL will request MSI to reallocate the license.
685	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS 3 Identify	Page 331 of 361	3. Identify - sub-set of the database	Please share more detail about the sub-set of database.Since ABIS identification should happens against entire database.		MSI may configure or use subset of database for 1:1 verification during lifecycle management.
686	**Vol-2**	Annexure-3, Clause 3.6.1.1 ABIS Reliability Requirements	Page 345 of 361	2 Reproducible The results should be reproducible on a variety of platforms.	Please share specific requirement about the variety of platform.		For MOSIP based solution, Java (server side) and Windows (Client side) are the two specified platform. Please refer to Reliability Requirements under 3.6.1.2
687	**Vol-3**	Section VII, Clause 12.4	19	Clause states payments will carry interest if it is delayed by Employer	No Interest rate has been mentioned. Interest rate may please be specified.		As per RFP.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
688	**Vol-3**	Section-VIII, Clause 13.2 (a) and 13.2(b)	62	There is requirement of advance security of Rs. 3 Cr and advance payment PBG also required.	Kindly confirm whether both securities will coexist or one replaces the other. Also, clarification required for advance payment PBG duration as same is not mentioned in RFP.		Both will co-exist
689	**Vol-1**	General Query	NA	Funds will move from NISG to Indian Embassy in Sri Lanka and then Indian Embassy to Contractor (in INR).	Please clarify if **all** funds movement will be in INR? If not, please specify who bears the FX fluctuation risk during conversion and reconversion processes.		Yes, all payments will be made in INR.
690	**Vol-3**	Section-VIII, Clause 12.5	62	RFP states payment will be made in INR.	Accordingly, contractor should issue invoices only in INR. Please confirm if interpretation is correct? Tax deductions as per Local laws of Sri Lanka will be applicable on invoice raised in INR, please clarify.		Invoices to be raised in INR. In regards to taxations, kindly refer volume 03 section 14.3 (PCC)
691	**Vol-3**	Section-IX, Appendix 7	81	Terms and Procedures for Payment	It is mentioned in Appendix 7 that the invoices for payment will be verified by GoSL and after acceptance by GoSL, it will be forwarded to Indian Embassy for payment. Indian Embassy will release the payment to bidder after release of funds from NISG or MEA. Please clarify if our understanding is correct.		Payment for the project to MSI will be released in India by GoSL through their Indian Rupee bank account.
692	**Vol-1**	Section-III, Clause 3.1.2.5	31	Technical Score Parameter- Criteria D: Team Constitution and Staffing+[@Column5]	Please clarify how many resumes are required to be attached to get full marks in below section? D1 Qualification, certification and experience of the MSI's team D1.1 Leadership D1.2 Architects D1.3 Engineers D1.4 Track Leads D1.5 BSP engineers		Lead and alternate for each position.
693	**Vol-1**	General Query	NA	MSI payment and Taxation related	As per RFP it has been stated that payment will be made only in INR, as per Indian GST law transaction will be considered as zero rated (i.e. no tax charged considering export) only if payment for the services received in convertible foreign currency or in INR if permitted by Reserve Bank of India (RBI), we understand that Sri Lankan recipient of services or goods is permitted by RBI to make payment in INR and for making payment the procedures defined under RBI Circular No.10 (RBI/2022-2023/90 A.P. (DIR Series)) dated 11th July, 2022 required to be followed. We request to confirm whether payment from Sri Lanka will be made following the procedure defined in referred Circular?		This response should be read in consonance with RBI circular. Withholding taxes in Sri Lanka would not be applicable.
694	**Vol-1**	General Query	NA	FEMA/Indian Contract Act	Please clarify if the FEMA/India Contract Act would be applicable to the RFP		All payments are made in INR. contract has been published as RFP Volume 03 of 03.
695	**Vol-1**	General Query	NA	Export Control/License Agreement	Is there list of Import control restrictions form Specific countries for HW/SW in Sri Lanka. If so request to please share the list. We also request GoSL to share Embargo list of countries.		No
696	**Vol-1**	General Query	NA	Office Space for local delivery	Kindly clarify whether registration of office should be in the name of Contractor only or in the name of lead bidder in case of consortium?		It can be in the name of the contractor or lead bidder or consortium partner.
697	**Vol-1**	Section-IV, Clause 4.12.4	85-87	Payment Milestones and Schedule: Balance amount of P1+P2+P4+P5	We requests the following addition- Balance amount of P1+P2+P3+P4+P5		Suggestion is accepted

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
698	**Vol-3**	Section-IX, Appendix 7 para(ii)	81	The Contractor (MSI) shall submit the invoice as per the contract along with all the supporting documents including necessary proof of milestone achievement, deliverable signoffs, system generated SLA monitoring reports, etc.	We request to provide the List of supporting documents along with invoices.		This will be decided at the time of project planning with GoSL.
699		General Query		Agreement signing	Pl clarify if the Successful bidder will sign agreement with GoSL?		Yes, The successful bidder will sign the contract with GoSL
700	Annexure 3	Annexure-3 3.6.2.5 SAN	354	The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection.	**Modification** : The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 99.9999% availability with built-in redundancy and dynamic drive protection. Justification : The asked availability is OEM specific and not practicle to deliver. 99.9999% is highest followed by all leading OEMs. Hence reqeut for modification.		99.9999% availability is acceptable
701		Annexure-3 3.6.2.5 SAN	355	Offered Storage array shall support heterogeneous storage virtualization (native/external) for vendors like, but not limited to, EMC, HP, IBM, Hitachi, Netapp etc. Storage should be supplied with Unlimited capacity of virtualization license for existing storage.	We request to **remove this clasue ,as this OEM restrictive** and also limits the performance of NMVe arrays. As the Virtualization engine becomes the bottleneck, as Virtualization engine sits in Data Path . Moever this has not been implemented across large Enteprises requiring High performance and availability.		Requirement dropped
702		Annexure-3 3.6.2.5 SAN	358	Storage management software should be able to send notifications for alerts generated in the end to end infrastructure i.e. virtual machines, Host OS, hypervisors, SAN devices, Storage devices	We reqeust to remove this clause, as this functionality is more of EMS solution and not native storage functionality, as storage Management sofware does not controller Host OS, Hypervisor or SAN Switch as all these components are outsdie storage.		Requirement dropped
703		Annexure-3 3.6.2.5 SAN	359	The proposed replication solution must support multi host and multi-array enterprise consistency in an open system environment. Should ensure data consistency for mission and business critical application data that spans across multiple LUNs and Raid groups	We request more elaboration on this clasue, as Single OEM arrays replicate among same OEM storage solution only and not in hetrogenious environemnt. Within same OEM storage arrays, this is supproted natively.		To support multi-LUN and multi-RAID-group consistency through OEM-native Consistency Groups / Replication Groups.
704		Annexure-3 3.6.2.5 SAN	359	The offered storage solution must be able to cater to file, block, and object workloads	**Modification** : The offered storage solution must be able to cater to file, block workloads **Justification** : Object protocols is way to different then block and file , hence keeping this as spearte protocol and storage will help SL-UDI, as object storage scales to multiple PBs and is normally used as archieval storage.		Already answered in S.No. 216
705		Annexure-3 Caluse 3.6.2.2	348		We request SL-UDI to allow solution built on Rack server , as Blade server solution will lock in OEM, taking away freedom to scale and choose different OEM with same x86 solution. Also Blade chassis are Power Hungry and Latest Xeon 6 CPU are not available on Blade servers.		Bidder may choose either rack server or blade server or a combination of rack & blade server and propose the solution
706		Annexure-3 Caluse 3.6.2.3	348	HDD: Minimum 2 x 600GB 10K/15K RPM SAS	Modification : minimum 2*480/960GB SSD for OS drives Justification : RPM dirves are not avaialbel and future is with SSD/NVMe Drives only. Hence reqeust for this change.		Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
707	Volume 1	4.12.8.1 TABLE 5 for P5: Cost of Supply and Commissioning of ABIS and BioSDK	96	Gallery size of 30 million active records	In the Pricing Table, the Gallery size is 30 million active records, However in Volume 2 of 3. Section 1.6. It mentioned that "The SL-UDI should be designed considering the 20-year scale (2025 – 2045) i.e., population size of 33 million citizens. (Refer Annexure 5: Demand Capacity)" In Vol 2 of 3 Annexure 15 Transition Framwork it mentioned that : MSI should verify the scalability of for meeting the volume requirements up to year 2045 for a gallery size of 35 Million and take a view accordingly to enhance the existing ABIS system or deploy a new ABIS system. Please advise what is the Gallery size needed, 30, 33 or 35 million?		30 million unique records aka gallery size
708	Volume 1	4.12.12 TABLE 9: ABIS Deduplication Services Payment will be made monthly based on a successful de-duplication transaction that generates total SL-UDI in a single month until coverage of the “Target Population” is achieved. Thereafter, every month, the new registrations and deduplicatio n	68	4.12.12 TABLE 9: ABIS Deduplication Services	Charging for biometric de-duplication services is an outdated model, since biometric de-duplication is one of the primary functions of an ABIS system. Many ABIS suppliers no longer charge for Deduplication services in a transactional model. Charging on a transactional basis is the business model perceived to be of a particular ABIS supplier. There are experiences from other countries that this model results in exorbitant charges for the customer. We therefore recommend that NISG may please consider not implementing a transactional model for deduplication services as this will help to save the costs.		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
709	Volume 1	4.12 BID SUBMISSION FORMS – PRICE BID-4.12.4 Payment Milestones and Schedule 4.12.8.1 TABLE 5 for P5: Cost of Supply and Commissioning of ABIS and BioSDK	85-87 and 96	Payment Milestome P0, Payment Milestome P5, Payment Milestome Go-Live and Payment Milestone Iteration 2 **and** Table 5 for P5 The price of ABIS per transaction (cumulative successful transaction in a month) may be bundled with a monthly Service fee invoice.	It is our understanding that during the Phase 1 - Design and Build Phase to Go Live (Implementation Phase), the payment for ABIS software system shall be made as per the milestones as mentioned under - Payment Milestone P0 - Payment Milestone P5 - Payment Milestone GoLive - Payment Milestone Iteration2 **Please re-confirm the above understanding.** **Please also confirm** our understanding that the Unit Price required to be quoted under Table 5 for P5 (Page 96) is only for price evaluation purposes wherein the total price quoted for ABIS software will be divided by 30 million active records to arrive at unit price.		Refer, Table 5 for P5, Cost of Supply and Commissioning of ABIS and BioSDK. **"Gallery size of 30 million active records" to be read as " Gallery size of 30 million unique records'.** Please also refer to Payment Milestone P6, page 87, Payment Milestones and Schedule.
710	Volume 1	4.12.12 TABLE 9: ABIS Deduplication Services	101		It is our understanding that during the "Phase II – Operations and Maintenance", the payment for ABIS deduplication services shall be separately made on a monthly basis based on the number of IDU numbers generated in a particular month, for which montly invoices are required to be submitted. **Please re-confirm the above understanding.**		Please refer to " 4.12.12 TABLE 9: ABIS Deduplication Services Payment will be made monthly based on a successful de-duplication transaction that generates total SL-UDI in a single month until coverage of the “Target Population” is achieved. Thereafter, every month, the new registrations and deduplication transactions till the end of the contract period." **Monthly to be read as Quarterly**

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
711	Volume 2	5. Scope of Services	19	4.The MSI shall provide a detailed cutover plan before migrating from the legacy system and a roll out plan. Upon providing the plans the approval must be taken from GoSL.	We refer to the discussion between the representatives of qualified Master System Integrators with the representatives of NISG, Government of Sri Lanka and Government of India during the meeting on 13th November 2025 at ICPA office in Colombo. It was clarified in the meeting that : 1. There is no legacy biometric data to be migrated and hence there is no migration of biometric data under the scope of MSI. **Please formally reconfirm.** 2. SL UDI ID will be created based on the fresh biometric enrolment of all three modalities - FingerPrint, Face and IRIS. **Please formally re-confirm.** 3. The current Sri Lanka eNIC has only the demographic data that will be used to populate the pre-registration module only for comparison or verification. **Please re-confirm formally.** **Please formally re-confirm on the above three points.**		1. Your understanding is correct 2. Your understanding is correct 3. Your understanding is correct. Provision to edit/update and append missing data columns should also be there
712	Volume 2 Annexure 3	3.3.2 MOSIP related components	17	Ability to generate multimodal biometric templates from Raw Biometric captured.	Do you mean the biometric template individually for Facial Image, Fingers and Iris separately,resulting in 3 different templates?		Understanding is correct.
713	Volume 2	5.10.2.8 Biometric Solution Management (ix)	119	(ix)The BSP shall supply ABIS for biometric deduplication and verification during the enrolment process. The workflow and integration of ABIS shall be the responsibility of BSP with support from MSI.	How many modalities is needed for Dedupulication?		Deduplication is the responsibility of the ABIS solution. However, the MSI shall be accountable for service levels of, deduplication
714	Volume 2	7 Schedule of Requirements	159	Field Infrastructure 64. Enrolment Fingerprint Scanner (4-4-2) 860 65. Enrolment Iris Scanner (Dual) 860 66. Signature Pad 860 70. Enrolment Kit Container for registration kits 860 71. Laptop for registration kits 860	Could you clarify how many Field Infra Enrollment Biometric Devices are required? Refer to No.7, Is No. of "860" or "806"? and Is it total fixed units " 860x2=1720" or "806x2=1612"?		Field Infra Enrollment Biometric Devices are 1612. Final count of biometri devices are now updated in Volume 2.
715	Volume 2 Annexure 5	5.1.3. Registration and Transaction Volumes	4	Total Enrolment Units (Fixed) (Two per Cluster – 806 x 2) 1,612	Could you clarify how many Field Infra Enrollment Biometric Devices are required? Refer to No.6, Is No. of "860" or "806"? and Is it total fixed units " 860x2=1720" or "806x2=1612"?		Field Infra Enrollment Biometric Devices are 1612. Final count of biometri devices are now updated in Volume 2.
716	Volume 2 Annexure 5	5.1.3. Registration and Transaction Volumes	4	Peak registration packet to be uploaded per day (incl. backlog) = 75,000	Is the Peak registration packet number of 75,000 uploaded per day span across 8 hours per day or span across 24 hours per day? Note : This is crucial information for sizing purposes		Working hours for enrolment is 8 hrs.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
717	Volume 2	5.1.6 Solution Testing	43 and 44	This testing will be carried out on datasets of 50,000 anonymized Biometric data of citizen or Biometric dummy data. The responsibility of supplying the biometric data or creating dummy data shall lie with GoSL.	Performance testing in Chapter 5.7.1 of Volume 2 indicates that the test scenarios for enrollment is between 0 to 4 million database size and 4 to 8 million database size. Will GoSL be providing the anoymized biometric dataset for 8 million records? What is the format of the datasets been given?		GoSL will provided anonymised 1000 dummy dataset of all three modalities. MSI may use this dataset to create 8 million dummy records for performance testing. MSI will be provided Raw datasets. Confirmation to be sought from GoSL.
718	Volume 2	5.7.1 Performanc e Testing. Table 15: Performanc e of SL-UDI information system	67 and 68		Given the requirements in the table whereby the maximum throughput is 8000 X 24 hours = 192,000 enrollment per day. Given an 8 million database, in order to verify the performance accurately, GoSL would need (8,000,000 / 192,000) = approx 41 days to do the performance testing. Is the performance testing for 24 hours enough to proof the capability of the system?		The maximum throughput to be demonstrated per day per 24 hours cyclce is peak enrollment rate of 75000 enrollments. Two test scenrios of 0-4 million and 4-8 million are considered for enrollement in deduplication in 24 hours cycle.
719	Volume 2	5.7.1 Performanc e Testing.	69	**Authentication Request Rate (Basic Performance)** – 0.1 million Authentication Requests are expected per hour with a response service time of **0.5 to 1 second** with 800 concurrent users during basic performance test at system level. **Authentication Request Rate (Advanced Performance)** – 0.1 million Authentication Requests are expected per hour with a response service time of **0.5 second** with 800 concurrent users during advanced performance test. Test Duration – Duration in which 1:1 matching authentication completes as per expected SLA of **0.5 to 1 second at the system level.**	The Response time for 0.5 to 1 seconds for 1:1 authenticaton seems to be highly unrealistic to meet in a complex system for 4 to 8 millon database size. (Fingerprint,Face and Iris template extraction at the registration client using BioSDK averages 200 milisecond (0.2 second) with quality check and without 1:1 authentication for most technology suppliers. To do a round trip 1:1 authentication and to retrieve the single template from the ABIS including network latency would easily be more that 0.5 second. Each 1:1 authentication requests needs to go through the MOSIP registration Processor and MOSIP authentication module. 1. Does the SLA response time include template extraction at the registration client? 2. Does the SLA response time include template extraction from the ABIS? 3. Does the SLA response time include the 1:1 matching time for the template extracted at the registration client to be compared with the template from the ABIS? 4.Would NSIG be able to give the breakdown for the timings required for the Biometric template extraction at the registration client, timing required for the single biometric template extraction from the ABIS and the 1:1 authentication timing at the MOSIP authentication processor?		1. The response time for 0.5 to 1 seconds for 1:1 authentication is at the system level and does not in account the network latency. 2. Authentication is outside the ABIS system and response time of 0.5-1 sec is measured at the system level 3. Answered at question no. 1 and 2

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
720	Volume 2	5 Scope of Services 5.1.3.2 Customer Relationship Management 5.1.4.1 SL-UDI Citizen Portal	20, 35,37	P20: 44. The proposed services/modules offered/interfaced to/with the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English). P35: 10. The CRM solution should support at least Sinhala, Tamil, and English Languages P37: (viii) The portals should support Sinhalese, Tamil, and English languages.	Could you please define what service or modules exactly to have tri-languages? or can you confirm only CRM/Portals are considered as public-facing? Is manual adjudication considered as well?		1. Citizen portal will be in tri-languages 2. MOSIP UX will be in tri-languages. 3. The contact center manpower will be provided by GoSL, who will be trained to answer the query in tri-language. Content to be provided by MSI in tri-language. 4. ABIS based manual adjudication will be done in english by GoSL.
721	Volume 2	5 Scope of Services	28	5. The MSI should carry out end-to-end security assessments prior to the Go Live of the Foundational ID platform launch and fix any issues found. Further, the GoSL / a GoSL nominated party will conduct security assessments periodically post implementation phase, and the MSI should fix any vulnerability issues identified during assessments.	a) Could you please elaborate on what is required from the bidder to support a GoSL nominated party (eg. Sri Lanka CERT)? b) What are the security compliances that bidder needs to implement and will be assessed / audited by GoSL nominated party?		The scope is self explainatory.
722	Volume 2	5.1.6 Solution Testing 5.2.1.1 Data Center Strategy of Project 5.8.1.7 Security Requirements – Security Operations	43, 49	P43 3 Security Testing (including Penetration and Vulnerability testing) The GoSL may also involve third party auditors to perform the audit/review/monitoring of the security testing carried out by the MSI. P49 (vi) Shall conduct periodic security audits of the data center and report annually. P80 8. Support SL-UDI during external certification and other security audits – such as ISO 22301, ISO 27001, etc.	It is our understanding that the all costs of certification security assessments and annual audit support will be borne by GoSL. **Please reconfirm our understanding.** In case the bidders have the bear the cost, please clarify what are the cost components involved and confirm the exact cost for each component that will be incurred to enable the bidder to take the same into its costing.		1. Yes
723	Volume 2	5.7 Performance Testing, Security Compliance & Audit, Acceptance and Go-Live	68	vi. Fingerprint (1 or multiple), Iris (both), Face or any combination thereof will be used for Performance testing.	For enrollment process, the capturing of biometrics such as Finger , Face and IRIS are sequential in nature, post enrollment, if any combination is needed, a fusion score for the matching is generated, please clarify that this understanding is correct. Please kindly remove the performance testing of "any combination" as different combinations have different speeds and accuracies.		1. Your understanding is correct 2. For performance testing all three combinations will be used.
724	Volume 2	Table 13: Volume of Biometric Capturing Devices	61 and 62		Does the MSI needs to provide for 3 different brands of Fingerprint authentication devices? 3 different brands of Iris Authentication devices and 3 different Brands of Facwe Authentication Device		Yes

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
725	Volume 2 Annexure 11	1. Introduction Overall Logical design of the SL-UDI system	4		The logical design of the SL-UDI System diagram depicts that the SL-UDI system is on a cloud infrastructure. Please kindly advise that the MOSIP foundation ID platform and the ABIS is hosted on-premises or on an cloud infrastructure		On Premise. The SLUID information system is proposed to be hosted on premise.
726	Volume 2	5.8.1.5 Security Requirements – ABIS and Biometric Device Security Requirements 5. Ensure encryption of enrolment packet at biometric device hardware level within the Secure element of the Biometric Hardware	78-79	**5.8.1.5** Security Requirements – ABIS and Biometric Device Security Requirements - Point 5 **Point 5:** Ensure encryption of enrolment packet at biometric device hardware level within the Secure element of the Biometric Hardware	TOR requirement - “Ensure encryption of enrolment packet at biometric device hardware level within the Secure element of the Biometric Hardware.” As per MOSIP specifications, the enrolment devices are at L0 level, meaning the encryption and signing of the enrolment packet is done at the host level and not on-board device. The on-board encryption and signing is required for authentication devices which are at L1 level. Please update this requirement according to MOSIP specification		Requirement remains unchanged.
727	Volume 3	General Conditions of Contract - Confidential Information	22-23	The Clause 17 is the unilateral clause, wherein Employer is the Disclosing party and the contractor is the Receiving party .	Since, both the parties will be sharing information, the clause should be bilateral wherein the party sharing the confidential information be termed as Disclosing party and other party be termed as Receiving party.		Clause is self explainatory
728	Volume 3	General Conditions of Contract - Execution of Facilitities - Representative	25-26	As per clause 18.2.7 for appointment, removal or change of Representative by Contractor, consent of employer is required.	It is suggested to change the requirement of "consent " to "**intimation**".		No Change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
729	Volume 3	General Conditions of Contract - Risk Distribution Transfer of ownership	41	As per clause 35.1 ownership of the IT Product and services (except software and documentation) will be transferred on the delivery.	It is suggested to amend the clause to transfer the ownership of the IT product and documentation **on the receipt of the payment** by the Contractor.		Agreed. The title would be passed on the receipt of the payment.
730	Volume 3	General Conditions of Contract - Termination	53	As per clause 46.3 (e): The contractor is under obligation to "deliver to the Employer all drawings, specifications, and other documents prepared by the Contractor or its Sub-Contractors as of the date of termination in connection with the Products and/or Services"	Since only the non - proprietory information/document can be shared, it is suggested that the clause should be amended by adding " to the extent legally possible" and " Non-propritary" word, as: "**to the extent legally possible** deliver to the Employer all **non-proprietory** drawings, specifications, and other documents prepared by the Contractor or its Sub- Contractors as of the date of termination in connection with the Products and/or Services."		This can be discussed at the time of contract or negotiation.
731	Volume 3 and Volume 2 - Annexure 9	Particular Condition, Completion Time Guarantee **and** 9.1.7 Performanc e and Liquidated Damages	66 (Volume 3) and 8,14, and 15 (Volume 2, Annexure 9)	As per clause 9.1.7 of Annexure 9 of Volume 2 the Liquidated Damages mentioned in RFP are applied as a percentage of total contract value (for the measured month)	It is recommended that clause should be amended and the liquidated damages should be calculated only on the delayed portion of the value of Biometric solution quoted in Financial Bid.		No change
732	Volume-2	Annexure 11	e number i	Web Portal and Mobile Application for multiple stakeholders. The portal shall support multiple channels including mobile devices.	Kindly confirm whether the SL-UDI solution is expected to include native Android and iOS mobile applications in addition to a responsive web portal, or if a responsive web-based experience alone will meet the requirement for mobile access.		Mobile application should run on both IOS and Android
733	Volume-2	Annexure 11	42–43	The SL-UDI system shall support Sinhala, Tamil and English across all user-facing interfaces, notifications and communications.	Please clarify whether the MSI is responsible for preparing all Sinhala and Tamil translations (including UI labels, notifications, help text and user manuals), or whether officially approved translations will be provided by the Government of Sri Lanka.		Yes, this is in scope of MSI.
734	Volume-2	Annexure 11	10–11	The SL-UDI system shall interface with various external systems through secure, standards-based integration mechanisms.	To enable accurate effort estimation and integration planning, we request a consolidated list of external systems that SL-UDI must integrate with, together with the expected protocols (REST/SOAP/Batch), authentication methods, and indicative transaction volumes for each.		Illustrative list of applications: 1. eNIC for data interfacing (Demographic) 2. SMS and payment gateway 3. 3 Sample application 4. Anti-DDOS to provided by GoSL (Telecom service provider) 5. Contact center, Helpdesk and Citizen portal.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
735	Volume-2	Annexure 11	33–35	The Service Billing System shall facilitate payments for services rendered through the SL-UDI ecosystem.	Kindly confirm whether the Service Billing System is expected to integrate with a national payment gateway approved by the Government of Sri Lanka, and if so, please identify the preferred gateway(s) to be used.		Payment gateway to be provided by GoSL. MSI to integrate
736	Volume-2	Annexure 3 –	2–4	The MSI shall provide all required tools necessary for development, testing, and ongoing operations of the SL-UDI system.	We request confirmation on whether the Government of Sri Lanka already operates any enterprise tools (such as ITSM platforms, monitoring systems, project management tools or code quality scanners) that MSI should use, or whether MSI is expected to provision and license all such tools independently.		BOM provides the list of tools and artificats to be supplied by MSI. In addition, any tool/artifact as required for the project, the MSI may propose.
737	Volume-2	Annexure 2 –	59–63	The SL-UDI system shall meet performance, scalability, availability and reliability requirements to support the expected national workload.	To size the solution appropriately, we request guidance on the baseline workload assumptions—including peak authentication throughput (TPS), daily enrolment volumes, expected number of concurrent portal users, and target API response times—that bidders should consider during system sizing and performance planning.		Please refer to Annexure 5 - Demand capacity.
738	Volume-2	Annexure 14	1–3	A list of indicative trainings for various SL-UDI stakeholders including operational teams, field staff, and administrators is provided.	For accurate estimation of training development and delivery efforts, kindly confirm the expected number of participants per batch, the number of batches required for each training category, and whether training materials must be delivered in Sinhala, Tamil and English.		Already answered in S.No. 36
739	Volume-2	Annexure 1A	3–6	The current DRP system and associated subsystems form the existing identity management environment.	Please confirm whether data migration from existing DRP, eNIC, and any other legacy repositories is within the MSI scope. If so, kindly provide approximate record volumes, the types of datasets involved, and any known data-quality considerations that should be factored into migration planning.		Data interfacing with eNIC for populating demographic data of applicants in the MOSIP module
740	Volume-2	Annexure 3 –	13–15	The SL-UDI system shall generate and deliver SMS and email notifications for various events and service workflows.	Please clarify whether the SMS and email gateway services will be provided centrally by the Government of Sri Lanka, or whether MSI is expected to procure, configure and integrate new gateway services as part of the solution.		SMS and payment gateway to be provided by GoSL and Integration with SL-UID information system has to be done by MSI.
741	Volume-1	Data Governa	40–42	The SL-UDI system shall comply with the Government of Sri Lanka's data retention, archival and disposal policies across all information categories.	Kindly specify the retention and archival durations applicable to key data categories such as identity repository records, logs, audit trails, CRM interactions, and documents to ensure that the solution's purge and archival mechanisms conform to regulatory expectations.		No data will be deleted. Active data logs will be maintained for a period of 1 year.Thereafter data will be archived. The IT policies will be shared with the successful MSI.
742	Volume-1	Security – Dig	46–48	The SL-UDI solution shall incorporate digital signing and certificate-based security mechanisms aligned to national standards and PKI policies.	We request confirmation on whether a national Root CA/PKI service will be made available for SL-UDI. Additionally, please provide guidance on the required signing algorithms, key sizes, certificate policies, and any mandated certificate issuance workflows for system-generated documents and transactions.		The reference is not found in volume 01 it is further clarified that there is no requirement of PKI solution or authentication.
743	Volume-3	Testing Requ	12–17	Performance, volume, scalability and stress testing shall be conducted to validate the SL-UDI system under peak and near-peak load conditions.	To appropriately size test environments and prepare performance test scripts, we request indicative load profiles including expected transactions per second, virtual user concurrency, and anticipated peak workload patterns that bidders should assume during performance and stress testing.		Already answered in S.No. 717
744	Volume-3	Test Data	18–19	Suitable test data sets, including anonymized or masked data, shall be used during various test phases to ensure compliance and security.	Please clarify whether GoSL will provide anonymized/masked test datasets and mock interfaces for external systems, or whether MSI must independently prepare these datasets and simulated endpoints as part of the testing activities.		Already answered in S.No. 717

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
745	Annexure-2	Annexure 11	29	The solution shall support fraud detection, risk scoring and monitoring capabilities to identify anomalous or suspicious identity-related events.	To design the fraud and risk detection components accurately, we request clarification on the specific fraud scenarios that must be addressed (e.g., duplicate identities, unusual transaction patterns, repeated failed authentications), and whether GoSL will provide any existing rules, datasets, watchlists or models that must be incorporated into the solution.		Illustrative list suggested by the bidder seems ok. Detailed requirement will be arrived at the stage of implementation.
746	Volume-1	Helpdesk & S	55–57	The MSI shall ensure that user support and helpdesk functions are integrated into the overall operational framework of SL-UDI.	We request confirmation on whether the MSI must integrate application-level support into an existing central ITSM platform operated by GoSL, or whether the MSI is expected to provision a separate ITSM tool with defined processes and integration points.		MSI is to provision ITSM tool with defined processes and integration. There is no GoSL operated ITSM tool.
747	Volume-1	Notifications	51-53	The SL-UDI solution shall support citizen communication and notifications across relevant service workflows in Sinhala, Tamil and English.	We kindly request clarification on whether the MSI is expected to draft and maintain all multilingual notification content (including SMS, email, and in-portal messages), or whether GoSL will provide approved Sinhala, Tamil, and English text templates to be used across the system.		Already answered in S.No. 733
748	Volume-2	Annexure 11	10-11	The integration middleware shall support secure, scalable interfaces for internal components and external partner systems.	To correctly size the integration middleware components, we request indicative figures for peak and average API transaction volumes expected across partner integrations and internal system-to-system interactions. This will enable accurate capacity planning and connection-pool sizing.		Please refer to annexure 5 - Demand Capacity
749		External Firewall		Firewall should support client-based ~~SSL/TLS as well as~~ IPSec VPN Tunnels.	Firewall should support client-based SSL/TLS or IPSec VPN Tunnels.	Since SSL/TLS has many vanuribilities in recent days vendors are moving to more secure protocal like IPSec for tunnel creation	The firewall solution shall support both client-based SSL/TLS VPN and IPSec VPN tunnel capabilities, to address diverse remote-access and site-to-site use cases. SSL/TLS VPN implementations shall support TLS 1.2 or higher, strong cipher suites, and secure authentication mechanisms, with legacy and insecure protocols disabled. Support for SSL/TLS VPN shall be implemented using current, secure protocol versions and configurations; deprecated or vulnerable SSL/TLS versions shall not be permitted.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
750		External Firewall		Minimum Concurrent Sessions with Layer 7 NGFW and Application control enabled: 5Million (if as per bidder architecture they require more capacity they should plan for it)	Minimum Concurrent Sessions- 5Million	Since connection establishment occurs at Layer 4, concurrent session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The proposed firewall architecture shall support a minimum of 5 million concurrent sessions under production conditions with Layer-7 NGFW and application control enabled, with bidders free to meet this requirement through scale-out or aggregated designs.
751		External Firewall		Minimum New Connections per Second with Layer 7 NGFW and Application control enabled: 200K (if as per bidder architecture they require more capacity they should plan for it)	Minimum New Connections per Second- 200K	Since connection establishment occurs at Layer 4, New session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The proposed firewall solution shall support a minimum of 200,000 new connections per second under production conditions with Layer-7 NGFW and application control enabled, with bidders permitted to meet this requirement through scale-out or distributed architectures.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
752		Internal Firewall		The firewall appliance should not include any wireless, Bluetooth, or infrared interfaces or tunnelling mechanisms that allow unauthorized access. Each appliance must be equipped with redundant and hot-swappable power supplies, ~~fan modules/trays,~~ SSDs, and interface slots.	The firewall appliance should not include any wireless, Bluetooth, or infrared interfaces or tunneling mechanisms that allow unauthorized access. Each appliance must be equipped with redundant and hot-swappable power supplies and storage (SSDs).	Hardware redundancy implementation varies by firewall platform design. In many enterprise-grade appliances, cooling components and interface ports are designed as fixed or chassis-level elements while still meeting high availability and reliability requirements. Mandating hot-swappable fan modules and interface slots makes the requirement vendor-specific and may exclude compact, high-performance platforms that achieve redundancy through alternate architectural designs. Retaining redundancy requirements for critical components such as power supplies and storage sufficiently meets availability objectives.	The firewall appliance shall not include any wireless, Bluetooth, or infrared interfaces or tunneling mechanisms that permit unauthorized access. Each appliance shall be equipped with redundant and hot-swappable power supplies and storage, and shall provide redundant cooling mechanisms and network interface redundancy, either through hot-swappable components or equivalent architectural design, without requiring service downtime.
753		Internal Firewall		Minimum Concurrent Sessions with Layer 7 NGFW and Application contron enabled: 15Million (if as per bidder architecture they require more capacity they should plan for it)	Minimum Concurrent Sessions- 15Million	Since connection establishment occurs at Layer 4, concurrent session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The proposed firewall solution shall support a minimum of 15 million concurrent sessions under production conditions with Layer-7 NGFW and application control enabled, with bidders permitted to meet this requirement through scale-out or distributed architectures.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
754		Internal Firewall		Minimum new Connections per Second with Layer 7 NGFW and Application control enabled: 300K (if as per bidder architecture they require more capacity they should plan for it)	Minimum New Connections per Second- 300K	Since connection establishment occurs at Layer 4, New session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The firewall solution shall support a minimum of 300,000 new connections per second under production conditions with Layer-7 NGFW and application control enabled, with bidders permitted to meet this requirement through scale-out or distributed architectures
755		Security Information and Event Monitoring (SIEM)		The solution should offer a single view of all the data captured from devices across all sites and the SIEM solution should be consistent in Gartner's Leaders Quadrant across last 5 years (2019-2024)	The solution should offer a single, centralized view of all data captured from devices across all sites, and the SIEM solution should be recognized by leading industry analysts such as Gartner.	1.Since this clause conflicts with the global clause defined in Volume 02 of 03 – Annexure 3: Minimum Technical Specifications (Page 3, Section 3.2: Product Benchmarking), we respectfully propose that this clause be removed to maintain consistency and avoid ambiguity in technical evaluation. 2.Mandating consistency in Gartner's Leaders Quadrant over a fixed multi-year period makes the requirement vendor-specific and commercially restrictive	The solution shall provide a single, centralized view of all security and log data captured from devices across all sites. The proposed SIEM solution shall be a widely adopted, enterprise-grade platform, and shall have been positioned as a Leader or equivalent top-tier category by at least one reputed global analyst firm in line with the benchmarking criteria defined in Volume 02 – Annexure 3.
756		Security Orchestration Automation and Response (SOAR)		Solution should provide for dissolvable agents for machines that are under investigation to unobtrusively perform forensic tasks on those machines for Windows, Linux, and Mac platforms.	Delete	Forensic analysis is not a native function of SOAR platforms; therefore, we respectfully request deletion of this requirement.	The item is dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (From Potential bidders)	Response (From NISG)
757		Network Access Control		The solution should support Federal Information Processing Standard (FIPS) 140-2	The solution should comply with applicable security and encryption standards relevant to Network Access Control (NAC) functionality.	**FIPS 140-2 certification applies to cryptographic module**s used for data encryption and is typically mandated for security devices such as firewalls, VPNs, and HSMs. Network Access Control solutions primarily perform authentication, authorization, posture assessment, and policy enforcement, and do not function as primary cryptographic enforcement points. Making FIPS 140-2 mandatory for NAC is not a standard industry requirement	FIPS 140-2 compliance is not mandated for the NAC solution as a whole. However, where the NAC solution implements cryptographic functions (e.g., TLS communication, RADIUS authentication, credential protection, API integrations), such cryptographic modules shall support FIPS 140-2 validated algorithms or operate in FIPS-compliant mode

RESPONSE TO QUERIES SET 2 OF NISG RFP NISG/SLUDI-2025

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
1	Annexure 3:	3.4.1.4	86	Solution shall consider rack awareness and failure domains while implementing	Please remove this clause, justification given below: **Justification** The object storage rack includes multiple PDUs to ensure redundancy and maintain failure domain isolation. Placing each node in a separate rack would significantly increase the rack footprint and exceed the available rack space requirements.		The concern raised by MSI regarding rack footprint and physical space constraints is noted. However, the intent of the original clause is not to mandate one node per rack, but to ensure that the solution supports rack awareness and appropriate failure-domain isolation in line
2	Annexure 3:	3.4.1.4	86	Nodes shall be placed with Rack awareness	Please remove this clause, justification given below: **Justification** Object Storage RACK has multiple PDU for redundency and		Same as S.No. 1
3	Annexure 3:	3.4.1.5	87	The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection.	Please modify the clause as given below, justtification for the same is also given below: The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% Data availability with built-in redundancy and dynamic drive protection. **Justification** 100% Data Availability ensures that data will be available for		Suggestion is acceptable provided the MSI adhere the overall uptime SLA as per the service level agreement Annexure 9.
4	Annexure 3:	3.4.1.5	89	The proposed storage solution should support snapshot capabilities, ensuring efficient data protection and recovery. It must include the necessary software licenses	Please modify the clause as given below, justtification for the same is also given below: The proposed storage solution should support snapshot capabilities upto 1000 snapshot per volume, ensuring efficient data protection and recovery. It must include the necessary software licenses **Justification** Supporting large number of snapshot (up to 1000 per volume)		The proposed storage solution should support scalable, policy-based snapshot capabilities and ensuring efficient data protection and recovery in line with SLUDI RPO/RTO requirements. The solution shall support enterprise-grade snapshot scalability without hard architectural limits and shall include all required
5	Annexure 3: Minimum Technical Specification	3.4.2.12 Project Management Tool	163	The tool should be supported by a mobile application	Is it mandatory for the Project Management tool to have a dedicated mobile application, or would access through a web browser using a URL to view reports and project status be acceptable?		MSI to bring their own project management tool.
6	Annexure 3: Minimum Technical Specification	3.4.2.12 Project Management Tool	163	The dashboards should provide a quick and complete view on every aspect of the project, in a form that is easy to grasp and understand. It should be available on a real time basis and allow for customizations to create different dashboards	1. Could you please clarify what is meant by 'every aspect of the project'? 2. If dashboards and reports such as sprint progress, task tracking, team member utilization and availability, Kanban boards, release dashboards, test and defect reports,		Already answered in S.No. 5
7	Annexure 3: Minimum Technical Specification	3.4.2.12 Project Management Tool	163	A Gantt chart or any related tool for visual interpretation of the milestones, dates and activities for the project is needed. The Gantt chart or related tool should be able to add tasks to people and monitor the status of each project task. The tool should also be able to add the	Is it mandatory for the tool to provide a traditional Gantt chart with task-level dependencies, or would a timeline view of features and stories across sprints within a planning interval (with weekly and monthly views), along with a story dependency visualization board across sprints and between teams, be acceptable for visualizing project progress and		Already answered in S.No. 5
8	Annexure 3: Minimum Technical Specification	3.4.2.12 Project Management Tool	163	The tool should be able to create a report on every project feature which can be customized to provide the data as required. The reporting should allow to track planned and actual progress of the different ongoing activities in place. The reports	Is it mandatory for all reports to be downloadable in formats such as CSV, Excel, and PDF, or would real-time view-only dashboards for planned versus actual progress, along with certain downloadable reports (e.g., custom DIY reports, test and defect reports), be acceptable to meet your reporting		Already answered in S.No. 5

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
9	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	Video wall with controllers, speakers, and other accessories	1. Please provide specifications of Video wall 2. what will be the size of NOC/SOC room size in LxWxH to accommodate the video wall display? 3. Wheather NOC/SOC resources will share the same work-space?		1. Video Wall requirement is dropped. 2. Video Wall requirement is dropped. 3. NOC and SOC premises are
10	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	LED TV- (4 X 4 configuration)	1.There is already a requirement of Video wall. Please confirm what is the requirement for LED TV. 2. If required what is the purpose and specifications of the LED TV, including size? 3. Whether 4x4 configuration, means 16 TV screens and wheather the room can accommodate 4x4 configuration in a		Requirement of LED TV and video wall is dropped. However, MSI is requested to look into the requirement of the desktop monitors for NOC and SOC as provided in annexure 3
11	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	57. Laptop (for manager and L1 analysts)	There is already a requirement of Desktop / Monitors for NOC/SOC resources. Please clarify wheather laptops are also need to be supplied for them? 2. If yes, please specify the qty of laptops?		1. We need desktop and monitors as provided in Annexure 3. We don't need laptop for NOC and SOC resources.
12	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	58. Desktops / Monitors (13 resources X 2 monitors each)	1. What is the exact requirement - Desktop or Monitor or both? 2. Wheather two monitors required with each desktop and the purpose of the same? 3. As per the manpower required for NOC/SOC in the demard capacity annexure, max number of resources in one shift is only 6, and the desktop for these resources can be shared		1. Please refer to demand capacity- Annexure 5 . 2. Two monitors per desktop is not required. Single is sufficient. 3. Yes, NOC and SOC desktop requirement should be calculated
13	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	60. IP Phone 61. IP PABX	Please provide quantity and specifications of the IP Phones and IP PABX		Requirement of IP phone and IP PABX is dropped for SOC .
14	Vol 2 of 3	7 Schedule of Requirements - NOC / SOC	159	63. UPS – 20KVA	1. As the electrical power and cabling is being done by GoSL, please clarify if UPS still needs to be provisioned by MSI. 2. If required, Please povide specifications of the same (In the Annexure 3 the UPS specifications are only for 650VA UPS)		In the NOC and SOC facility , UPS is not be provisioned by MSI for desktops.
15	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.3.3.17 Email Solution	67	12. User mail box size should be 20 GB minimum	How many Mail boxes of this size?		Email solution is dropped.
16	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.3 Blade Chassis	83	2. Blade enclosure should support all x86 based Intel/AMD processor blade servers	Is it mandatory to support both Intel and AMD processor blade servers? Can we propose Blade Chassis that supports intel only blades?		yes
17	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.3 Blade Chassis	83	3. Chassis should have sufficient number of redundant converged modules with 100Gbps ports to provide a minimum FCoE uplink bandwidth of 100 Gbps per blade server for a fully populated chassis for converged Traffic	Instead of 100 G FCOE cards , can we propose 100G ethernet and 32G FC separately?		The blade chassis shall provide sufficient redundant network and storage connectivity to ensure an effective bandwidth equivalent to a minimum of 100 Gbps per blade server for converged workloads. This may be achieved through FCoE or through a combination of high-speed Ethernet (minimum

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
18	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.3 Blade Chassis	84	11. The same management solution should also be capable to manage Rack Servers along with Blade Servers and it should provide the visibility to virtualization infra of the leading hypervisor as well as to the SAN environment of leading OEMs like	Can we propose separate Management solutions for external Storage Management and Virtualization Infra Management?		Agreed
19	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.4 STORAGE: ENTERPRISE GRADE OBJECT STORAGE SOLUTION	85	7. Storage solution should support MOSIP platform via RESTAPI integration	Is it acceptable if the storage provides a standards-based REST API, such as S3-compatible, that MOSIP's object-store module can call		Agreed
20	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.10 Network: Core Switches - LAN	98	1. Core Switch should meet/exceed following hardware features/capacity.	The transceiver requirement for 2 switches or per switch?		Requirement Is dropped.
21	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.1.10 Network: Core Switches - LAN	98	1) 1U to 3U and rack mountable in standard 19" rack. 2) 8 GB RAM and 8 GB Flash and 80MB Packet buffer. 3) Hot swappable 1:1 redundant internal power supply and redundant fan. 4) Minimum 3Tbps of switching fabric and minimum 1Bpps of forwarding rate. 5) Loaded with 6x 100Gbps transceiver, 24x 10Gbps transceiver and 8x 1/10Gbps Base-T copper module. Both fiber	Is it possible to increase the Rack unit size to 8U?		Requirement Is dropped.
22	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.1 VIRTUALIZATION PLATFORM	123	Have in-built software defined storage capability integrated within the hypervisor itself and shall work without the need for any specialized dedicated controller virtual appliance.	This feature appears tailored to a single vendor (VMware). Given the RFP's inclusion of blade/rack servers and SAN storage, is the platform intended to be vendor-agnostic for running VMs on those resources, or is VMware prescribed?		The virtualization platform shall support software-defined storage or external enterprise storage solutions to provide resilient, high-performance VM storage. Storage services may be integrated within the hypervisor
23	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.1 VIRTUALIZATION PLATFORM	122	11. Provide continuous availability for critical application workloads in the event of server failures by creating a live shadow instance of a virtual machine that is always up-todate with the primary virtual machine thus enabling fault	Is this Mandatory feature? This feature appears tailored to a single vendor (VMware).		Already answered in S.No. 22

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
24	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.2 BACKUP AND SECURITY	129	**Disaster Recovery Capabilities:** 1) Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site. It should also include failover and failback capabilities and should be able to perform automatic acquisition of network addresses at the destination site. 2) The Proposed solution should support Continuous replication at VM level. The RPO must be less than 5 Seconds and it must deliver Application consistency. 3) Backup and replication software must deliver maximum investment protection by supporting replication of workloads between dissimilar systems like hyperconverged infrastructure to stand alone servers and storage running similar hypervisors across sites, thereby creating a Disaster recovery environment for production workloads irrespective of the underlying hardware. 4) Backup software should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence	RPOs below 5 seconds are feasible only with Continuous Data Protection (CDP), not standard backups. Is an RPO around 1 minute acceptable to you?		Please refer to RACI Matrix - Annexure 16, for latest RPO and RTO parameters
25	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.3 CLOUD NATIVE BACKUP AND RESTORE	130	3.4.2.3 CLOUD NATIVE BACKUP AND RESTORE	1. If the backup solution proposed under 3.4.2.2 already meets the requirements of 3.4.2.3, is a separate solution for cloud-native backups still needed?		Requirement of Cloud native backup and restore is dropped.
26	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.3 CLOUD NATIVE BACKUP AND RESTORE	131	5. Solution shall provide volume snapshots and App consistent backup and application cloning.	What is meant by Application cloning here?		Already answered in S.No. 25
27	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.2.3 CLOUD NATIVE BACKUP AND RESTORE	131	10. Solution shall support DR and HA	Please elaborate this requirement		Already answered in S.No. 25
28	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.7 VIRTUAL DESKTOP INFRASTRUCTURE (VDI)	194	3.4.3.7 VIRTUAL DESKTOP INFRASTRUCTURE (VDI)	Are You OK with cloud-based VDI Solution?		Requirement of VDI is dropped.
29	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.7 VIRTUAL DESKTOP INFRASTRUCTURE (VDI)	196	19. Proposed hardware solution should have a blade center in both locations with FS SAN connectivity and High availability for VDI.	We note the RFP specifies a blade chassis and blade servers (outside the Biometric section). Is this intended for a VDI use case? We recommend evaluating rack-mount servers instead: they typically offer lower TCO (no chassis tax), simpler scaling in		Already answered in S.No. 28

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
30	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.2 Anti-Advanced Persistent Threat (APT) with High Availability	196	3.4.3.2 Anti-Advanced Persistent Threat (APT) with High Availability	• Kindly clarify the basis or criteria used to derive the stated 30 Gbps throughput specification • Could you provide the file scanning rate in terms of files per hour?		The requirement is hereby clarified that the APT solution shall support a minimum effective throughput of 1 Gbps with all threat prevention features enabled, including IPS, anti-malware, sandboxing, and SSL/TLS inspection. The proposed solution must meet this
31	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.5 Web Gateway with High Availability	190	3.4.3.5 Web Gateway with High Availability	Please confirm if a user count of 4,000 can be considered for sizing and designing the Web Gateway solution		Agreed. The assumption is correct.
32	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.13 Email Gateway with High Availability	222	3.4.3.13 Email Gateway with High Availability	• Please confirm if a user count of 4,000 can be considered for sizing and designing the mail Gateway solution • Could you please specify the expected email routing volume, measured in number of emails per hour?		Requirement of email Gateway is dropped
33	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.21 Security Orchestration Automation and Response (SOAR) with High Availability	251	3.4.3.21 Security Orchestration Automation and Response (SOAR) with High Availability	• Could you please specify the required number of concurrent analysts for the SOAR solution?		Requirement of SOAR is dropped.
34	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.26 Network Detection and Response (NDR)	275		• Could you please specify the required throughput capacity for the NDR solution? • Number of IPs in the environment (excluding VMs): • Virtual Environment: Virtual environment in used? (e.g. VMWare, Hyper-V, Nutanix) • Number of VM Host: How many VM Host?		Requirement of NDR is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
35	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.18 Web Application Firewall (WAF) with High Availability	242	3.4.3.18 Web Application Firewall (WAF) with High Availability	1.Please specify whether you require a hardware or virtual appliance for the WAF deployment. 2.Please specify the average and peak HTTP/S throughput per second (Mbps) related to the above FQDN/Web Applications. • Average throughput for all the above - • Peak throughput for all the above – 3.There are two components in the On-premise WAF deployment: MX and Gateway. MX is the management server which is not mission critical and the gateway is mission critical as the traffic passes through this component. An active – passive HA in between the gateways is possible, do you require gateway HA? 4.Below protections are add-ons and if any of these are required, please specify. Attack analytics - Attack Analytics is a tool to help speed up the security investigation of WAF alerts. It provides a comprehensive view of attacks and attackers targeting your resources. The Attack Analytics service aggregates and analyzes your account's security alerts, identifies common characteristics, and groups them into meaningful security incidents. ThreatRadar - ThreatRadar is an advanced threat intelligence service integrated with Imperva's SecureSphere Web Application Firewall (WAF). It enhances WAF capabilities by		The WAF solution shall be proposed as a hardware appliance and shall be sized in alignment with the APT throughput assumptions already provided in S.No.30 . For web access, bidders shall consider approximately 4,000 concurrent users and size the WAF to support the corresponding average and peak HTTPS traffic, including a minimum 15% growth headroom. The WAF gateway shall be deployed in a High Availability configuration (active–passive), and the remaining node shall be capable of handling 100% peak traffic during failover. The management component is not mission-critical and need not be deployed in HA. The MSI shall propose, justify, and quote the final WAF sizing and throughput based on the above inputs and clearly indicate any optional add-on security features and their performance impact.
36	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.9 Hardware Security Module (HSM) with High Availability	202		• Does the application handle payment-related transactions? • Will Disaster Recovery (DR) capabilities be required? • Please elaborate the point "The solution should support the standard algorithms as per the CCA Guidelines"		1. SL-UDI HSM module will not handle payment related transactions. 2. No. DR capabilities are not required for payment related transactions. 3. HSM solution should meet the
37	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	3.4.3.14 Database Activity Monitoring with High Availability	230	3.4.3.14 Database Activity Monitoring with High Availability	Please fill the following form: https://docs.google.com/spreadsheets/d/1ZbHogxUlDzVTzCliEnnE6S9apY8ixv9F/edit?usp=drive_link&ouid=114431623012823738060&rtpof=true&sd=true		Query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
38	SL-UDI-Volume-02-of-03-Annexure-3-Minimum Tech	General Clarifications			1. Can software solutions be proposed in conjunction with third-party hardware, without including OEM-specific hardware components? • Is it mandatory to propose products in alignment with points a, b, and c under section 3.2 Product Benchmarking, or is compliance with point d alone sufficient? • Do we need Servers/VMs for all the software components? Who will provide these? • Do we need to include server specs to the BOM? • For solutions, where no personal data is processed (EDR and NDR solutions), can cloud based options be used. Gartner quadrant products are cloud based for these solutions • For solutions, where personal data may be processed (DLP and Email Security), can cloud based options be used. Gartner quadrant products are cloud based for these solutions • For directory services and IAM, can we use a non-Gartner product. Sri Lankan solution (WSO2) is being used in other key projects • For purpose of consistent policy management, operational efficiency and cost management can combined solutions such as SASE + XDR be proposed. These would still address the requirement although not explicitly mentioned. If cloud-based options are acceptable then it's something we should consider from a solutioning perspective • Do we need to provide GRC solution. This would require consultancy work to ensure policies and compliance processes are in place in addition to the solution.		1.Can software solutions be proposed in conjunction with third-party hardware, without including OEM-specific hardware components? Ans. Yes. The MSI may propose the solution. 2.Is it mandatory to propose products in alignment with points a, b, and c under section 3.2 Product Benchmarking, or is compliance with point d alone sufficient? Ans. It should be in compliance with section 3.2 3.Do we need Servers/VMs for all the software components? Who will provide these? Ans. MSI should supply according to its solution 4.Do we need to include server specs to the BOM? Ans. Query not clear 5.For solutions, where no personal data is processed (EDR and NDR solutions), can cloud based options be used. Gartner quadrant products are cloud based for these solutions Ans. Cloud based solutions are not acceptable. 6.For solutions where personal
39	SL-UDI-Vol-3-of-Vol-3	14. Taxes and Duties	64	In this Procurement the following taxes are exempted. • Value Added Tax (VAT) • Ports and Airport Development Levy (PAL) • CESS • Customs Import Duty (CID)	• CIF Colombo mean, our responsibility up to port, Ownership will be transferred to Govt entity via Bonded Warehouse.Tthen, who is going clear the shipment and do we have to cost the clearance of equipment, local transport, warehousing, Insurance during the transport and warehousing etc,		Please refer to RFP addendum
40	General	Biometric			Please specify how many of the 1.75M authentications per day will be biometric authentications		Sizing of authentication system should be done for 1.75 Million
41	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023	Requesting a change in the clause as Analyst like Gartner, Forester etc do not publish quadrants for mature technologies and deprecate the quadrants from time to time. With few product quadrants not been updated since last 7-8 years for products like IPS, GSLB, ADC, Rack Server, Blade Server etc. Thus requesting the following change ""Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, AV Test, SE Labs for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. In case quadrant are depreciated or not updated, alternate reputed analyst report to be provided along with 2 large deployment		Please refer to Volume 02 of 03 - Annexure 3: Minimum Technical Specification (Amended), section 3.2 for details on product benchmarking

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
42	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: d. the Vendor has to mandatorily provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario	Requesting a change in the clause as there no many similar projects rolled out. "d. the Vendor has to mandatorily provide at least 2 case studies of ~~similar~~ complex~~ity~~, Large scale, sensitivity and scale where the proposed product is successfully implemented and is in operations ~~for at least last two one years~~ ~~i.e. calendar year 2022 and 2023~~. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario		The condition remains unchanged
43	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	4	Product Benchmarking: e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of	Requesting a change in the clause as there no many similar projects rolled out. " e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of ~~similar complexity~~ complex and ~~dimension~~ large scale where the proposed product is successfully implemented and has been in operation ~~for at least two years as on March 2024.~~ The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms		The condition remains unchanged
44	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 1	204 of 361	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. Suggested Clause: The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).		Already answered in S.No. 55
45	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 6	204 of 361	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. Suggested Clause : SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card. Appliance should also support TLS 1.3 PFS Hardware Acceleration support along with RSA support. The Appliance should also support		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
46	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 10	242 of 361	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	We request team to lower down the requirement a little to accommodate right filt solution with compliance and allow participation. Suggested Clause: Throughput minimum 30 Gbps from day 1 with scalability to upto 90Gbps without changing the hardware appliance		Already answered in S.No. 35
47	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 15	243 of 361	SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. Suggested Clause: SSL throughput 10 Gbps scalable to 20Gbps.		Please consider answer at S.No. 35 above and align the SSL throughput
48	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 22	243 of 361	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. Suggested Clause : Compliance Certificates – RoHS, Compliant EU, EN 60950-1, KCC, TUV FCC etc		Agreed
49	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 11	116 of 361	Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. Suggested Clause : Solution should have VXLAN and VLAN Support.		Agreed. The Server Load Balancer solution shall support standard network encapsulation technologies including VLAN and VXLAN.
50	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 12	116 of 361	Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : Suggested Clause : Should have IPv6 Support for SLB, interfaces, routing.		Agreed. The intent of the clause is to ensure IPv6 support for load balancing, interfaces, routing, and basic traffic filtering relevant to SLB functions, and not to mandate full firewall capabilities

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
51	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 14	116 of 361	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. Suggested Clause: The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Hash, f. Bandwidth, etc		The Server Load Balancer shall support standard load-balancing algorithms, including but not limited to Round-Robin, Weighted Round-Robin, Least Connections, response-time/latency-based methods (bandwidth), and hashing-based methods (e.g., source IP, header, or URL).
52	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023	Requesting a change in the clause as Analyst like Gartner, Forester etc do not publish quadrants for mature technologies and deprecate the quadrants from time to time. With few product quadrants not been updated since last 7-8 years for products like IPS, GSLB, ADC, Rack Server, Blade Server etc. Thus requesting the following change ""Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, AV Test, SE Labs for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. In case quadrant are depreciated or not updated, alternate reputed analyst report to be provided along with 2 large deployment		Already answered in S.No. 41
53	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: d. the Vendor has to mandatorily provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario	Requesting a change in the clause as there no many similar projects rolled out. "d. the Vendor has to mandatorily provide at least 2 case studies of ~~similar~~ complex~~ity~~, Large scale, sensitivity and scale where the proposed product is successfully implemented and is in operations ~~for at least last two one years~~ ~~i.e. calendar year 2022 and 2023~~. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario		Already answered in S.No. 42
54	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	4	Product Benchmarking: e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of	Requesting a change in the clause as there no many similar projects rolled out. " e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of ~~similar complexity~~ complex and ~~dimension~~ large scale where the proposed product is successfully implemented and has been in operation ~~for at least two years as on March 2024.~~ The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms		Already answered in S.No. 43
55	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 1	204 of 361	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. Suggested Clause: The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).		Anti-DDOS is to be provided as a service by GoSL.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
56	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 6	204 of 361	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. Suggested Clause : SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card. Appliance should also support TLS 1.3 PFS Hardware Acceleration support along with RSA support. The Appliance should also support		Already answered in S.No. 55
57	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 10	242 of 361	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	We request team to lower down the requirement a little to accommodate right filt solution with compliance and allow participation. Suggested Clause: Throughput minimum 30 Gbps from day 1 with scalability to upto 90Gbps without changing the hardware appliance		Already answered in S.No. 46
58	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 15	243 of 361	SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. Suggested Clause: SSL throughput 10 Gbps scalable to 20Gbps.		Already answered in S.No. 47
59	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 22	243 of 361	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. Suggested Clause : Compliance Certificates – RoHS, Compliant EU, EN 60950-1, KCC, TUV FCC etc		Already answered in S.No. 48

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
60	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 11	116 of 361	Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. Suggested Clause : Solution should have VXLAN and VLAN Support.		Already answered in S.No. 49
61	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 12	116 of 361	Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : Suggested Clause : Should have IPv6 Support for SLB, interfaces, routing.		Already answered in S.No. 50
62	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 14	116 of 361	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. Suggested Clause: The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Hash, f. Bandwidth, etc		Already answered in S.No. 51
63	Volume 1	3.1.2.5 Technical Score Parameter-Criteria D: Team Constitution and Staffing	31	D1 Qualification, certification and experience of the MSI's team D1.1 Leadership D1.2 Architects D1.3 Engineers D1.4 Track Leads D.15 BSP engineers	As per CV format we have to share 2 profiles for each category under D1 of Criteria D - Lead and Alternate profiles. OR how many profiles to be submitted for each roles D1.1, D1.2, D1.3, D1.4 & D1.5 to score the full marks. Please clarify		Lead and alternate for each position.
64	Annexure 10: Manpower Requirement	10.2 Minimum Qualifications of Key Professional Staff	6 to 50	Experience is mandatory in a similar capacity on - biometric based projects for Project Management Role, Architects, etc.	Requesting to change the mandatory experience on Biometric based projects to Digital Transformation projects for maximum participation		Agreed.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
65	Annexure 10: Manpower Requirement	Security Team	39	***Key Professional Staff*** 1. Information Security Manager Minimum Overall Experience - 10 years Minimum Experience in the proposed role - 6 years ***Specific Qualifications / Requirements*** Experience as information security manager for at least five large scale technology led projects. Experience in following is mandatory in a similar capacity: (a) Experience in managing all aspects of large cybersecurity projects. (b) Managing and performing internal audits at regular intervals and manage external audits. (c) Periodic reviews of emerging technology risks and vulnerability es that may impact the SL UDI project. (d) Ensuring that threats, vulnerabilities, cyber risks are proactively identified and appropriately mitigated, avoided or accepted. (e) Experience in managing at least 3 completed projects for large, enterprise scale clients for security related work.	Request to share the understanding on the term "large scale technology led projects" as the current ask is to have 5 large technology led projects experience. The large projects usually takes 1 to 2 years implementation and 3 to 5 years for support / operations. Hence the ask of 5 large projects experience in 10 years / 6 years is difficult to match. Requesting to relax the experience to 2 large projects for both cases highlighted in RED font in the requirements.		Agreed. The clause should be read as "Experience as information security manager for at least two large scale technology led projects. "
66	Annexure 10: Manpower Requirement	Software Development	42	Key Professional Staff : IT Helpdesk Agents Academic & Professional: BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	Request to modify the academic requirement as below BE / BTech / MCA / Mtech / B.Sc/B.Com/BCA or equivalent		BE / BTech / MCA / Mtech / B.Sc/BCA or equivalent
67	Annexure 10: Manpower Requirement	Software Development	43	Key Professional Staff : NOC Agents Academic & Professional: BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	Request to modify the academic requirement as below BE / BTech / MCA / Mtech / B.Sc/B.Com/BCA or equivalent		BE / BTech / MCA / Mtech / B.Sc/BCA or equivalent
68	Annexure 10: Manpower Requirement	Software Development	43	Key Professional Staff : SOC Agents Academic & Professional: BE / BTech / MCA / MTech or equivalent Certification in relevant tools and technologies, wherever available is desired	Request to modify the academic requirement as below BE / BTech / MCA / Mtech / B.Sc/B.Com/BCA or equivalent		BE / BTech / MCA / Mtech / B.Sc/BCA or equivalent

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
69	Annexure 10: Manpower Requirement	Software Development	43	Key Professional Staff: Administrators (Server, Network, Storage, Database) Specific Qualifications / Requirements: At least 5 years of experience as a Server / Network / Database administrator in a large organization At least 5 years of experience as a Storage administrator in DCs larger than 5000 m² Experience in administering large Storage solutions (>	1. Request to clarify if we have to submit the CV's for Server, Network, Storage, Database separately?		No. However, The resume shall be submitted before deployment of resources at project site for review of GoSL
70	Annexure 10: Manpower Requirement	Experts and Administrators	31	Key Professional Staff: Infrastructure Engineer Specific Qualifications / Requirements: Experience in leading infrastructure aspects for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity (a) Experience in managing all aspects of large infrastructure projects (b) Experience in managing at least 3 completed	Request to share the understanding on the term "large scale technology led projects" as the current ask is to have 5 large technology led projects experience. The large projects usually takes 1 to 2 years implementation and 3 to 5 years for support / operations. Hence the ask of 3 completed large projects experience in 10 years / 5 years is difficult to match. Requesting to relax the experience to 1 large projects for both cases highlighted in RED font in the requirements.		The clause should be read as "Experience in managing at least 2 completed projects for large, enterprise scale clients for IT Infrastructure related work "
71	Annexure 10: Manpower Requirement	Experts and Administrators	32	Key Professional Staff: Network Engineer Specific Qualifications / Requirements: Experience in leading networking aspects for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in a similar capacity (a) Deploying Network Components within the Data Centre and Disaster Recovery Site (b) Experience in implementation and operations of at	Request to share the understanding on the term "large scale technology led projects" as the current ask is to have 5 large technology led projects experience. The large projects usually takes 1 to 2 years implementation and 3 to 5 years for support / operations. Hence the ask of 3 completed large projects experience in 8 years / 5 years is difficult to match. Requesting to relax the experience to 1 large projects for both cases highlighted in RED font in the requirements. And request to remove SDWAN from the mandatory requirement list		It has been clarified that the networking services and the bandwidth shall be provided by GoSL. Hence the network engineer role will perform the implementation and commissioning of network devices within the DC and DR. Considering this, the experience of network engineer should be read as " Experience in implementation and operations

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
72+A73:F73	Annexure 10: Manpower Requirement	Team Leads	22	Key Professional Staff: Track Lead – Network & Security Specific Qualifications / Requirements: Experience in leading the network and security tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a)At least 6 years of experience in IT / networks and telecommunicat ions including at least 4 years as network administration for large missions. (b)Experienc e as main administrator of 3 large network installations (c)Experience in managing at least 5 completed projects for large, enterprise scale clients for information security related work. (d)Should have indepth knowledge of international information security related standards such as ISO 27001, NIST cybersecurity framework, etc. (e)Experience in advising senior management on IS strategies and implementation plans at the organization ecosystem level. (f)Experience in using open sources tools and	Request to modify as below as there are multiple experince requirements and it is diffulclt match with Overall exp ask for Track leads Experience in leading the network and security tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience in following is mandatory in similar capacity (a)At least 6 years of experience in IT / networks and telecommunicat ions including at least 4 years as network administration for large missions. OR (b)Experienc e as main administrator of 3 large network installations OR (c)Experience in managing at least 5 completed projects for large, enterprise scale clients for information security related work. Other Mandatory Requirements: (d)Should have indepth knowledge of international information security related standards such as ISO 27001, NIST cybersecurity framework, etc. (e)Experience in advising senior management on IS strategies and implementation plans at the organization ecosystem level. (f)Experience in using open sources tools and technologies and managing risks and vulnerabilities across the same		Agreed

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
73	Annexure 10: Manpower Requirement	Architects	11	Key Professional Staff: Security and Network Architect Specific Qualifications / Requirements: Experience in designing security architecture for at least 5 (give) large scale technology-led projects. Experience is mandatory on (a) Biometric based projects, (b) DevSecOps, (c) establishing and managing security operation center, (d) governance, risk, and compliance, (e) authentication and authorization standard, (f) information security products design and deployment and (g) business continuity planning Experience is mandatory in information technology security design, operations, encryption, information access, biometric security, and authentication processes. Relevant experience in managing and reviewing the configuration of security devices and solutions such as IAM, DLP, WAF, firewall etc. Experience of projects with ISO 27001 and ISO 22301 compliances	Request to modify the qualifications requirements as below Experience in designing security architecture for at least 5 (give) large scale technology-led projects. Experience is mandatory on (a) ~~Biometric based projects,~~ (b) DevSecOps, (c) establishing and managing security operation center, (d) governance, risk, and compliance, (e) authentication and authorization standard, (f) information security products design and deployment and (g) business continuity planning Experience is mandatory in information technology security design, operations, encryption, information access, ~~biometric security~~, and authentication processes. Relevant experience in managing and reviewing the configuration of security devices and solutions such as IAM, DLP, WAF, firewall etc. Experience of projects with ISO 27001 and ISO 22301 compliances Experience of National Identity project is mandatory Experience or knowledge of MOSIP is desirable		It is clarified that there is a dedicate biometric engineer as a team lead for implementation of biometric solution. The position of Security and Network Architect is for overall SL-UDI solution, hence mandatory condition of chief architect having experience in biometric based project and biometric security is no longer required.
74	Annexure 10: Manpower Requirement	Project Management Roles	8	Key Professional Staff : Support and Operations Manager Specific Qualifications / Requirements "Experience of at least 3 (three) technology-led projects as support manager role in a project of similar scale (scope, timeline, and budget) Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project in the government sector Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project with multiple OEMs, ecosystem partners, subcontractors, etc.	Request to modify as below for maximum participation: Specific Qualifications / Requirements "Experience of at least 3 (three) technology-led projects as support manager role in a project of similar scale (scope, timeline, and budget) Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project in the government sector Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project with multiple OEMs, ecosystem partners, subcontractors, etc. Experience is mandatory in a similar capacity on ~~(a) biometric based projects, (b) DevSecOps,~~ (c) Cloud Infrastructure, (d) Network and		Agreed. Mandatory experience in biometric based projects and Devsecops and cloud infrastructure is no longer required.
75	Vol-2	5.2.1	49	5.2.1.2 Site Set-up GoSL shall provide the physical space for hosting IT Infrastructure in Data Center and Disaster Recovery Center. Upon availability of space for each of the Data Center sites, the MSI shall set-up the site for hosting of SL-UDI Information System. The MSI, in consultation	As per industry best practice , primary datacenter and secondary datacenter should be in different seismic zones to avoid both being affected by the same earthquake, flood, cyclones , power outage, etc. . kindly requesting GOSL to facilitate datacenter accordingly..		The location shall be identified by GoSL and MSI is required to host the infrastructure in the identified locations.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
76	Vol-2	5.8.4	97	5.8.4 Support (Contact Center and Helpdesk) 5.8.4.1 Contact Center Setup and Administration The SL-UDI Information System will require a Contact Center which will be facilitated by GoSL. The Contact Center shall act as a citizen and partner touchpoint and provide resolution of queries of residents and Ecosystem Partners regarding SL-UDI services, Enrolment services, Authentication services, Trusted	1.What is the total number of agents required for the contact center? 2.How many inbound agents are needed? 3.How many Outbound Blaster Voice agents are required? 4.Should the contact center handle multimedia channels such as email, web chat, web callback, SMS, third-party IM chats, social media, and video? If yes, please specify the quantity for each channel.		1. Refer to Demand Capacity Annexure. 2. Refer to Demand Capacity Annexure. 3. MSI to size accordingly 4. Social media and video is not required.
77	Vol-2	5.8.4	97	5.8.4 Support (Contact Center and Helpdesk) 5.8.4.1 Contact Center Setup and Administration The SL-UDI Information System will require a Contact Center which will be facilitated by GoSL. The Contact Center shall act as a citizen and partner touchpoint and provide resolution of queries of residents and Ecosystem Partners regarding SL-UDI services, Enrolment services, Authentication services, Trusted	5.How many Outbound Blaster Multimedia agents are required? 6.What is the expected number of outbound calls per hour? 7.What is the expected number of inbound calls per hour? 8.What is the average queue wait time expected?		5. MSI to size 6. No outbound calls are required 7. Refer to Annexure 5 - Demand Capacity 8. Refer to Annexure 5 - Demand Capacity
78	Vol-2	5.8.4	97	5.8.4 Support (Contact Center and Helpdesk) 5.8.4.1 Contact Center Setup and Administration The SL-UDI Information System will require a Contact Center which will be facilitated by GoSL. The Contact Center shall act as a citizen and partner touchpoint and provide resolution of queries of residents and Ecosystem Partners regarding SL-UDI services, Enrolment services, Authentication services, Trusted Service Providers (TSP) and User Agency (UA) related queries, etc.	9.What is the average talk time on IVR? 10.Please specify busy hours, days, or dates that represent peak periods for your company. 11.Does the contact center experience peak call volumes? If yes, how frequently, for what duration, and what are the typical call volumes? 12.What is the retention period for reports and call recordings?		9. MSI will have to write the script and average talk time on IVR to be decided. 10. The volume is not based on peak periods or busy hours. However, fixed no, of agents have be deployed according to Annexure 5 - Demand capacity 11. Extra volume can be expected during morning hours. However, there is no concept of peak call volume. waiting time have been specified in Annexure 5- DEmand
79	Vol-1	4.12.11	101	4.12.11 TABLE 8 for P7: Cost of Software ATS (Annual Technical Support) 12.Laptop 13.MS Office	Please clarify that the bidder need to procure 1. No. MS office licenses 2. No . Laptops 3. No.Desktops		The quantities of desktop and laptops can easily be calculated by the count of users provided in the Demand Capacity Annexure. These are laoptop for enrollment
80	Tech Spec	3.3.3.17	67	3.3.3.17 Email Solution 12.User mail box size should be 20 GB minimum	Please do confirm for how many users the email solution that bidder needs to consider.is there any preference for cloud or on-		Requirement Is dropped.
81	Tech Spec	3.4.3.7	194	3.4.3.7 Virtual Desktop Infrastructure (VDI) Virtual Desktop Infrastructure (VDI) must have native clients for Windows 8, Windows 10, Macintosh, Linux, Chrome OS, Blackberry OS, IOS, Android and HP WebOS 17.Hardware proposed should ensure performance	our understanding from the RFP that only 200 licenses is required for whose going to use VDI. Pls do confirm		Already answered in S.No. 28
82	Annexure 1:	1.3.2.2	11	Captured biographic and biometric data and payment data, scanned documents, confirmation and certification of captured information are submitted to DRP-HO for Registration Confirmation Process. Following are the steps carried out before the enrolment packet is submitted to IDMS.	As per mosip registration process and workflow, all registration which are initiated are only persisted as reg packet, when registration flow is complete. In event of cancelling the flow, the data is deleted from memory for security and privacy reasons. The encrypted packet once created can only be decrypted on the server side.		Yes. Your understanding is correct.
83	Annexure 1:	1.3.2.2	11	Channel Selection (Auto) - Based on the above, Biographic verification results and according to the verified and not verified fields marked at ARQA task, applications will be diverted automatically into three channels	can you elaborate if there is a need of separate portal for channel selection in amber and red and all the integration touchpoints for the same. Are authorization Green/Amber/Red specific to integration with NRP and independent to SLUDI generation?		The process has been modified to the extent that this channel would be workflow based channels and this will be customized in the MOSIP

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
84	Annexure 1:	*1.3.2.1.1 Pre-Enrolment*	11	After the enrolment completion, the ICAO photograph stored in the e-Studio of DRP will be attached with the enrolment packet. The enrolment packet will be submitted to IDMS and to the Automated Biometric Identification System (ABIS) for 1: N verification.	An ICAO compliant photo is already captured as part of mosip registration process at registration centers (https://docs.mosip.io/1.2.0/id-lifecycle-management/supporting-components/biometrics/biometric-specification#face-capture) Is this a separate system designed by GOSL which has to be		ICAO based photograph would be captured during enrollment process and the same photograph would be used during packet creation.
85	SL-UDI-Volume-02-of-03-Annexure-3	3.6.1.1 ABIS	330	Compliance to MOSIP specification https://docs.mosip.io/1.1.5/biometrics/automated-biometric-identification-system-abis	The current long term support version of MOSIP is 1.2.0 LTS. 1.1.5 is the old version and as per our knowledge this is not supported. Kindly confirm which version to consider as all the deployments		Latest version to be used.
86	SL-UDI-Volume-02-of-03-Annexure-3	3.6.1.2 Multimodal SDK	339	The SDK should come with latest industry practices such as liveness detection	Please clarify in what phase it is requested liveness detection. World over enrolment of applicants does not need liveness a it is operator assisted. Moreover the environment conditions are such that facial liveness detection will be greatly impacted. It is a humble		Agreed. Liveness detection during enrollment process is not required. However, SDK used in facial authentication should have
87	SL-UDI-Volume-02-of-03-Annexure-3	3.6.1.1 ABIS	332	"The DELETE functionality of the ABIS should be disabled by the BSP."	This sentence contradict the following sentence :"On rare occasion, the ABIS will be subsequently directed by the SL-UDI application to delete an existing record". Please clarify.		The delete functionality will be disabled in the ABIS. Howwber on recieveing written instruction from Go-SL a particlular record
88	SL-UDI-Volume-02-of-03-Annexure-3	3.6.1.2 Multimodal SDK	339	Allow customizations as per the country requirements.	Please clarify what are the country requirements that require customization. The SDK is compliant with MOSIP reg client requirements and we believe that any such customization will also		Yes. Your understanding is correct.
89	Annexure-3	3.3.3.19	76-78	N/A (General)	Will the application servers / web servers be deployed on containers / Kubernetes or on traditional Virtual Machine		MSI to decide the details of the solution.
90	Annexure-3	3.4.2.15	168-169	N/A (General)	Are cloud based tools, where the necessary application endpoints need to be exposed to the tool via the internet, acceptable?		No.
91	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement			In addition to installing and tuning its own software, the BSP will also be support for installation and configuration of other software being provided by the MSI. The indicative list of such software includes:	We believe that the BSP role should be specific to the biometric software components. The rest of the software is expected to be managed by MSI. please clarify		your understanding is correct.
92	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		41	The BSP shall roll out the solution after testing. The BSP shall be responsible for application availability while in production and shall deploy the solution at both Primary and Disaster Recovery sites and adhere to BCP plan.	We assume this clause is related to the biometric software components like ABIS, Adjudication Clients and BioSDKs on the client/server.		Yes. Your understanding is correct.
93	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		42	Integration of the manual adjudication with IDMS (BSP to integrate, MSI to support) • Integration of ABIS and biometric middleware with IDMS (BSP to integrate, MSI to support)	We believe this clause needs to read as follows: Integration of the manual adjudication with IDMS (MSI to integrate, BSP to support) • Integration of ABIS and biometric middleware with IDMS (MSI to integrate, BSP to support)		yes. Your understanding is correct. However, In all intergration of aspect, wherever there is ABIS interface or SDK integeration, BSP will support the MSI
94	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		42	The integration of biometric solution with other components of SL-UDI solution as required (BSP and MSI to integrate together)	Please clarify that this means BSP to support on integration while the MSI will deploy resources to actually perform the integration		Aleady answered in S.No. 93
95	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		116	(vi) For biometric manual adjudication, MSI shall be responsible for: a. Support BSP MSI to define a process for biometric manual adjudication b. Support BSP MSI in training on biometric manual	We believe that the BSP will offer training on the Adjudication clients in a train the trainer model with the help of the MSI. This clause is unclear and request to reword the same.		Agreed.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
96	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		119	(ii) The MSI shall provide physical separation of the BSP racks shall be considered as part of the Primary Site and Disaster Recovery Site design by the MSI in consultation with BSP and GoSL.	We understand that this clause is related to providing the ABIS, BioSDKs as part of the BSP scope in a separate rack in both Primary and DR site. Kindly confirm		Yes
97	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		119	(vi) BSP shall be responsible for performing operations as per the BCP plan and shall ensure recovery/backup as per the BCP policy. The BSP will also be responsible for resuming (including rolling back to Primary Site) the biometric solution and associated data. Thus, BSP will be responsible for managing the	We believe this should be under the MSI scope with support from BSP. Kindly confirm.		Biometric data shall be backed up BSP. However, the BCP plan will be responsibility of MSI.
98	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		120	(vii) BSP shall be responsible for coordinating with OEM(s) of infrastructure provided by it.	We believe that the infrastructure will be managed by the MSI and this should be in the scope of the MSI. BSP will work with the MSI to provide hardware sizing for the ABIS, BioSDK (Server) software.		Agreed.
99	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		120	(xii) The Manual Adjudication application of BSP shall be used for manual adjudication post deduplication and for resolution of duplicates. The workflow and integration of manual adjudication shall be the responsibility of BSP with	The workflow of the Adjudication client is generally discussed and agreed with the MSI in collaboration with the end customer. Hence while the BSP provides the Adjudication client software, the final integration will be done by MSI with support from BSP. Hope this is in alignment with your requirements.		Agreed.
100	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		140	The BSP will report on the following: • Quality of Data Capture and Matching: Analysis of captured quality and accuracy of matching on weekly basis o Data Mix-up: Weekly reports regarding mix-up of the particulars relating to one applicant with those of others, if any. The mix-up may be in any of the demographic or biometric data. o Biometric Exception: The Enrolment Software may allow the biometrics to be not captured in exceptional circumstances such as children, old persons, persons with one or no hands, technological issues, etc. The BSP should submit a report about such biometric exceptions. Quality of Operators and Devices: The quality of data is also dependent upon the operator, enrolment center facility and device. Thus, to ensure the good quality of enrolment, the BSP should submit a statistical and quality analysis for	The BSP can support in these tasks but the overall responsibility should be with the MSI. Kindly confirm.		Report to be generated by BSP. Overall responsibility is with MSI
101	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		140	e) The BSP would present the statistical data to GoSL authority on a monthly basis. This will help GoSL to take a decision in case threshold value needs to be adjusted based on inputs from field.	This should be responsibility of the MSI with support from BSP.		Agreed.
102	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		140	f) The BSP should implement a mechanism to remote update of threshold value of capturing process in SL-UDI data capturing application. The patch should be automatically pushed when capture application connects next to SL-UDI data	This should be responsibility of the MSI with support from BSP.		Agreed.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
103	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement		159	49. Replication and Backup Solution (Note: MSI and BSP may bring same solution or their separate solutions)	We assume this clause is related to how we will perform backups using software solution and not related to hardware. The BSP will provide the hardware sizing to the MSI who will be responsible for the deployment and maintenance of the hardware. Kindly confirm		Agreed with the clarification below : Schedule 7, provides an indicative schedule of requirements (list of hardware and software). The MSI
104	Volume 1	3.1(a)	8	In the case of a Joint Venture (JV)/Consortium: a) all partners shall be jointly and severally liable for the execution of the Contract by the Contract terms and	While we understand that in case of JV this clause of jointly and severally liability holds true, our request is that in case of consortium of companies, please make the liability to the extent of the scope of the consortium partner. Since a consortium has a		In case of Consortium, the liability of the consortium parter will to the extent of scope of the partner. However, MSI will be
105	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement	5.1.5.1	40	On its infrastructure, the MSI should install all necessary software and biometric solution supplied by BSP. In addition to installing and tuning its own software, the BSP will also be responsible for installation and configuration of other software (Anti-virus, enterprise management system, etc.) provided by the MSI. The overall responsibility shall lie with the MSI. In addition to installing and tuning its own software, the BSP will also be support for installation and configuration of other software being provided by the MSI. The indicative list of such software includes: a)Enterprise Management System (EMS) Agent b)Security Information and Event Management (SIEM)	The responsibilities mentioned in this clause are part of MSI and BSP will not be able to provide these as they are very specific to the MSI. The BSP will ensure that the core ABIS Engine, BioSDK, Adjudication clients are installed and tuned to the requirements. We request you to remove the rest of the responsibilities from BSP scope and put them under MSI scope with a support from BSP in case it is needed.		Agreed
106	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement	5.7.1	68	Enrolment Rate – Successful capture and encryption of demographic and biometric details of citizen at the rate of 25 minutes per enrolment per kit (1650 kits => 3960 per hour)	Please clarify if the enrolment rate is 3960 / hr or 8000/ hr as there is contradicting information in this clause versus the table given above the clause.		Enrollment is 3960 per hour.. However, 8000 is the peak enrollment rate. The performance testing has to be done considering peak
107	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement	5.7.1	69	Authentication Request Rate (Basic Performance) – 0.1 million Authentication Requests are expected per hour with a response service time of 0.5 to 1 second with 800 concurrent users during basic performance test at system level. Authentication Request Rate (Advanced Performance) – 0.1 million Authentication Requests are expected per hour with a response service time of 0.5 second with	Please confirm what is the authentication request rate as there is contradiction in this clause versus the table above.		In the basic performance test, the gallery size is 4 Million and in the advanced performance test, the gallery size is 8 million. In both basic and advanced perofmrance test, the authentication response time at the system level should be 0.5 to 1 second.
108	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement	5.8.1.10(6)	83	Authentication server shall have replay (presentation attack) detection capabilities. Controls shall be deployed so that the authentication packet once sent for authentication cannot be used again for authentication. ISO/IEC has provided a framework, data format, and testing methodology via its standards ISO/IEC 30107-1, ISO/IEC 30107-2, and ISO/IEC 30107-	Please confirm that this requirement is related to fraud detection from a point of view of reply of a specific transaction and NOT with respect to biometric technology requirement.		The requirement is NOT related to generic fraud detection. The reference to ISO/IEC 30107-1, 30107-2 and 30107-3 clearly establishes that the intent of this clause is Biometric Presentation Attack Detection (PAD)
109	SL-UDI-Volume-02-of-03-Annexure-10-Manpower-Requirement	3.2	3	All components proposed (hardware/software except Biometric Devices and Biometric Software), unless otherwise specified, must be as per criteria defined below: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the	There is no benchmarking for Biometric Software in either of the mentioned reports. NIST is the one that evaluates all biometric algorithms. Kindly change this clause to include NIST.		Agreed.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
110	Volume-2	1.8	10	Knowledge Transfer and Support MSI can access the relevant documentation from MOSIP's website. MSI shall coordinate with the MOSIP team and arrange detailed training for its	We understand that MSP will carry-out its KT on its own and MSI will not be responsible for it. Is our understanding correct.		MSI shall inform the GoSL and MSP about the KT sessions with MOSIP. MSP can also join these sessions
111	Volume-2	5(4)	19	The MSI shall provide a detailed cutover plan before migrating from the legacy system and a roll out plan. Upon providing the plans the	As discussed with NISG, this is a green field project and no migration required. Please confirm.		your understanding is correct.
112	Volume-2	20	11	Card Activation At the time of issuance, the card is in inactive state and before usage of card, it needs to be activated. MSI needs to build and provide the functionality to activate the cards in both online	We understand that beyond card personalisation, all the activities pertaining to card issuance will be the reponsibility of GoSL. Is our understanding correct.		your understanding is correct.
113	Annexure 1: High Level Process Flow	1.3.2.1.1	9	Pre-Enrolment	As discussed with NISG, integration of external system like NRP, etc will with the Pre-enrolment stage only for the purpose of fetching data from the external system. This will be possible only in case the external system allows API based intergrationand facilitates the intehration.		your understanding is correct. Kindly refer Annexure 15
114	Annexure 1: High Level Process Flow	1.3.2.1.2	10	Enrolment Completion Auto Transliteration	Auto Transliteration will be provided from English to Sinhala and Tamil only. This same captured data will be used for the purpose of card personalisation. Please		Your understanding is correct.
115	Annexure 1: High Level Process Flow	1.4.3	18	Diagrammatic View of SL-UDI System	Biometric recollection module is incorrectly mentioned. The only way bioetric recollection will happen be through the enrolment & update process. Please confirm.		Understanding is correct. Recollection will happen through update and correction process.
116	Volume-2	5.8.2.3	89	In the event of a catastrophe, such as a flood or fire, it might lose both your working HSMs and locally stored backup HSMs. To fully protect against such events, always store a copy of	Since HSMs will be availble at DC and DR only and there is no other locally stored back-up, Please amend/remove this clause. It has mentioned Locally stored backup, please clarify what		Locally stored backup data means location other than DC and DR. This location would be specified by GoSL
117	Volume-2	5.8.2.4	89	MSI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible.	MSI will provide and enable a certain number of VPN connections. Please mention how many VPN connections/licenses are required and amend the clause. What exactly is mean to Data Center staff? Please clarify.		Data Center staff implies the technical resources deployed by the MSI. MSI can refer the Annexure 10 - Manpower requirements and provision for the VPN connections / licenses.
118	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.9 Network – Core Router	97	3.4.1.9 Network – Core Router	Please clarify the device quantity required		Solution shall be proposed by the MSI keeping in consideration the SLA and HA requirements. Accordingly exact number should be proposed by the MSI
119	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.9 Network – Core Router	97	3.4.1.9 Network – Core Router	Please ellaborate the requirement for the use of this specific router		Core router has Industry Standard meaning and usage in DC and DRC

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
120	Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.9 Network – Core Router	97	3.4.1.9 Network – Core Router	Clarify whether ISP or MSI should provide this router		MSI shall provision for core router
121	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.10 Network: Core Switches - LAN	98	Core Switch should meet/exceed following hardware features/capacity.	Please specify whether the all 4 CORE Switches will be a single cluster or else specify the architecture		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
122	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.10 Network: Core Switches - LAN	98	Core Switch should meet/exceed following hardware features/capacity.	Please clarify whether fans are Port-Side-Exhaust or Port-Side-Intake		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
123	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.11 Access Switches LAN	100	All 24/48 port should support PoE (802.3af) and PoE+ (802.3at) with a PoE power budget of 740W/1440W	Please specify whether to use 1440W or 720W as the POE Power and for which switches		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
124	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.11 Access Switches LAN	100	3.4.1.11 Access Switches LAN	Please clarify whether this will serve as the core for both the LAN and the Data Center?		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
125	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.13. DC Software Defined networking (SDN) Fabric Architectur	104	3.4.1.13. DC Software Defined networking (SDN) Fabric Architecture	Please clarify the SDN requirement and which components are going to be used in SDN for the solution		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
126	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.13. DC Software Defined networking (SDN) Fabric Architectur	104	3.4.1.13. DC Software Defined networking (SDN) Fabric Architecture	This item is not included in the Schedule of Requirement but a Technical Specification is presented in the Minimum Technical Specification document, Please clarify this.		Please refer to Amended RFP

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
127	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.13. DC Software Defined networking (SDN) Fabric Architecture	104	3.4.1.13. DC Software Defined networking (SDN) Fabric Architecture	Please clarify whether Spine Switches should be considered, as they are listed in the Minimum Technical Specification document but not in the schedule of requirement. If they are required, kindly specify the quantity.		Please refer to Amended RFP
128	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.14 Data Center Spine Switch	107	3.4.1.14 Data Center Spine Switch	This Data Center Spine and Leaf Switches are not Listed under IT Infrastructure section of Schedule of Reuirement in the Volume2-of 3, Please clarify this		Please refer to Amended RFP
129	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.14 Data Center Spine Switch	107	3.4.1.14 Data Center Spine Switch	If required, kindly provide the quantities for the Spine Switches.		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
130	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.15 Data Centre Leaf Switch	107	3.4.1.15 Data Centre Leaf Switch	This Data Center Spine and Leaf Switches are not Listed under IT Infrastructure section of Schedule of Reuirement in the Volume2-of 3, Please clarify this		Please refer to Amended RFP
131	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.15 Data Centre Leaf Switch	107	3.4.1.15 Data Centre Leaf Switch	If required, kindly provide the specifications quantities for the Leaf Switches.		Please refer to Amended RFP
132	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.16 DC/DR Network Monitoring and Operations Dashboard	111	3.4.1.16 DC/DR Network Monitoring and Operations Dashboard	This DC/DR Network Monitoring and Operations Dashboard not Listed under IT Infrastructure section of Schedule of Reuirement in the Volume2-of 3, Please clarify this		Please refer to Amended RFP
133	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.20 Miscellaneous Hardware: Rack	120	42U Rack with USB KVM Switches with LCD monitor. Power panels and connectors shall support dual source and power panels shall include power meters.	Please specify the Rack quantity		MSI has to propose the solution

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
134	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.20 Miscellaneous Hardware: Rack	120	42U Rack with USB KVM Switches with LCD monitor. Power panels and connectors shall support dual source and power panels shall include power meters.	Please specify the connector type of the Power Panel (C13 or UK Type)		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
135	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.20 Miscellaneous Hardware: Rack	120	42U Rack with USB KVM Switches with LCD monitor. Power panels and connectors shall support dual source and power panels shall include power meters.	Please specify whether Horizontal or Vertical power panels are required.		High level Architectural requirements are provided. SLA are also specified. MSI has to propose the solution
136	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Schedule of Requirements	161	Schedule of Requirements	Please clarify who will provide the conectivity among Primary, DC and DR?		GoSL will provide the connectivity
137	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Schedule of Requirements	161	Schedule of Requirements	Please clarify the required bandwidth and throughput for site-to-site connectivity.		Bidder to suggest requirement to meet RTO and RPO, along with justification note.
138	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Schedule of Requirements	161	Schedule of Requirements	Please clarify the Uplink Bnadwidth among CORE and Access, If applicable Spine and Leaf.		Bidder to suggest requirement to meet RTO and RPO, along with justification note.
139	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.31 SOC / NOC – UPS	290	3.4.3.31 SOC / NOC – UPS	Please prvide the proposed Technical Specifications for 20KVA - MSI		Requirement Is dropped.
140	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.5.1.3 USB Hub	302	3.5.1.3 USB Hub	Kindly specify the Quantities		GoSL will provide the USB hub

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
141	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.5.1.3 Internet Dongle	304	3.5.1.3 Internet Dongle	Kindly specify the Quantities		Dongles are to provided by GoSL
142	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Minimum Technical Specifications for Biometric Registration Kits (including Biometric Capture Devices)	304	3.5.1.3 Flashlight	The item has a Technical Specification but the Ite is not listed in the Schedule of Requirement, Please clarify whether the item should be or should not be in the Schedule of Requirement		GoSL will provide the flashlight
143	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Minimum Technical Specifications for Biometric Registration Kits (including Biometric Capture Devices)	304	3.5.1.3 Flashlight	Kindly specify the Quantities		GoSL will provide the flashlight
144	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.5.1.11 QR Code Reader	306	3.5.1.11 QR Code Reader	The item has a Technical Specification but the Ite is not listed in the Schedule of Requirement, Please clarify whether the item should be or should not be in the Schedule of Requirement		Refer to ammended RFP
145	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.5.1.11 QR Code Reader	306	3.5.1.11 QR Code Reader	Kindly specify the warranty details		Already answered in S.No. 144
146	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.5.1.11 QR Code Reader	306	3.5.1.11 QR Code Reader	Kindly specify the Quantities		Already answered in S.No. 144

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
147	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	49	5.2.1.1 Data Center Strategy of Project	Please provide the Floor Plans of the **TWO DATA CENTERS** designed by the GoSL, to do the assessment and Rack Planning.		GoSL will provide the Co-location space for the DC-DR . The MSI to propose the solution as per the RFP meeting the SLAs .
148	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	49	5.2.1.1 Data Center Strategy of Project	Please clarify whether the Fiber connectivity is provided by the MSI or GoSL.		Connectivity between DC and DR shall be provided by GoSL
149	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	49	5.2.1.1 Data Center Strategy of Project	Clarify whose responsible for implementing Physical security suh as physical security, Biometrics access and CCTV		Responsibility of physical security will be responsibility of GoSL
150	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	49	5.2.1.1 Data Center Strategy of Project	Please Expalin in detail the Staging environment described in the Table 9 - Hosting Environment 5.2.2 Hosting Environments in Volume - 2 of 3 under 5.2.1.1. Data Center Strategy Project		Requirement is self explainatory.
151	Volume 02 of 03	5.2.1.1 Data Center Strategy of Project	51	5.2.1.1 Data Center Strategy of Project	Please explain whether the Primary and DR sites are Hot Sites, and Do both of them require Identical configuration.		Kindly Refer to RFP volume 2 of 3, section No. 5.8.2 and 5.8.2.1. Accordingly DC and DR may be designed, sized and configured and meet the SLAs
152	Volume 02 of 03	Table 10: Network Connectivity	55	Table 10: Network Connectivity	Please clarify whether we should provide Human Resources as well as Technical Solution.		Bandwidth / connectivity will be provided by GoSL. The MSI will be responsible for integrating the network connectivity between
153	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	Video wall with controllers, speakers, and other accessories - MSI Decide Kindly specify the Technical Specifications		Requirement Is dropped.
154	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	Video wall with controllers, speakers, and other accessories - Kindly specify the Quantities		Requirement Is dropped.
155	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	Video wall with controllers, speakers, and other accessories - Kindly specify the warranty details		Requirement Is dropped.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
156	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	LED TV - MSI Deide Kindly specify the Technical Specifications		Requirement Is dropped.
157	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	LED TV - Kindly specify the Quantities		Requirement Is dropped.
158	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	LED TV - Kindly specify the warranty details		Requirement Is dropped.
159	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	IP Phones - Specify the Quantities		Requirement Is dropped.
160	Volume 02 of 03	5.9 Security and Network Operations	107	Table 27: Indicative Bill of Material for SOC	IP PABX - Specify the Quantities		Requirement Is dropped.
161	Volume 02 of 03	5.9 Security and Network Operations	109	The MSI is required to setup the NOC for which physical space will be provided by GoSL. The responsibility of the MSI include the following:	Clarify whether the implementation processs and Planning is done by which side and the procedure		MSI will plan the implementation process and take approval from the GoSL SLUDI Project Governance team
162	Volume 02 of 03	Schedule of Requirements - IT Infrastructure	158	47. Data Center Access Switches	Please scpecify whether this is referring to the Data Center Leaf Switches Specified in Volume 2 of 3 - Annexure 3		Refer amended RFP volume 02 of 3, Annexure 3
163	Volume 02 of 03	Schedule of Requirements - IT Infrastructure	158	47. Data Center Access Switches	Clarify whether should we stick to the given quantity or else could we differ the quantity according to proposing architecture		MSI may propose the quantity as per the proposed architecture.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
164	Volume 02 of 03	Schedule of Requirements - IT Infrastructure	158	47. Data Center Access Switches	In Volume 2 of 3, the document specifies 24-Port Data Center Access Switches. However, in Volume 2 of 3, Annexure 3, the Access Switches are listed without a clear decision between 24-Port and 48-Port models. Kindly clarify the requirement.		Refer amended RFP volume 02 of 3, Annexure 3 - Minimum tech requirement.
165	Volume 02 of 03	Schedule of Requirements - IT Infrastructure	158	48. Enteprise Management System	Although the Schedule of Requirements in Volume 2 of 3 mentions an Enterprise Management System, no corresponding Technical Specifications are provided in Volume 2 of 3 – Annexure 3: Minimum Technical Specifications. Kindly clarify.		Refer amended RFP volume 02 of 3, Annexure 3 - Minimum tech requirement.
166	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.1 Blade Servers	80	Blade server should be quoted with minimum 1024 1TB memory, expandable up to 8TB, 4800/5600 MHz DDR4/DDR5 DIMMS	Need clarification on this - To fulfill the initial memory requirement of 1TB, with scalability up to 8TB, the memory module capacity needs to be 256GB. However, this is a costly solution. Additionally, achieving the 8TB memory requirement per server is only possible by populating 32 DIMM slots with 256GB modules. Since servers with AMD		Bidders are free to propose any compliant server architecture (Intel/AMD) and any DIMM sizes that meet the above requirements.
167	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.1 Blade Servers	80	The management solution should provide the capability to manage the blade servers across multiple chassis , rack servers from the same unified console. It should provide the complete administration including operating system installation and firmware management from the single console with a unified view of all the blade servers, server identities, configuration details, monitoring and alerting System shall	Is it possible to offer a server management solution as a SaaS-based service, or should it be provided only as an on-premises (local) solution? Please clarify this.		On-premises (local) solution is only required.
168	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.2 Rack Servers	81	Memory (RAM): Min. 1024 GB scalable up to 8TB of Memory with DDR5 memory DIMMS	Need clarification on this - To fulfill the initial memory requirement of 1TB, with scalability up to 8TB, the memory module capacity needs to be 256GB. However, this is a costly solution. Additionally, achieving the 8TB memory requirement per server is only possible by populating 32 DIMM slots with 256GB modules. Since servers with AMD		Bidders are free to propose any compliant server architecture (Intel/AMD) and any DIMM sizes that meet the above requirements.
169	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.2 Rack Servers	82	Server should support 64Gbps FC ports. Min 4 ports per storage controller	Does each server require 4 Fibre Channel (FC) HBAs with direct connections to each storage controller individually, or are the 4 HBAs connected to the storage appliance in a high-availability (HA) configuration that provides access to multiple controllers? Please confirm		Requirement is self explainatory.
170	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.2 Rack Servers	82	Rear: 1 USB ports (Ver 3.0 or higher); RJ-45 Ethernet;; two RJ-45 Ethernet; Front: One USB (Ver 3.0)/KVM Connector	Please specify - Are these RJ-45 Ethernet connections intended for server management, or are they used for a different purpose? Also, are they 1GbE or 10GbE?		Requirement is self explainatory.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
171	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.4 Storage: Enterprise Grade Object Storage Solution	85	3.4.1.4 Storage: Enterprise Grade Object Storage Solution	This item is not included in the Schedule of Requirement but a Technical Specification is presented in the Minimum Technical Specification document, Please specify the quantities in Schedule of Requirement.		Refer to ammended RFP
172	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.4 Storage: Enterprise Grade Object Storage Solution	85	Delivered as a pre-integrated appliance with minimum 4 active nodes; supports 500TB usable on Day-1 and scales to 1PB within one year.	Please clarify - Is it four active nodes distributed across multiple sites, or four nodes per single site?		Four nodes per single site
173	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.5 SAN (Storage Area Network)	87	3.4.1.5 SAN (Storage Area Network)	The capacity requirement for the SAN storage has not been specified. Please specify the required SAN storage capacity.		Usable size in TB is 200 in addition to 30% overheads and 15% head room with raid 10
174	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.5 SAN (Storage Area Network)	87	3.4.1.5 SAN (Storage Area Network)	The SAN storage requirement for 'other than the biometric solution' has not been specified in the Schedule of Requirement. Please specify.		Already answered in S.No. 173
175	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.5 SAN (Storage Area Network)	89	The Proposed storage system should support Active-Active Storage configuration across two sites replicating to each other for same LUN/volume for zero RPO/zero RTO configuration.	To support an Active-Active storage configuration across two sites, it is essential to specify key parameters such as the distance between the two data centers, the link bandwidth, and the round-trip time (RTT). These factors are critical for ensuring optimal performance, synchronization, and failover capabilities in an Active-		Distance between DC and DR is anticipated to be 20 to 25 kms. MSI has to suggest the bandwidth requirement which will be provisioned by GoSL.
176	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.6 SAN Switch	91	3.4.1.6 SAN Switch	The required SAN switch quantities for 'other than the biometric solution' have not been specified in the Schedule of Requirement. Please specify the required quantities.		Refer amended RFP Volume 02 of 3 : Annexure 3

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
177	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking Clause C	3 of 361	In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave of Forrester Wave or Major Players in IDC MarketScape.	This is an ambiguous clause for Web Application Firewall Solution. Being a technology leading OEM for Web application Firewall, we seek some clarifications. It is important to note that recent third-party reports on Web Application Firewalls (WAF) now include a broader range of solutions, such as cloud-based services (WAAP-as-a-Service) OEMs in addition to traditional hardware OEMs. However, since the current requirement specifically pertains to hardware-based solutions, please clarify whether, for the purpose of evaluating the 4 distinct		Technology OEMs offering Hardware will be counted and considered.
178	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking Clause E	4 of 361	In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of [illegible]	Regarding the Load Balancer (ADC) category, we would like to clarify that the most recent Gartner report available was published in 2016. Additionally, there are currently no relevant reports available from IDC or Forrester for this category. In light of this, kindly advise whether: 1. We may submit a relevant customer use case instead, or 2. The 2016 Gartner report can still be considered valid for evaluation purposes.		In the absence of recent standalone analyst reports for ADCs, the 2016 Gartner report will be considered acceptable. Relevant Customer Use Case of similar complexity will also be considered.
179	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.6 Code Review Tool	193	General for Sizing purpose	How Many Number of Developers going to use this Tool		User count for the Code Review Tool is indicative for sizing; bidders shall quote the minimum available user license and ensure scalability.
180	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 1	204 of 361	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. **Suggested Clause:** **The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM,**		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
181	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 2	204 of 361	Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	The proposed sizing appears to be misaligned with the other specified requirements like throughput which is only 1 Gbps scalable to 10 Gbps. 40G port will increase the size and overall cost of the solution. Hence, we request technical team to streamline sizing as per the requirement. **Suggested Clause :**		Already answered in S.No. 55
182	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 3	204 of 361	System should have scalable inspection throughput of 5 Gbps scalable to 10 Gbps without additional hardware.	This clause is ambiguous as there are different throughput is asked. Generally DDoS Solution are sized on the basis of mitigation throughput and Legitimate throughput. Hence we recommend to amend the clause accordingly for ease of sizing. **Suggested Clause :** **System should have scalable mitigation throughput of 10 Gbps scalable to 20 Gbps without additional**		Already answered in S.No. 55
183	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 6	204 of 361	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. **Suggested Clause :** **SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card.**		Already answered in S.No. 55
184	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability (Point 38)	241	The solution should support multi-tenancy functionality, including dedicated RAM, CPU cores, independent reboot and upgrades and most important, predictable performance.	Point 38: Dedicated RAM and Core can be allocated on multi-tenant feature. Please specify the virtual tenant amount. further any upgrade to the base appliance will need a reboot of that entire appliance. Please clarify this reboot point. Further what is meant by "predictable performance."		Independent reboot and upgrade refers to the ability to restart or upgrade tenant-specific services and to support rolling or non-disruptive platform upgrades. Along with no noisy-neighbour effect. Predictable performance means

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
185	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	Is a Firewall management needed? If so, would an on-prem solution or a Cloud solution be considered? If On-prem, will the necessary provisions be provided?		Firewall shall be supplied, installed, and commissioned by the MSI at the GoSL' provided on-premises Data Centre. Standard data centre facilities, including rack space, power, cooling, and network connectivity required for installation will be provided by GoSL provided DC
186	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	IPSec is required, what are the connections that will be utilizing this feature and the speed of these links as well as the connection method (fiber/Copper).		IPsec shall be used for secure site-to-site and external connectivity; link speeds and media (fiber/copper) shall be as per bidder's design, meeting RFP throughput requirements.
187	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	One RFP point states all on 3.4 that all Servers and network devices should have 25Gbps or higher, but 10G interfaces are requested from the spec sheet. Which should we consider?		Reference page not found.
188	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	Do the switches need to be a DC fabric or Enterprise solution?		MSI may propose Data Centre–class or Enterprise-class switches, provided the proposed solution meets all performance, resiliency, scalability, and feature requirements specified in the RFP and is suitable for continuous
189	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	What should be the Switching Capacity of the Switches?		MSI shall design the solution and propose appropriate specification for switching capacity which shall support all ports at full line rate for East–West and North–South traffic
190	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	Are there a Dynamic Routing requirement on Switch level and what are they?		Switches must support industry-standard dynamic routing protocols
191	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	How many devices are needed for the solution?		MSI to design the solution and meet the High Availability requirements.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
192	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	How many Ports are required of the following for each of the switches in the infrastructure 1G Base-T 10G Base-T 1G Base-SX/LX 10G Base-SX/LX 25G Base-SX/LX 40G Base-SX/LX 50G Base-SX/LX 100G Base-SX/LX 400G Base-SX/LX		MSI to design the solution
193	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	Is a Switch management needed? If so, would an on-prem solution or an Cloud solution be considered? If On-prem, will the necessary provisions be provided?		Already answered in S.No. 185
194	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	What will be the distance from each connecting device with respect to the Switches? (ie; Servers, Firewalls, Rack Switches)		MSI to design the solution
195	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17 Internal Firewall (Next-Gen) with High Availability	238	General for Internal Firewall	What is the power consideration for all Network devices (Switches/Routers/Firewalls)? AC or DC power?		MSI to design the solution
196	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 1	242 of 361	The solution must be appliance based.	Appliance should be dedicated only, there should not have any option to import 3rd party OS on same hardware. **Suggested Clause:** **Application Delivery Controller shall be purpose built dedicated hardware appliance, there should not have any option to run 3rd party OS on same appliance**		The clause remains unchanged.
197	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 9	242 of 361	Should have a minimum set of rules defined to prevent OWASP Top 10 and SANS Top 25 attacks in default configuration	Every OEM has its own way of Handle OWASP TOP10/SANS 25 Attacks. Hence, we request to generalize the clause. **Suggested Clause:** **Should have rules to prevent OWASP Top 10 and SANS Top 25 attacks.**		The clause remains unchanged.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
198	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 10	242 of 361	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	Solution can be oversized when considering the solution scalability. We request technical team to lower down the requirement a little to accommodate the solution. **Suggested Clause:** **Throughput minimum 30 Gbps from day 1 with scalability to upto 90Gbps without changing the hardware appliance**		Already answered in S.No. 46
199	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 12	243 of 361	SSL transaction 10,000 CPS/TPS	From the provided specifications, it appears that support for ECC (Elliptic Curve Cryptography) and the TLS 1.3 protocol is currently missing. Modern applications increasingly rely on ECC for its lightweight performance and strong security, along with TLS 1.3 for enhanced privacy and reduced handshake latency. These are now considered best practices in securing web communications. We strongly recommend including support for ECC and TLS 1.3 in the specifications to ensure future readiness and compliance with modern security standards.		Revised specification: WAF shall handle 10,000 SSL CPS/TPS and support TLS 1.3 with ECC.
200	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 14	243 of 361	Network interface ports – 24, 4*40Gbps and	Network interfaces requirement is not clear, may be some typo. Additional 40 Gbps is an over kill. Hence, request to amend this. **Suggested Clause:** **Network interface ports - 24*10 Gbps port (without use of breakout cables)**		It is clarified that 24×10Gbps network ports for server/storage connectivity, with 4×40Gbps uplinks for aggregation or high-speed connectivity. MSI may propose equivalent designs that meet the overall throughput, scalability, and performance requirements of the
201	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 15	243 of 361	SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. **Suggested Clause:** **SSL throughput 10 Gbps scalable to 20Gbps.**		Already answered in S.no. 47
202	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 18	243 of 361	Internet link connections supported by load balancer – 8191	We are talking about WAF here, so link doesn't not make sense. We request to add more related terms for reference to generalize the clause. **Suggested Clause :** **Internet link connections/backend Nodes/real servers supported by load balancer – 8191**		The clause should be read as "For a projected peak concurrency of 7,500 users, the WAF / load balancer shall support a minimum of 100,000 concurrent HTTPS connections, inclusive of security inspection and session persistence.". Refer Annexure 5 - Demand

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
203	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 22	243 of 361	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. **Suggested Clause :** **Compliance Certificates – RoHS, Compliant EU, EN 60950-1, KCC, TUV FCC etc**		Already answered in S.No. 48
204	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 31	244 of 361	Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client- side malware.	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause:** **Proposed WAF Solution should Identify and limit / block suspicious clients, BOT Traffic**		Agreed.
205	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 33	244 of 361	Should provide encryption for user input fields to protect from browser-based malwares stealing users credentials	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause :** **Should support encrypted session between user and WAF (to protect against any data hijacking in transit) and should have provision to select between encrypted or decrypted traffic between WAF and**		Agreed.
206	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 34	244 of 361	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time	Every OEM has its own way of Handling Attack packet.Hence, we request to generalize the clause. **Suggested Clause:** **On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses or block the TCP session or block the application user, or block the IP address. For particularly destructive**		The clause remains unchanged.
207	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 1	115 of 361	Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax and include more SLB based requirements : **Suggested Clause :** **Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, L4/L7 content routing, Script**		The clause remains unchanged.However, MSI may propose SLB with additional features such as script-based health checks, cluster-based health checks, user-written scripts, and high availability mechanisms to enhance performance and reliability

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
208	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 11	116 of 361	Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. **Suggested Clause :** **Solution should have VLAN Support.**		Already answered in S.No. 49
209	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 12	116 of 361	Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : **Suggested Clause :**		Already answered in S.No. 50
210	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 14	116 of 361	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. **Suggested Clause:** **The solution should supports the following load balancing methods:** **a. Round-Robin** **b. Weighted Round-Robin** **c. Least Connections**		Already answered in S.No. 51
211	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 15	116 of 361	Solutions should provide application & server health checks for well-known protocols like ICMP, TCP, TCP_ECHO, HTTP, HTTPS etc.	TCP_Echo is not the primary health check setting. Rather the solution should support Script Based Health check and Logical Expresssion Based Health check for Combining multiple rules. **Suggested Clause:** **The proposed solution should supports the following health check types:** **• Link Health Checks,** **• TCP Health Checks,** **• UDP Health Checks,** **• ICMP Health Checks,** **• HTTP/S Health Checks,** **• TCP and UDP-based DNS Health Checks,** **• WAP Gateway Health Checks,** **• Virtual Wire Health Checks,**		It is clarified in regards to Health Check Requirements: The solution must support monitoring of servers and applications using: Standard protocol checks such as : TCP, UDP, ICMP, HTTP/HTTPS, DNS Advanced checks: WAP Gateway, Virtual Wire, DSSP, Cluster-based health checks Flexible custom checks: Script-Based and Logical Expression-Based health checks to combine multiple rules The solution should allow configurable primary and secondary health check mechanisms to ensure accurate
212	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.19 (Point 03)	245	The solution should deliver a sustained throughput of at least as follows: Minimum 30 Gbps with 8x1Gbps and 8X10Gbps and 4 x 100G interfaces at the Public Zone Minimum 50 Gbps with 8x10G and 8X100G interfaces at MZ and DMZ Zone	Request customer to provide the clarity on overall Throughput required considering multiple zones and the number of 1G, 10G and 100G interface required?		The exact distribution of throughput across multiple zones, and the low-level interface utilization, is a design/implementation detail that will be finalized during the solution design phase. MSI

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
213	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.19 (Point 23)	247	the ability to create custom intrusion policies; the ability to detect sensitive data such as identity number or credit card or personal information in ASCII text;	This function is part of DLP and not IPS. Dedicated and purpose built in IPS solution will focus on threat detection / mitigation including zero day attacks,		MSI are required to propose solutions that provide: Threat detection and mitigation, including zero-day attacks The ability to create custom intrusion policies
214	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.26	275	General for Sizing purpose - NDR	NDR Solution should cover for How Many Sandboxes, Mail Users, and Traffic Throughput between NDR Server and Switch Span port		MSI are expected to propose scalable solutions that meet the stated performance and functional requirements and specifications as mentioned in the RFP Annexure 3 - Minimum Tech Requirement
215	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.3.3.10,3.4.3.8	53197	General for IAM and API Gateway	For the database, will you be providing it? If yes, what database will be used?		MSI will propose the database
216	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.3.3.10,3.4.3.8	53197	General for IAM and API Gateway	What is the total number of users for IAM ?		Refer Annexure 5 - Demand Capacity
217	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.3.3.10,3.4.3.8	53197	General for IAM and API Gateway	How many monthly active users are expected for IAM?		Refer Annexure 5 - Demand Capacity
218	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.3.3.10,3.4.3.8	53197	General for IAM and API Gateway	How many concurrent users are expected for IAM?		Refer Annexure 5 - Demand Capacity
219	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.1	169	General for DLP	Do we need to protect Database . If yes what is the Database solution.		Yes. MSI to propose the Database.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
220	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.1 (Point 19)	171	The solution should be able to monitor FTP traffic.	Do we need to protect Network traffic (data in motion)		Yes
221	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	Total Number of IP enabled devices		Refer RFP Volume 02 of 03 : 7 Schedule of Requirements
222	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	IP Enabled devices per location (eg-: HO, NOC,)		Refer RFP Volume 02 of 03 : 7 Schedule of Requirements
223	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	Do You have DR site? If yes, is DC and DR active at the same time? How is DC & DR network structure?		Already answered in S.No. 151
224	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	Details of L2/L3 device Count including all sites? (Switch, routers, Firewall & other L3 devices)---Kindly share the vendor details.		MSI to design the solution as per RFP requirement.
225	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	WLAN device count (WLC & WAP)		MSI to design the solution as per RFP requirement.
226	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	Are all the switches manageable? Please provide complete details with OEM		MSI to design the solution as per RFP requirement.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
227	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	Advance level integration for on- premises VA, ATD , SIEM , ePO, EMM/MDM or any in-house develop application integration like ticketing system?----Yes/No, also share the details of Vendors for each		MSI to design the solution as per RFP requirement.
228	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	HA or Non-HA solution between DC/DR?		MSI to design the solution as per RFP requirement.
229	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC IT Devices	VM or Forescout Hardware required?		MSI to design the solution as per RFP requirement.
230	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Is virtual an option? We can offer both hardware and virtualized components based on the requirements.		Query not clear
231	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What does the architecture look like? Is a network diagram available?		Query not clear
232	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Based on the diagram, what is the optimal location to place a sensor(s) to gain visibility into the OT traffic?		Query not clear
233	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What types of switches are in the OT environment?		Query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
234	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Basically, we want to make sure they have SPAN or port mirroring capabilities and capacity; otherwise, a network tap may be needed		Query not clear
235	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Can the SPAN traffic be filtered to only include the OT traffic?		Query not clear
236	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	How many switches need to be SPAN'd to capture all of the OT traffic?		Query not clear
237	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What is the anticipated throughput that you would expect the sensor to see (based on what is in the SPAN)?		Query not clear
238	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What are the network ranges that make up the OT environment(s)?		Query not clear
239	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What media is needed for the connection to the sensor(s) and the Command Center? (as in copper or fiber)		Query not clear
240	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What is the expected connection speed (10/100/1000/10Gb) for the sensor(s) and Command Center?		Query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
241	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	How many interfaces will be needed on the monitoring sensor?		Query not clear
242	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Are there any traffic aggregation solutions that are part of this? (Gigamon, Ixia, etc. – which will help us answer how many interfaces would be needed, etc.)		Query not clear
243	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	How many sites will be in scope?		Query not clear
244	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Can you provide an estimate of the number of assets we would be expected to see?		Query not clear
245	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Who are the automation vendors in use that the site? (Siemens, ABB, Honeywell, GE, etc.)		Query not clear
246	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	What protocols are in the environment?		Query not clear
247	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Is active monitoring required for this implementation?		Query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
248	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.19	117	General for NAC OT Devices	Are there any requirements for integration, such as with a SIEM?		MSI to design as per RFP requirement.
249	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.12 (Point 43)	220	The solution should be able to integrate with databases including but not limited to MSSQL, MySQL, HBase, etc	We can path all mentioned databases except HBase. We need the expectation because it mentioned as "Intergration" and not as patching.		Clause is self explainatory
250	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.12 (Point 63)	222	Monitor the status of the clients reporting to Patch Management Solution. All aspects of Installation, De-installation,Configuration, Reconfiguration, relocation, enhancements, updates, upgrades, bug fixes, problem analysis, performance analysis, audits, on - site as well	Need More eleboration/explanation		Clause is self explainatory
251	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.12	216	General for Patch Management Solution	We need following information for the licensing. Number of Technicians/Servers/Workstations/Network Devices		The Bill of Materials (BOM) and detailed device counts will be proposed by the MSI as part of the solution design. Licensing for the Patch Management Solution should be sized to meet the functional,
252	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.11 (Point 03)	160	The proposed helpdesk solution must provide seamless integration to log incident automatically via system and network management.	Need further information on the integration to what solution to be integrated. Solution support direct integrations as well as REST API integrations		The Helpdesk solution must support automatic incident creation via standard integrations (out-of-box such as webhooks, and event ingestion and REST APIs) with system, network, and security management tools;
253	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.11 (Point 11)	161	The proposed helpdesk solution must integrate with EMS event management and support automatic problem registration, based on predefined policies	Need further information on the integration to what solution to be integrated. Solution support direct integrations as well as REST API integrations		Already answered in S.No. 252
254	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.11 (Point 10)	211	The proposed SIEM solution must be fully integrated with the central repository of logs data without the need to duplicate the collected raw logs and the searchable data is for 180 days (6 months)	RFP is mentioned that they require a Hot storage for 180 days but it's NOT mentioned any cold storage for all the logs. Assume that Cold storage is not a requirement.		The SIEM must support one year of searchable log retention and permanent archival thereafter

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
255	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.1 (Poin	171	The solution should support the recovery of the password for a remote user.	Need More Elaboration on this Point		The solution shall support secure password reset (not retrieval) for remote users using MFA or equivalent identity verification, with full audit logging
256	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.25	274	General Sizing Related	Number of Hosts need to Scan		MSI to propose the solution as per the RFP and accordingly NMS should be sized.
257	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.3 (Poin	184	The solution should have the ability to start a terminal connection and launch using a single line and include 2FA for access.	Need More Elaboration on this Point		Clause is self explainatory
258	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.6	193-194	General Sizing Related	Number of Contributed Developers		MSI to size the solution as per the RFP requirement
259	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.8	197	General Sizing Related	This requirement for IAM and MFA can be fulfilled with a single solution — **miniOrange** 1. Where the organization users exist? (Ex: any application database/ LDAP or AD directory) 2. Does your organization have an SMS Gateway or Email Gateway available? 3. **Explain point 14 of IAM**: Monitoring: Support for SNMP protocol for real time monitoring		Query not clear
260	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.11	210	General Sizing Related	1) How many offline/archive days of logs are required? (Answer in Days) 2) Do you require 8x5 or 24x7 support? 3) Do you Have IBM OS/Servers (AS 400)? How many LPAR? 4) Are there any custom in-house applications that needs to be monitored?		1) already answered in S.No. 255 2-6) Query not clear
261	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.14	230	General Sizing Related	Please fill the additional Reqirment Gathering sheet		Query not clear

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
262	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.17	240	Firewall should have 8*10Gbps SFP integrated data ports, 8 x 100Gbps ports. Fiber interfaces should be populated with multi-mode transceiver modules.	1)Is that 8 * 100G port necessary propsed firewall include 6 * 100G? If that Aaggregrating 40G couple and 2 * 10G to complete remaining 2 * 100G is okay?		The clause remains unchanged.
263	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.11	160	General Sizing Related	1.How many technicians and IT assets will be onboarded? (ITSM and CMDB are licensed separately but accessible via a unified console; licenses are depended on no of technicians and number of assets.) 2.Are there any NMS or third-party systems that need to integrate with the ITSM platform? If yes, which vendors?		MSI to size the solution as per the RFP requirement
264	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.7	134	General Sizing Related	1) Number of Virtual Machines with containers, including CI/CD build nodes 2) Number of Container images in registries 3) Number of serverless containers 4) Number of hosts for FIM		MSI to size the solution as per the RFP requirement
265	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.24	261	General Sizing Related	1) Number of Web Apps/URLs 2) Number of locally hosted Web Apps and number of public Web Apps		Please refer to SL-UDI-Volume-02-of-03-Annexure-11-Overview-of-Technology and SL-UDI-Volume-02-of-03
266	SL-UDI-Vol-2-of-Vol-3;	Section 7: It	160	SBI 2.0 – FTM supported security	As SBI 2.0 FTM-certified devices are currently limited in availability, we propose the use of an SBI 1.0 compliant device that supports all required biometric capture and integration functionalities. This alternative ensures operational compatibility with the MOSIP platform while		SBI 1.0 and above is acceptable
267	SL-UDI-Volume-02-of-03	Annexure-3;	317 & 320				NA
268	SL-UDI-Volume-02-of-03	Annexure-3;	304	3 Size Should be able to accommodate items in	As we understand that multiple devices within the field infrastructure fall under the scope of GoSL; therefore, detailed information regarding each device is required so that we can design the rugged carry bag accordingly.		Exsiting devices with GoSL. MSI to assess the compatibility of these devices with MOSIP required compliances : 1. Finger Print Scanner - Kojak, KJ220DA-EOO. 2. Signature Pad - Kojak, KJ220DA-EOO Signotec, Gamma 3. Finger Print Auth Scanner - Signotec, Gamma 4. Dual Display Monitor - Eizo,

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
269	SL-UDI-Vol-2-of-Vol-3;		60 & 160	1. Desktop PC and other components GoSL 71. L	Field infrastructure scope on page 60 mentioned that Desktops in GoSL scope. Whereas schedule of requirement mentions Laptops in MSI scope.		MSI scope
270	SL-UDI-Volume-02-of-03-Annexure-3; 3.5.2.7	Section 5.3:	324	• Resolution - 600 x 600 dpi • Paper Size - A4 • PP	Ink Tank printers are not suitable for mobile registration kits as they are bulky & it is also not suitable for transportatiion as inkTank would spill Can this changed to Thermal Receipt printer?		Agreed. Please refer to specification of Thermal printers in revised annexure 3 .
271	SL-UDI-Volume-02-of-03	Annexure-3	328	Safe storage of keys using HSM FIPS 140-2 Level	There are hardly 3000 units of devices to be managed. setting up a dedicated device management server with HSM would be exorbitantly high. Can device provider host the server outside Sri Lanka? Can it be a shared set-up with oher MOSIP implementingg countries? The Partition & channeling would be separate &		No
272	SL-UDI-Vol-2-of-Vol-3;	Section 7: It	160	81. UPS 40	Requirement of UPS will be bulky for Mobile registration kits. it will affect the Mobility. Can a heavy duty battter y of +50,000 MAH can be used to		Agreed.
273	SL-UDI-Volume-02-of-03	Annexure-3	300	7 Ports: Two x USB 3.2 Port One x USB 2.0 One x	Is it acceptable to meet the VGA port requirement using an HDMI to VGA adapter? Lately VGA port is obsolete with major laptop brands		Agreed
274	SL-UDI-Volume-02-of-03	Annexure-3	300	Battery Minimum 4 Cell lithium-ion or lithium po	Mostly Laptops have 5-6 hourss of battery back-up. Can the 10 hours be relaxed. Also these kits are part of Field infrastructure where stable power supply would be		5 to 6 hours of battery backup is acceptable
275	SL-UDI-Volume-02-of-03	Annexure-3	310	Speaker requirement Memory Card Supported u	Can Speaker with BT based connection be accepted? Speakers with SD cards are obsolete now		No change
276	SL-UDI-Volume-02-of-03	Annexure-3	304	1 Material High-Quality Fibre	Is 'High-Quality Fibre' a mandatory material specification, or are alternatives like ABS or PP also permissible under the tender?		Agreed
277	SL-UDI-Volume-02-of-03	Annexure-3	305	Water resistant	Is water resistance a mandatory requirement for the internet dongle as per the tender specifications? The dongle would be part of the kit		Dongles are to provided by GoSL
278	SL-UDI-Volume-02-of-03	Annexure-3	321	Laptop: - Processor: Latest Generation, min 2 GH	Laptops with HDD are obsolete now. Is it acceptable to meet the storage requirement with a 512 GB SSD alone, or is the inclusion of a 1 TB HDD mandatory under the tender		No change
279	SL-UDI-Volume-02-of-03	Annexure-3	318	Operating Temperature* 0 to °50 C	Considering standard webcams do not typically carry official operating temperature ratings, is this acceptable under the tender requirement?		Refer to MOSIP website for latest values.
280		General			Request NISG to provide the confirmation on Number of required environments (Dev/QA/UAT/Pre-prod/Prod)?		Please refer to Annexure 02 of 03 section 5.2.2 Hosting
281		General			Can we have the remote access from Intra country for accessing servers.		Access to servers from intra country i.e., Sri Lanka would be policy driven. Devices accessing the servers would be whitelisted

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
282		General			Please suggest do we need to comply with any firewall, IPS, or proxy rules ?		Yes. These will be defined and detailed at the time of
283		General			Please confirm whether we need to comply with any country-specific NID requirements or GDPR guidelines.		Yes. Personal Data Protection Act (PDPA) – Sri Lanka
284		General			We request to NISG to provide relevant details for data migration. Please confirm how many existing records are available in gallery. Please also confirm which all		Already answered in S.No. 111
285		General			Please confirm whether we need to consider the existing schema of the running application as it is currently developed into new MOSIP platform or we will develop		Already answered in S.No. 111
286		General			Please confirm the existing server count and configuration if we need to use the same existing infrastructure.Are these servers are rack or blade servers ?		Already answered in S.No. 111. MSI has to procure, supply, commission and test all IT infra
287		General			Please confirm what format ISO standards existing biometric data has been captured. Should we use the existing data or will do the new enrolment for existing		Already answered in S.No. 113
288		General			How many enrolments kits are available on site and how the new implementation will cover the device		Refer to Volume 02 of 3: Section 07
289	Volume 2	5	20	The MSI should understand the existing data vol	We request to NISG to provide relevant details for data migration. Please confirm how many existing records are available in gallery. Please also confirm which all		Already answered in S.No. 284
290	Annexure 5	5.1.2.	3	5.1.2. Registration Statics Information	The registration number is **16,851,019,**so the data migration needs to be done for these many users ,please confirm,Do you any specific timeline for this migration out		Already answered in S.No. 211
291	Annexure 5	5.1.2.	3	5.1.2. Registration Statics Information	The registration number is **16,851,019,**so for this many registartion,you already have the demographic and		Already answered in S.No. 290
292	Anenxure 1 A	1.3	10	Physical Layout of DC and DR of DRP	Please confirm that in the new proposed solution will use also utilize the same components (servers.switches,storage,etc) as indicated in the Physical Layout of DC & DR of DRP,if yes the configuartions		SLUDI will be implemented in GoSL provided DC and DRC. Already answered in S.No. 111
293	Annexure-3	3.4.1.9	6	Internet Router	As per the technical specifications, the Internet Router configuration appears to be similar to that of the Core Router, which seems to be on the higher side. Kindly		Refer Amended RFP : Annexure 3 : Minimum Tech requirement
294	Annexure-3	3.4.1.9	6	MPLS Router	As per the RFP, a Core Router has already been requested from the MSI; however, the MPLS Router is also specified with same high-end specifications. Considering that only two types of traffic will enter the DC—one from MPLS and the other from the Internet—please clarify the specific role		Refer Amended RFP : Annexure 3 : Minimum Tech requirement
295	Annexure-3	3.4.1.10	98	Network: Core Switches - LAN	As per the RFP, a Leaf-Spine architecture has been specified, and separate specifications for the Spine Switch are provided in Section 3.4.1.14 of Annexure-3. However, the requirement for a Core Switch (LAN) is also mentioned. Kindly clarify the intended role and purpose of the Core		Refer Amended RFP : Annexure 3 : Minimum Tech requirement
296	Annexure-3		6	Line Item 35 & 49 Data Centre Access Switch (Sec	As per Annexure-3, Section 3.4.1.1 mentions both the Blade Server and the Data Centre Access Switch; however, the specifications provided pertain only to the Blade Server. Kindly confirm which section the MSI should refer		Refer Amended RFP : Annexure 3 : Minimum Tech requirement

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
297	Annexure-3		6	Line item 46 Application Load Controller (Server / Application Load Balancer) (Section 3.4.1.14 and 3.4.1.13)	As per Annexure-3, line item **46 — Application Load Controller (Server / Application Load Balancer**) — has been mapped to **Sections 3.4.1.14 and 3.4.1.13**. However, these sections pertain to the **DC Software Defined Networking (SDN) Fabric Architecture and the Data Centre Spine Switch.** Kindly confirm the correct section that the MSI should refer to.		Refer Amended RFP : Annexure 3 : Minimum Tech requirement
298	Annexure-3		6	Line item 45 - Global Load Balancer (Section 3.4.1.14)	As per Annexure-3, Line Item **45 (Global Load Balancer) is mapped to Section 3.4.1.14**; however, the specifications for the Global Load Balancer are provided in **Section**		Refer Amended RFP : Annexure 3 : Minimum Tech requirement
299	Volume-2			General Query	As per the RFP, both Tape Library and VTL have been specified. Since Tape Library technology is considered outdated, we request that the Tape Library requirement		VTL is dropped and refer Amended RFP.
300	Annexure-3	3.4.1.17 Ser	115		There is currently insufficient clarity regarding the expected traffic requirements. For Example: "The proposed solution must handle high-capacity traffic, including L7 requests per second: 450K L4 connections per second:150K		Already answered in S.No. 427
301	Annexure-3	3.4.1.18 Glo	116-117	General Query	Clarity required on the number of expected DNS Request per second, which would help in sizing the appliacne		Already answered in S.No. 428
302	Annexure-3	3.4.1.18 Glo	116-117		"Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS and Must support resolution for A,		Already answered in S.No. 429
303	Annexure-3	3.4.3.15 SSL	232	Support for VRRP, QoS and full OSPF routing protocol.	Please change it to as per the below mentioned as VRRP is gateway redundancy protocol and OSPF is a routing protocol.		Already answered in S.No. 430
304	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	242	11. RAM 64 GB	To support 30 Gbps throughput, while preventing OWASP Top 10 and SANS Top 25 attacks, significant memory is required for packet inspection, state tracking, and rule processing. 64 GB RAM may cause bottlenecks under high traffic or attack scenarios. At least 128 GB RAM is essential to ensure performance, scalability, and reliable threat prevention.		Already answered in S.No. 431
305	Annexure-3	3.4.3.18 Web Application Firewall (WAF) with High Availability	243	14. NETOWRK INTERFACE PORTS 24, 4*40	Clarity required. In a modern spine-leaf network, the emphasis is on high-speed links (e.g., 10/25/40/ Gbps) rather than a large number of ports. Efficient interconnections with aggregated uplinks reduce the need for devices with 24 ports. The architecture uses fewer, faster ports for scalability and performance, making excessive port counts unnecessary. **It should have**		The requirement for “24, 4×40” ports is indicative, not strict. A modern port mix with higher-speed interfaces (such as 25G/100G uplinks) that meets or exceeds the switching capacity and performance requirements is acceptable.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
306	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	5. Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	The requirement for a fixed latency of <75 microseconds should be reconsidered, as latency is influenced by multiple factors beyond the hardware's capabilities, including network topology, connection quality, external routing, and environmental conditions		Already answered in S.No. 55
307	Annexure-3	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability	204	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	Please change it to "SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 7000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key from day 1 and scalable upto 15K TPS."		Already answered in S.No. 55
308	Annexure-3	3.3.3.10 API	53	The proposed solution shall provide API Lifecycle maintenance capabilities including definition, creation, security, monitoring and	Please change it to "The proposed solution shall provide API Lifecycle maintenance capabilities including definition, security monitoring and management."		The condition remains
309	Annexure-3	3.3.3.10 API	53	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.	Please change it to **"The proposed solution shall have the capability to externalise APIs and should provide cataloguing capabilities with third party integrations."** because API cataloguing is not inherently a primary function of API gateway servers, as the core purpose of an API gateway is to manage, secure, and route API traffic. Their primary responsibility is to act as a central access point for APIs, handling authentication, load balancing, rate limiting, and request/response management. For advanced cataloguing capabilities such as detailed documentation, taxonomy management, or developer		Yes Agreed
310	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking Clause C	3 of 361	In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave of Forrester Wave or Major Players in IDC MarketScape.	**This is an ambiguous clause for Web Application Firewall Solution. Being a technology leading OEM for Web application Firewall, we seek some clarifications.** **It is important to note that recent third-party reports on Web Application Firewalls (WAF) now include a broader range of solutions, such as cloud-based services (WAAP-as-a-Service) OEMs in addition to traditional hardware OEMs.** **However, since the current requirement specifically pertains to hardware-based solutions, please clarify whether, for the purpose of evaluating the 4 distinct**		Already answered in S.No. 177

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
311	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.2 Product Benchmarking Clause E	4 of 361	In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in	**Regarding the Load Balancer (ADC) category, we would like to clarify that the most recent Gartner report available was published in 2016. Additionally, there are currently no relevant reports available from IDC or Forrester for this category.** **In light of this, kindly advise whether:** **1. We may submit a relevant customer use case instead, or** **2. The 2016 Gartner report can still be considered valid**		Already answered in S.No. 178
312	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 1	204 of 361	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. **Suggested Clause:** **The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM,**		Already answered in S.No. 55
313	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 2	204 of 361	Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	The proposed sizing appears to be misaligned with the other specified requirements like throughput which is only 1 Gbps scalable to 10 Gbps. 40G port will increase the size and overall cost of the solution. Hence, we request technical team to streamline sizing as per the requirement. **Suggested Clause :** **Should have 4X10Gbps (Populated with SR) and 8 X 1 Gbps copper with internal bypass Interfaces.**		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
314	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 3	204 of 361	System should have scalable inspection throughput of 5 Gbps scalable to 10 Gbps without additional hardware.	This clause is ambiguous as there are different throughput is asked. Generally DDoS Solution are sized on the basis of mitigation throughput and Legitimate throughput. Hence we recommend to amend the clause accordingly for ease of sizing. **Suggested Clause :** **System should have scalable mitigation throughput of 10 Gbps scalable to 20 Gbps without additional hardware.**		Already answered in S.No. 55
315	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 6	204 of 361	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. **Suggested Clause :** **SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card.**		Already answered in S.No. 55
316	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		New Clause	**Proposed Appliance should use real-time-signature creation technology to protect against DNS based DDoS Attack which should include but not limited to Packet Checksum, DNS FQDN, DNS Domain Name, Source IP address, Packet Size, DNS Query ID, DNS Query Count (Qcount), Port numbers, Destination IP address.**		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
317	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		New Clause	**The proposed solution should have Geo Fencing/Geo Blocking to block the traffic or allow the traffic from specific Geo Location.** **Geo Fencing should also support Threshold based blocking based on configure PPS or Kbps value, to determine the rate of permitted traffic from the selected geolocations. Once any of the thresholds is reached, all traffic from the specified geolocations is blocked until it drops below the configured thresholds.**		Already answered in S.No. 55
318	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability		New Clause	**The proposed appliance should support Integration with OEM owned Cloud based Scrubbing Centers, in case of Bandwidth Saturation attacks, using the same technology, in case it is required by department with additional license.** **OEM Should have atleast once Cloud Scrubbing Centre in SAARC for reduced Latency with minimum capacity of 15 Tbps.**		Already answered in S.No. 55
319	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 1	242 of 361	The solution must be appliance based.	Appliance should be dedicated only, there should not have any option to import 3rd party OS on same hardware. **Suggested Clause:** **Application Delivery Controller shall be purpose built dedicated hardware appliance, there should not have any option to run 3rd party OS on same appliance**		Already answered in S.No. 196

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
320	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 9	242 of 361	Should have a minimum set of rules defined to prevent OWASP Top 10 and SANS Top 25 attacks in default configuration	Every OEM has its own way of Handle OWASP TOP10/SANS 25 Attacks. Hence, we request to generalize the clause. **Suggested Clause:** **Should have rules to prevent OWASP Top 10 and SANS Top 25 attacks.**		Already answered in S.No. 197
321	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 10	242 of 361	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	Solution can be oversized when considering the solution scalability. We request technical team to lower down the requirement a little to accommodate the solution. **Suggested Clause:** **Throughput minimum 30 Gbps from day 1 with scalability to upto 90Gbps without changing the hardware appliance**		Already answered in S.No. 46
322	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 12	243 of 361	SSL transaction 10,000 CPS/TPS	From the provided specifications, it appears that support for ECC (Elliptic Curve Cryptography) and the TLS 1.3 protocol is currently missing. Modern applications increasingly rely on ECC for its lightweight performance and strong security, along with TLS 1.3 for enhanced privacy and reduced handshake latency. These are now considered best practices in securing web communications. We strongly recommend including support for ECC and TLS 1.3 in the specifications to ensure future readiness and compliance with modern security standards.		Already answered in S.No. 199

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
323	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 14	243 of 361	Network interface ports – 24, 4*40Gbps and	Network interfaces requirement is not clear, may be some typo. Additional 40 Gbps is an over kill. Hence, request to amend this. **Suggested Clause:** **Network interface ports - 24*10 Gbps port (without use of breakout cables)**		Already answered in S.No. 200
324	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 15	243 of 361	SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. **Suggested Clause:** **SSL throughput 10 Gbps scalable to 20Gbps.**		already answered in S.no. 47
325	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 18	243 of 361	Internet link connections supported by load balancer – 8191	We are talking about WAF here, so link doesn't not make sense. We request to add more related terms for reference to generalize the clause. **Suggested Clause :** **Internet link connections/backend Nodes/real servers supported by load balancer – 8191**		Already answered in S.No. 202

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
326	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 22	243 of 361	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. **Suggested Clause :** **Compliance Certificates – RoHS, Compliant EU, EN 60950-1, KCC, TUV FCC etc**		Already answered in S.No. 48
327	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 31	244 of 361	Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client- side malware.	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause:** **Proposed WAF Solution should Identify and limit / block suspicious clients, BOT Traffic**		Already answered in S.No. 204
328	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 33	244 of 361	Should provide encryption for user input fields to protect from browser-based malwares stealing users credentials	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause :** **Should support encrypted session between user and WAF (to protect against any data hijacking in transit) and should have provision to select between encrypted or decrypted traffic between WAF and backend server.**		Already answered in S.NO. 205

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
329	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 34	244 of 361	On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.	Every OEM has its own way of Handling Attack packet.Hence, we request to generalize the clause. **Suggested Clause:** **On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses or block the TCP session or block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to**		Already answered in S.NO. 206
330	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability	244 of 361	New Clause	**Appliance should support virtualization feature with option to create isolated environment from application and management perspective. 5 Virtual Instance from day1 and scalable upto 30 Virtual Instance** **Each instance should have dedicated: Resource, management, configuration and operating system. There should not have any option to import 3rd party software on same hardware.**		No change
331	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.3.18 Web Application Firewall (WAF) with High Availability	244 of 361	New Clause	**The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No proprietary Protocol).**		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
332	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.17 Server Load Balancer Clause 1	115 of 361	Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax and include more SLB based requirements : **Suggested Clause :** **Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, L4/L7 content routing, Script-Based Health Checks, Cluster-based Health Checks,**		Already answered in S.No. 207
333	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.17 Server Load Balancer Clause 11	116 of 361	Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. **Suggested Clause :** **Solution should have VLAN Support.**		Already answered in S.No. 49
334	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.17 Server Load Balancer Clause 12	116 of 361	Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : **Suggested Clause :** **Should have IPv6 Support for SLB, interfaces, routing.**		Already answered in S.No. 50

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
335	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.17 Server Load Balancer Clause 14	116 of 361	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. **Suggested Clause:** **The solution should supports the following load balancing methods:** **a. Round-Robin** **b. Weighted Round-Robin** **c. Least Connections** **d. Fastest Response**		Already answered in S.No. 51
336	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 15	116 of 361	Solutions should provide application & server health checks for well-known protocols like ICMP, TCP, TCP_ECHO, HTTP, HTTPS etc.	TCP_Echo is not the primary health check setting. Rather the solution should support Script Based Health check and Logical Expresssion Based Health check for Combining multiple rules. **Suggested Clause:** **The proposed solution should supports the following health check types:** **• Link Health Checks,** **• TCP Health Checks,** **• UDP Health Checks,** **• ICMP Health Checks,** **• HTTP/S Health Checks,** **• TCP and UDP-based DNS Health Checks,** **• WAP Gateway Health Checks,** **• Virtual Wire Health Checks,**		Already answered in S.No. 211
337	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer		New Clause	In the specifications for Server Load Balancer, Sizing requiement is missing. Hence, we request technical comiitte to include mising sizing requirement . **Suggested Clause :** **Traffic Ports: 2 x 10 GE Fiber and 8 x 1G Copper from day1. Option for additional 8 x 1 GE Fiber and 8 x1G copper for future use (Break-Out should not be used)** **L4 Throughput: 20 Gbps and scalable upto 40 Gbps** **Layer 4 connection per second: 500,000** **RSA CPS(2K Key): 20,000** **ECC CPS (EC-P256): 12,000 with TLS1.3 Support** **The appliance should have dedicated 2x1G RJ45 Out-of-**		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
338	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer		New Clause	**Virtualization is a very important feature in load balancers enables efficient resource utilization by allowing multiple virtual instances to run on a single physical device, enhancing scalability and flexibility. It also simplifies deployment and management in dynamic, multi-tenant environments covering different applications zones, critical applications, etc.** **VIRTUALIZATION:** 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 **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, **d) Operating System** The proposed device should support 5 Virtual Instance		No change
339	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer		New Clause	**Bidder should propose Centralized Management & Reporting Solution from Day 1.** **Centralized management solution should provide:** **Application Dashboard** **Per Application Analytics** **SLA Breakdown (Network, per server)** **SSL Statistics (handshake and cypher breakdown, rejected handshake)** **SSL CPS** **System Dashboard** **Network Dashboard** **L4 Events**		No change
340	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.17 Server Load Balancer		New Clause	**The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.**		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
341	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.18 Global Load Balancer		New Clause	In the specifications for Server Load Balancer, Sizing requiement is missing. Hence, we request technical comiitte to include mising sizing requirement . **Suggested Clause :** **Traffic Ports: 2 x 10 GE Fiber and 8 x 1G Copper from day1. (Break-Out should not be used)** **L4 Throughput: 6 Gbps and scalable upto 25 Gbps** **Layer 4 connection per second: 500,000** **RSA CPS(2K Key): 20,000**		Already answered in S.No. 337
342	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.18 Global Load Balancer		New Clause	**Virtualization is a very important feature in load balancers enables efficient resource utilization by allowing multiple virtual instances to run on a single physical device, enhancing scalability and flexibility. It also simplifies deployment and management in dynamic, multi-tenant environments covering different applications zones, critical applications, etc.** **VIRTUALIZATION:** 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 **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, **d) Operating System** The proposed device should support 5 Virtual Instance		Already answered in S.No. 338
343	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.18 Global Load Balancer		New Clause	**The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP creation, Node/Real Sever Creation, Farms/Group Creation, SSL Binding etc.**		Already answered in S.No. 340

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
344	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.18 Global Load Balancer		New Clause	**The proposed device should support blelow GSLB Metrics:** **Least Connections** **Round Robin** **Response** **Geographical** **Network** **Availability** **QoS** **Minmisses** **Hash** **Local** **Always** **Remote** **Persistence**		Already answered in S,No. 51
345	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical	3.4.1.18 Global Load Balancer		New Clause	**The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Propertary Protocol).**		Already answered in S.No. 331
346	Annexure-3	3.4.3.5 Web Gateway with High Availability	190	Proposed Web Solution should be an on premise having Proxy, URL filter Caching, SSL Inspection, Anti-Virus, Antimalware, multiple detection engines.	1.Kindly confirm whether the solution is required to be deployed on a physical hardware appliance, or if deployment on a virtual machine is acceptable. In the case of a virtual deployment, will the required infrastructure be provisioned by the SLUDI ? 2. Please confirm if a cloud-based deployment model is acceptable for this solution.		1) The Web Gateway solution with High Availability shall be deployed in the on-premises Data Centre (DC) and Disaster Recovery Centre (DRC). The solution may be implemented using physical appliances or virtual appliances, provided all RFP functional, non-functional, security, performance, and availability requirements are met. The MSI shall be fully responsible for provisioning and licensing all required infrastructure, including
347	Annexure-3	3.4.3.5 Web Gateway with High Availability	190	The Solution should integrate with SIEM, APT solution and the proposed/existing Ticket Management system for proactive detection and incident management.	Which exisiting SIEM/APT/Ticketing system is SLUDI using		New SIEM APT system will be proposed by MSI. GoSL does not have an existing SIEM or APT solution

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
348	Annexure-3	3.4.3.5 Web Gateway with High Availability	191	The solution must support different types of compression algorithms and should be able to scan encoded and compressed files.	Please explain the use of the mentioned clause.		Web Application Gateway/WAF should be able to handle traffic or files that are compressed using various standard compression methods, such as: HTTP/HTTPS level compression;
349	Annexure-3	3.4.3.5 Web Gateway with High Availability	193	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall	These are either encrypted, non-HTTP-based or not inspectable using standard web proxy mechanisms. Kindly confirm if all these are mandatory or flexible based on actual use case.		The solution shall detect and block spyware and malware attempting to connect to external networks beyond standard HTTP/HTTPS traffic. While inspection across multiple ports
350	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking	Page 3 of 361	In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of size, number of transactions, data and users	We understand that in case the OEM whose product is not cited in the Gartner Quadrant / Forrester Wave / IDC MarketScape report will need to submit 1 case study of similar complexity and dimension where the same product is deployed, kindly confirm whether our understanding is correct. Furthermore, we interpret that solutions with comparable complexity and scale—such as those delivered for Telecom, Smart City, Safe City, large enterprise, Government, or PSU projects— shall be considered under this category, Kindly confirm.		Clause is self explainatory
351	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking	Page 3 of 361	The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the	Mandating that the product be in the Leaders Quadrant of Gartner Magic Quadrant, Forrester Wave, or IDC MarketScape significantly restricts competition and may inadvertently exclude technically qualified OEMs whose solutions meet internationally recognized standards. Many capable vendors maintain rigorous certifications such as CMMI Level 3, ISO 27001, ISO 27034, and ISO 9001, demonstrating high-quality processes, robust security practices, and global compliance. Such restrictive criteria could: Reduce the pool of eligible bidders, Increase procurement costs,Limit innovation and technology diversity		No change
352	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking	Page 3 of 361	In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of			No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
353	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2 Product Benchmarking	Page 3 of 361	The Vendor has to mandatorily provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario for	We understand this clause is applicable for the bidder only.		Clause is self explainatory
354	Volume 02 of 03 Two Stage Bidding Procedure	5.11.2.12 Incident Management	Page 132 of 164	b. For IT Service Management, ITIL v3 is the chosen framework and ISO/IEC20000 is the chosen quality standard.	Please confirm our understanding that the latest version of ITIL, i.e., ITIL v4, shall be considered for IT Service Management compliance. Furthermore, ISO/IEC 20000-1 is a certification for a Service Management System (SMS) focused on process quality and continual improvement for trusted service delivery and support processes. Thereby we request that		ITIL v4 shall be considered as the reference framework for IT Service Management compliance. ISO/IEC 20000 certification, if required, shall be applicable to the entity responsible for delivering IT services (e.g., MSI / DC service provider). OEM
355	Volume 02 of 03 Two Stage Bidding Procedure	5.1.3.1 Business Intelligence and Analytics	Page 33 of 164	GoSL is seeking the capability to analyze large quantities of business data, transform the data into intelligence and insight, and deliver this intelligence and insight to the GoSL's processes and users. In a move aimed towards digital economy in Sri Lanka, the GoSL has taken up a Data Analytics and Business Intelligence initiative for SL-UDI Information System. SL-UDI Information System would help increase efficiency and availability of reliable data in a timely manner. GoSL desires to build enterprise-level DA and BI system with definition of Key Performance Indicators (KPIs) for	Request clarification on the expected volumetrics to be considered for optimal estimation, sizing , and solution: 1. Data volume to be considered for the proposed solution, i.e., whether 20TB or 40TB ,100TB or higher, or higher 2. Tentative number of KPIs to be provided as part of the BI 3. Number of data sources to be integrated and type of integration format such as REST API, DB links etc. 4. Number of Reports and Dashboards required 5. Data retention duration.		Please refer to Refer Vol 2 of 3, page 34, point xiii for requirements and volume 02 of 03 : Annexure 03 Minimum tech requirement 3.3.3.5 for specifications
356	Volume 02 of 03 Two Stage Bidding Procedure	5.1.3.1 Busir	Page 33 of 164	The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of Data Analytics and Business Intelligence Solution for SL-UDI Information System. The MSI shall enable the system to provide comprehensive monitoring of enrolment and	Request clarification on the number of data sources to be integrated with the proposed solution, along with details of the integration types or interfaces expected. This information will assist in accurate sizing and architectural planning of the solution.		Already answered in S.No. 355
357	Volume 02 of 03 Two Stage Bidding Procedure	5.1.3.1 Busir	Page 33 of 164	The proposed product should preferably be an open-source solution along with Enterprise support.	We understand that the OEM of the proposed solution shall provide support for any open-source components utilized within their overall solution, as the ownership and responsibility for the complete solution rest with the OEM of the offered product line. Please confirm our		Open Source product should come with enterprise support. License/subscription for any open-source or closed close product shall be in the name of GoSL. MSI shall be responsible

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
358	Volume 02 of 03 Two Stage Bidding Procedure	5.1.3.1 Busir	Page 34 of 164	GoSL shall prescribe reports to be developed which will be identified at requirements stage as well as operations phase.	Request clarification on the expected number of reports required at both the requirements stage and the operational phase to assist the OEM in accurately sizing, estimating and designing the solution.		Clause is self explainatory
359	Volume 02 of 03 Two Stage Bidding Procedure	5.1.3.1 Busir	Page 34 of 164	The Data Analytics system should allow GoSL to customize notification of certain indicator that GoSL is interested in to trigger activities/actions. The Data Analytics module should have a user interface to extract data based on the data required for self-analytics and report generation. The Data Analytics module should also allow for ad-hoc queries	We understand that the total requirement for BI users is five. Kindly also specify the expected number of concurrent application users for accurate solution sizing and capacity planning. Please also confirm the data retention duration.		Please refer to Refer Vol 2 of 3, page 34, point xiii for requirements. Number of Concurrent users may be kept at 5. The data will be retained for one year and thereafter archived. No data will be deleted. This will be done in consultation with GoSL
360	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.9 Enterprise Monitoring system	Page 151 of 361	3.4.2.9 Enterprise Monitoring system	To optimize the sizing and Bill of Materials for the Enterprise Monitoring System, we request you to kindly share the total number of users and concurrent users required for proper capacity planning and proposing the optimal solution. Please also confirm the data retention duration		Refer Annexure 5 - Demand Capacity Planning, Table 5.1.4. For Internal Users No 20% - 30% of the Total Users may be considered for concurrent users. Data will be retained for a period of one year and thereafter
361	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.2.11 IT Service Management	Page 160 of 361	3.4.2.11 IT Service Management	To optimize the sizing and Bill of Materials, we kindly request you to provide the number of end users, number of operators/technicians, and the number of concurrent users for accurate solution sizing and solution BoQ.		Already answered in S.No. 360
362	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	4 Application Performance Management (APM)	Page 145 of 361	The proposed APM platform must support both Linux and Windows flavours for deployment of its core components (such as management server) and should not require any kind of "root access" or "root privilege" to deploy agents in the monitored applications.	Asking for deployment on both Windows and Linux OS restricts participation of capable OEMs, the focus should be to have a soliton that runs on modern open technologies like docker/containers and microservices architecture to ensure scalability, flexibility and performance. Additionally Linux-based operating systems are widely recognized for their robust security architecture and are preferred platforms for most OEM solutions. Considering best practices and to encourage broader		No change

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
363	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	4 Application Performance Management (APM)	Page 150 of 361	The platform should offer automatic Runtime Application Self- Protection (RASP) for modern applications, keeping both users and the digital business secure by detecting vulnerabilities at runtime and defending against attacks to prevent breaches on real time basis without having a need to deploy any extra agent. The module should offer following capabilities around application security: 1. Monitor common vulnerabilities in OWASP Top 10 along with providing the related CVE details of vulnerability detected in application runtime and provide recommendation related to remediation of these vulnerabilities.2. Harvest threat intelligence feeds from multiple sources including open source databases like NIST NVD and other OEM threat feeds assisting team in identifying any potential risks. 3. Flag any risk through API ecosystem and correlate these security context with business transactions through risk score helping team to prioritise and respond to security risks and reduce overall organisational risk profile. 4. Detects and block attacks on near real-time	The features specified in this clause pertain to security & vulnerability assessment solutions typically provided by security OEMs and are not integral to standard NMS/EMS frameworks. Inclusion of this feature may inadvertently Favor a particular OEM and limit broader participation. We request that this clause be removed for wider OEM participation.		No change
364	Volume 02 of 03 Two Stage Bidding Procedure	5.1.4.5 Service Billing System	Page 39 of 164	Generic Query	Please confirm the expected monthly transaction volume, number of services, and record growth (G2C/G2B) to size the system accurately.		Refer Annexure 5 - Demand Capacity Planning
365	Volume 02 of 03 Two Stage Bidding Procedure	5.1.4.5 Service Billing System	Page 39 of 164	Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.	Please specify whether a central service catalogue need otbe propsoed as part ofhte solution . If yes, kindly provide: 1. Specification of catalogue structure 2. Approval workflows		Detailed Requirements to be captured at the stage of implementation
366	Volume 02 of 03 Two Stage Bidding Procedure	5.1.4.5 Service Billing System	Page 39 of 164	Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.	Please confirm whether billing includes: 1. Subscription-based billing 2. Usage-based billing 3. Invoice-based billing		Detailed Requirements to be captured at the stage of implementation

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
367	Volume 02 of 03 Two Stage Bidding Procedure	5.1.4.5 Service Billing System	Page 39 of 164	Generic Query	The RFP states that SBS must integrate with multiple systems (Payment Gateway, SSO, portals, service delivery systems). Kindly provide: 1. List of systems & technology stack where integtrations are required		Detailed Requirements to be captured at the stage of implementation.
368	Volume 02 of 03 Two Stage Bidding Procedure	5.1.4.5 Service Billing System	Page 39 of 164	Generic Query	1. Please confirm the data retention policy: 2. How many years' invoices must be stored? 3. Cold storage vs hot storage requirements 4. Retrieval time expectations for archived invoices		Data will be retained for a period of one year and thereafter archived. No data would be deleted / purged. The data
369	Annexure 3: Minimum Technical Specification	3.4.1.4 Storage: Enterprise Grade Object Storage Solution #	86	Point no. 15. Solution shall consider rack awareness and failure domains while implementing	Please remove this clause **Justification** The object storage rack includes multiple PDUs to ensure redundancy and maintain failure domain isolation. Placing each node in a separate rack would significantly increase the rack footprint and exceed the available rack space requirement		Already answered in S.No. 1
370	Annexure 3: Minimum Technical Specification	3.4.1.4 Storage: Enterprise Grade Object Storage Solution #	86	Point no. 20. Nodes shall be placed with Rack awareness	Please remove this clause **Justification** Object Storage RACK has multiple PDU for redundency and maitin failure domain.		Already answered in S.No. 1
371	Annexure 3: Minimum Technical Specification	3.4.1.5 SAN (Storage Area Network)	87	Point no. 8. The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection	Please change it to "The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% Data availability with built-in redundancy and dynamic drive protection." **Justification** 100% Data Availability ensures that data will be available		Already answered in S.No. 3
372	Annexure 3: Minimum Technical Specification	3.4.1.5 SAN (Storage Area Network)	89	The proposed storage solution should support snapshot capabilities, ensuring efficient data protection and recovery. It must include the necessary software licenses	Please change it to "The proposed storage solution should support snapshot capabilities upto 1000 snapshot per volume, ensuring efficient data protection and recovery. It must include the necessary software licenses" **Justification** Supporting large number of snapshot (up to 1000 per volume) supports finer-grained data recovery, enabling		Already answered in S.No. 4
373	Annexure-3	3.4.3.23	259	The solution must support log collection and retention	What is the duration (in months/years) that logs should be retained?		logs will be retained for a period of one year and thereafter

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
374	Annexure-3	3.4.3.23	256	N/A	What is the number of endpoints to be considered for the solution? Please confirm		Refer RFP Vol 2 of 3, Section 7, Schedule of Requirements - Field Infrastructure. The end point items which need to be integrated are listed there. At the enrolment centers 1612 of each such devices(end points) need to integrated. For Authentication purposes - Authentication - Fingreprints;
375	Annexure-3	3.4.3.15	233	Support hot swappable (1+1) field replaceable redundant power supply and fan module	While field replaceable power supplies are generlly available for the requested VPN gateway spec size, field replaceable fans are included in higher models, which will result in a much higher cost. Therefore, is it mandatory to		No change
376	Annexure-3	3.4.3.15	235	Support for VRRP, QoS and full OSPF routing protocol.	VRRP is an open standard protocol used to provide high availability and fault tolerance for the solution. If the proposed solution includes it's own method to provide high availablity clustering (active/passive, active/active), is		Already answered in S.No. 430
377	Annexure-3	3.4.3.17	241	All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated environment without any need to connect with the Internet.	Threat protection functions such as IPS/vulnerability protection, Antivirus, C&C protection etc., require updates to be received on the firewall through the Internet to provide effective protection. Therefore, Is it acceptable to for the firewall to receive these updates through the Internet?		Clarification - The intent of the requirement is to ensure that threat protection functions do not require direct Internet connectivity from the firewall. Signature and threat intelligence updates may be obtained through controlled and secure mechanisms such as centralized patch management systems or
378	Annexure-3	3.4.3.21	251	Solution should support multitenancy and provide a clear Architecture for function in multitenant environment.	Is it sufficient for the solution to support multitenant environment or should the solution include the required licensing to deploy a multitenant architecture? If licenses are required to be included, please provide		Item is dropped.
379	Annexure-3	3.4.3.21	254	The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.	Please indicate the number of users (analysts) that licensing should be included for with the provided solution. - Number of users will full access (read/write permissions) - Number of users with audit access (read-only		Item is dropped.
380	Annexure-3	3.4.3.21	254	Retaining the data of all multiple runs of SOAR playbooks ensure the retention of key artifacts especially with dynamic information such as	This clause refers to threat reputation information. Would like to know whether or not threat intel licenses should be included with the SOAR platform?		Already answered in S.No. 33
381	Annexure-3	3.4.3.21	254	The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.	What is the required retention period for incidents?		Item is dropped.
382	**Vol-2**	Section VI, Clause 7	156- 162	Table 35: Bill of Material Under Schedule of Requirement	As per our understaing the Bill of Material list contains only the inticative quantities against the Procuct/Service. However, during proposal submission, the bidder may change **(increase /decrease)** the quantities on any product/Service in his Proposal to ensure the		Please refer to Amended RFP Volume 02 of 03. The indicative quantities have been removed.Hence, the bidder is

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
383	**Vol-1**	Section III, Clause 3.1.2.2 (A1.1)	29	A1.1 MOSIP Partnership and Experience A1.1.1 MOSIP Partner System Integrator: Weighage 2%, Technical Marks 20 A 1.1.2 Experience of implementing MOSIP ID Platform: Weighage 2%, Technical Marks 20	We request you to consider that any member of the JV/Consortium must fulfill these Requirement.		Agreed.
384	**Vol-3**	Section VII, Clause 38.1 Insurance	42	To the extent specified in the Appendix to the Contract titled Insurance Requirements, the Contractor shall at its expense take out and maintain in effect, or cause to be taken out and maintained in effect, during the performance of the Contract, the insurances set forth below in the sums and with the deductibles and other conditions specified in the said Appendix. The identity of the insurers and the form of the policies shall be	Please clarify if insurance policy(ies) are to be arranged from Local insurance company in Sri Lanka or We can take policies from Indian Insurance companies. If expected form/format may be advised in advance to bidders.?		
385	**Vol-1**	Section-III, Clause 3.1.2.5, Technical Score Parameter-Criteria D	31	Technical Score Parameter- Criteria D Team Consulting and Staffing	Please clarifiy, (i) whether key personnel has to be of lead bidder/consortium partners (ii) whether they have to be on roll of company or contractual professional can be deployed for project specific requirement. (iii) whether sub contractor's staff can be considered for key personnel for respective scope for the purpose of key personnel.		Subcontractor staff can be considered as key personnel provided evidence is submitted along with the CV in the form of an employment letter . However, short term contractual employees (<=2 year) shall not be
386	Vol-2	Annexure-3, Clause 3.6.1.1 ABIS 31 Miscellaneous	338	a. Should be able to work where segmentation is difficult due to missing Iris. d. Should be able to work where segmentation is difficult due to poor quality Fingerprint, Face and Iris. h. Should be able to deduplicate even with exceptionally low quality of images	If ABIS gets a packet where segmentation is difficult due to missing or exceptionally poor quality of iris, fingerprint or Face, ABIS will be able to work with available modalities assuming correct modality type, sub-type are provided in the biometric packet. Kindly confirm correct position number would be available for each modality in the biometric packet.		Quality threshold are maintained at the enrollment stage. Hence a scenario where ABIS gets a packet where segmnetation is difficult is minimal. Secondly, fusion score thersholds are also set for deduplication. Hence ABIS
387	Vol-2	Annexure-9, Clause 9.5 Service Levels for Biometric Solution	15	**6. Fine tuning of Biometric Solution**: For each instance when fine- tuning is not carried out by the bidder within the specified timeline Severity: 8, or 9 (if breach occurred for two consecutive fine-tunings)	We suggest that fine tuning would be required only in case of deviation of SLAs like Accuracy & performance. As fine tuning is not a continuous process and also it require downtime, we would recommend to keep it as when required instead of monthly basis. Kindly modify the clause accordingly.		If the bidder is not able to meet deduplication SLAs fine tuning would be required. This would have to be done during the planned downtime. It is agreed that this should be done as and when required.
388	Vol-2	Annexure-3, Clause 3.6.1.1 ABIS 12 Verify	333	12. Fingerprint, Iris and Photograph verification utilizing biometric standard compliant templates will be done without use of proprietary extended data.	As on date, Biometric standard compliant template is available only for Fingerprint and there is no standard template defined for Face and Iris. Kindly modify the clause accordingly.		The standard template would mean the standard image for face and IRIS.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
389	Vol-2	Section VI, Clause 5.1.5.1 Setup of Biometric Solution	40	In addition to installing and tuning its own software, **the BSP will also be responsible** for installation and configuration of other software (Anti-virus, enterprise management system, etc.) provided by the MSI. The overall responsibility shall lie with the MSI. In addition to installing and tuning its own software, the BSP will also be support for installation and configuration of other software being provided by the MSI. The indicative list of such software includes: a) Enterprise Management System (EMS) Agent b) Security Information and Event Management (SIEM) Agent c) Anti-Virus d) Data Lead Prevention (DLP)	BSP is responsible for installation, configuration of Biometric ABIS software. BSP will support MSI by providing access to ABIS system to get these elements installed as required. Kindly modify the clause accordingly by excluding BSP from the **responsibility** for installation, confirguration and tuning for other software.		Agreed.
390	Vol-2	Annexure 3: Minimum Technical Specification. , Clause 3.6.1.1 (27) Platform Requirement	337	ABIS should be compatible with Windows as well as Linux OS with both 32- and 64-bit support on X86 COTS H/W.	ABIS processes large data so it require huge capacity of RAM i.e. much larger than 4GB, whereas 32-bit HW will support only up to 4GB RAM. Please update the requirement accordingly.		The ABIS solution shall be compatible with Windows and Linux operating systems on x86-based COTS hardware and shall support 64-bit architecture. Support for 32-bit components, if any, shall be optional and not mandatory.
391				General Query	The VPN Access to the DC /DC will be required for development/ Testing, CD?CI or various elements of the solution. Kindly ensure		To be discussed and finalized at the time of implementation in
392	Volume-2	Section VI, Clause 5 (4)	19	The MSI shall provide a detailed cutover plan before migrating from the legacy system and a roll out plan. Upon providing the plans the approval must be taken	As discussed with NISG, there will be no migration of existing data. The MSI is only required to integrate the SL-UDI with the current system to retrieve pre-existing citizen information from the existing		Yes the understanding is correct
393	Volume-2	Section VI, Clause 5.2.1.1	49	The MSI should augment a fiber-based connectivity for data replication between the two sites, if required. The MSI shall undertake a capacity assessment and undertake capacity augmentation to meet the required	As discussed with NISG, all link-related activities will be managed by the MSP, not the MSI. Accordingly, connectivity between the DC and DR, along with uptime requirements, will be handled by GoSL or the MSP. Kindly confirm.		Yes the understanding is correct
394	Volume-2	Section VI, Clause 5.2.1.1 (iii)	49	Should provide Access cards, Gate passes to the GoSL personnel / GoSL appointed system integrators as and when they require visit the site. (Such access should be provided 24 X 7 and will not have any time restriction).	As discussed with NISG, GoSL will engage a co-location service provider to host the DC & DR services. Therefore, all physical access to the Data Centre will be managed by GoSL, with necessary coordination from the MSI. Kindly Confirm		Yes the understanding is correct
395	Volume-2	Section VI, Clause 5.2.1.1 (iv)	49	Should regularly monitor the access to the provided space (cage with necessary physical security) by means of access control system, physical security, biometric access, and CCTV (Closed-circuit television) and should	Since the DC will be hosted at the GoSL-designated co-location service provider, all physical security responsibilities should rest with the service provider and not with the MSI. Kindly Confirm.		Yes the understanding is correct
396	Volume-2	Section VI, Clause 5.2.6 Table 10: Network Connectivity	55	**Partner Network** The first TSP will be implemented by MSI where segregation of networks should be implemented.	Since GoSL will manage the links and the service provider, these responsibilities should be assigned to the MSP rather than the MSI. Kindly Confirm.		Appropriate modifcation has been made in the relevant clasue.
397	Volume-2	Section VI, Clause 5.2.6	55	**SL-UDI Wide Area Network** MSI will be required to provide secure and reliable connectivity.	As GoSL will be taking care of the links then it should be removed from the scope of MSI. Kindly Confirm		GoSL shall provide the connectivty

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
398	Volume-2	Section VI, Clause 5.2.6 Table 10: Network Connectivity	56	**Internet Connectivity** MSI will be required to provide secure and reliable internet dongles for connectivity of mobile registration centers with the DC and DR.	As GoSL will be taking care of the links then it should be removed from the scope of MSI. Kindly Confirm.		Dongles are to provided by GoSL
399	Volume-2	Section VI, Clause 5.3.1 Table 12: Mobile Kits	61	It is required to facilitate Mobile Kits with including the KIT items. **Internet Dongle**	As GoSL/MSP will be responsible for managing the links, the Internet dongle should fall under the MSP's scope, as they will benefit from the associated cost advantages. Kindly Confirm.		Dongles are to provided by GoSL
400	Volume-2	Section VI, Clause 5.8.2.2 (i) d.	87	**Data Backup Strategy** Tapes shall be moved by MSI to offsite location on Daily basis at a geographically separate location with appropriate physical security controls, at par with banking regulator of Sri Lanka for such secure transfer,	We Request this responsibility should be under GoSL scope. Kindly Confirm.		Data backup as per policy and Data Restoration would be the responsibility of the MSI. Shipment of Tape would be the responsibility of GoSL
401	Volume-2	Section VI, Clause 5.8.2.3	89	**HSM Recovery** MSI shall ensure HSM encryption keys (signing, encryption keys and master keys) are replicated to the High Availability HSM cluster and backed up every time a new key pair is generated, and the keys are stored	As the RFP BOQ does not specify the required quantity of HSMs, please confirm whether two HSMs are needed at the DC and two at the DR, or if one HSM per location will suffice. Kindly confirm.		Total Three - 1 HSM that can be partitioned. 1 backup HSM. 1 for the authentication
402	Volume-2	Section VI, Clause 5.8.2.3 (iii)	89	In the event of a catastrophe, such as a flood or fire, it might lose both your working HSMs and locally stored backup HSMs. To fully protect against such events, always store a copy of your backups at a remote	It has mentioned Locally stored backup, please clarify what does locally stored backup means.		Remote means location other than DC and this will be the responsibility of GoSL Localy stored backup means local
403	Volume-2	Section VI, Clause 5.8.2.3 (iv) Table 21: HSM Recovery	89	Offsite location (other than DC and DR) in fireproof safe. Offsite location (other than DC and DR) in biometric enabled locker with dual access control.	To store the keys in offsite location has be taken care by GoSl itself it should be removed from MSI scope.		Yes, removed from MSI scope , but the copy of backup shall be provided by MSI to GoSL
404	Volume-2	Section VI, Clause 5.8.2.4 (i)	89	MSI shall enable remote working of Data Center staff via VPN in case the sites are physically inaccessible.	What exactly the Data Center staff means? Please clarify.		The requirement is self expalnatory
405	Volume-2	Section VI, Clause 5.8.2.4 (iii)	89	Key staff to run the operations from locations designated by GoSL, if data center site is physically inaccessible.	What excatly is mean to key staff along with what type of VPN require Site to Site or RAVPN? Please confirm.		The requirement is self expalnatory
406	Volume-2	Section VI, Clause 5.8.4.1 (iv)	97	GoSL will be required to provide necessary IT (Hardware, Software, Network) and Non- IT Infrastructure (Communication Equipment such as	As per the the clause Contact center equipment will be provided by GoSL, requesting GoSL to include Voice Gateway as well.		Requirment of Voice gateway is dropped. MSI to provide required PBX and IP Phones.
407	Volume-2	Generic	NA		Please share the location of the NOC, SOC and IT-Helpdesk.		Location will be shared later with
408	Volume-2	Generic	NA		As per the asked BOQ for NOC, L3 device is missing then who will perform the routing. Please include and share the technical specification as well. Also please confirm if L3 device is not present		Bidder to call and propose L3 device if required.
409	Volume-2	Section VI, Clause 5.9.1.1	107	An indicative manpower for SOC is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of manpower required: (i) Analysts – 2 (ii) Technical Manager – 1 (iii) Supervisor - 1 (iv) Total - 4	Please confirm whether the total number mentioned in the clause is calculated per shift. If it is per shift, then the requirement appears higher, and typically a Supervisor is required only during the general shift. Please Confirm		The numbers provided in the RFP as indicative reqt/per shift. Bidder needs to assess the required number of staff and propose.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
410	Volume-2	Section VI, Clause 5.9.1.1 Table 27: Indicative Bill of Material for SOC	107	An indicative bill of material for SOC related items is provided below, the MSI should do its own analysis, design and estimation of arrive at the number of components required: 1. Video wall with controllers, speakers, and other accessories 2. LED TV 3. Laptop 4. Desktops / Monitors 5. Keyboards and Mouse 6. IP Phone 7. IP PABX	As per the asked BOQ for SOC, L3 device is missing who will perform the routing. Please include and share the technical specification as well.		Already answered in S.No. 408
411	Volume-2	Section VI, Clause 7	156	Clause 7 Schedule of Requirements	As per the BOQ bifurcation of the component is not mentioned, please clarify bidder need to consider qty as per the best of solution or not? Additionally, certain BOQ line items specify quantities—for example, 32 blade servers are mentioned in the RFP. Please confirm		The quantity may be read as NIL. However the sizing and the form factor has to be done by MSI according to its solution requiremnt
412	Volume-2	Generic	NA		Please share the locations of the DC and DR, along with the distance between them. Additionally, kindly provide the maximum rack capacity that the MSI can be allocated, along with the maximum supported power load for both the DC and DR.		Distance between DC-DR is 20 km(approx.) Space for 20 racks is available in the DC.
413	Volume-2	Annexure-12, Clause 12.1	3	**3 DRP Regional Offices:** Kurunegala Galle Vavunia Batticaloa Nuwara Eliya	Please confirm whether these sites will be connected to both the DC and DR over MPLS. If MPLS connectivity to the DC and DR is required, then routers/L3 device supporting the BGP routing protocol should be present at mentioned sites. Kindly confirm.		Yes this will be connected over MPLS but a dedicated pipe will be provided by GoSL.Any device required for backup and replication has to be provided by MIS
414	Volume-2	Section VI, Clause 5.8.4.1 (iv)	97	GoSL will be required to provide necessary IT (Hardware, Software, Network) and Non-ITInfrastructure (Communication Equipment such as	As per mentioned RFP clause, EPBX is going to provided by GoSL but in RFP SOR line item it it mentioned to provided by MSI, Please clarify.		Kindly refer amended RFP Annexure 3 : Minimum Tech requirement and RFP Volum 02
415	Volume-2	Section VI, Clause 7 Table 35: Bill of Material	162	112. Network Intrusion Prevention System (NIPS) and NIDS 113. Intrusion Detection System / Intrusion Prevention System	Both are the same things and only line item 113 having the technical compliances, please remove the 112 line item from SOR.		Refer to Amended RFP : Annexure 3 : Minimum Tech requirement
416	Volume-2	Generic	NA		As per the RFP, the MSI is required to use the existing citizen data to perform the necessary activities. For this activity, during implementation and testing, GoSL will be required to provide necessary access to the MSI's executives. Kindly confirm.		GoSL will provided anonymised 1000 dummy dataset of all three modalities. MSI may use this dataset to create 8 million dummy records for performance
417	Volume-2	Generic	NA		If the bidder can deliver a fully RFP-compliant solution using fewer equipment than specified in the RFP, will GoSL still permit such a solution? Kindly confirm.		Please configure the solution as per FR, NFR, Performance and SLA asked in the RFP and position
418	Volume-2	Annexure-10	NA	Generic Query	As Annexure-10 does not provide a bifurcation of DC and DR manpower, our understanding is that the same NOC and SOC teams will manage both DC and DR operations. Please confirm if this understanding is correct.		NOC and SOC will me masnaged by MSI. The numbers provided in the RFP as indicative reqt/per shift. Bidder needs to assess the
419	Volume-2	Generic	NA		As per discussion with NISG some Nos of Biometric scanner has already been procured by GoSL last year kindly share the count,		1. Finger Print Scanner - Kojak, KJ220DA-EOO

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
420	Volume-2	Annexure-3, Clause 3.2 (g) (43) and Clause 3.4.1.9	6 and 96	43) Internet Router 3.4.1.9 Network - Core Router	As per the technical specifications, the Internet Router configuration appears to be similar to that of the Core Router, which seems to be on the higher side. Kindly consider revising and optimizing the specifications.		Already answered in S.No. 293
421	Volume-2	Annexure-3, Clause 3.2 (g) (44) and Clause 3.4.1.9	6 and 96	44) MPLS Router 3.4.1.9 Network - Core Router	As per the RFP, a Core Router has already been requested from the MSI; however, the MPLS Router is also specified with same high-end specifications. Considering that only two types of traffic will enter the DC—one from MPLS and the other from the Internet—please clarify the specific role of the Core Router.		Already answered in S.No. 294
422	Volume-2	Annexure-3, Clause 3.4.1.10	98	Network: Core Switches - LAN	As per the RFP, a Leaf-Spine architecture has been specified, and separate specifications for the Spine Switch are provided in Section 3.4.1.14 of Annexure-3. However, the requirement for a Core Switch (LAN) is also mentioned. Kindly clarify the intended role and		Already answered in S.No. 295
423	Volume-2	Annexure-3, Clause 3.2 (g) (35) ,(49) and Clause 3.4.1.1	6	35) Blade Servers 49) Data Centre Access Switch 3.4.1.1 Blade Servers	As per Annexure-3, Section 3.4.1.1 mentions both the Blade Server and the Data Centre Access Switch; however, the specifications provided pertain only to the Blade Server. Kindly confirm which section the MSI should refer to for the Data Centre Access Switch specifications.		Already answered in S.No. 296
424	Volume-2	Annexure-3, Clause 3.2 (g) (46) and Clause 3.4.1.14 and Clause 3.4.1.13	6	46) Application Load Controller (Server / Application Load Balancer) 3.4.1.14 Data Center Spine Switch and 3.4.1.13 DC Software Defined networking (SDN) Fabric Architecture	As per Annexure-3, line item **46 — Application Load Controller (Server / Application Load Balancer**) — has been mapped to **Sections 3.4.1.14 and 3.4.1.13**. However, these sections pertain to the **DC Software Defined Networking (SDN) Fabric Architecture and the Data Centre Spine Switch.** Kindly confirm the correct section that the MSI should refer to. Additionally, we request that this line item be removed from the SOR, as the Server Load Balancer has already been included		Already answered in S.No. 297
425	Volume-2	Annexure-3, Clause 3.2 (g) (45) and Clause 3.4.1.14	6	45) Global Load Balancer 3.4.1.14 Data Center Spine Switch	As per Annexure-3, Line Item **45 (Global Load Balancer) is mapped to Section 3.4.1.14**; however, the specifications for the Global Load Balancer are provided in **Section 3.14.1.18 on page 117**. Kindly confirm.		Already answered in S.No. 298
426	Volume-2		NA	Generic Query	As per the RFP, both Tape Library and VTL have been specified. Since Tape Library technology is considered outdated, we request		Already answered in S.No. 299
427	Volume-2	Annexure-3, Clause 3.4.1.17 Server Load Balancer	115	Clause 3.4.1.17 Server Load Balancer	There is currently insufficient clarity regarding the expected traffic requirements. For Example: "The proposed solution must handle high-capacity traffic, including L7 requests per second: 450K L4 connections per second:150K concurrent L4 connections:18M L4 throuput 20 Gbps on day 1 and scalable upto 25 Gbps"		The expected traffic requirements are as under, based on which MSI may size L7, L4 and throughput parameters. 1. The current user base is 2000 with 200 concurrent users. 2. The authentication requests per second is 14. 3. OTP request per second is 150 4. Packet size given in demand capacity annexure A5 , both for authentication and enrollment

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
428	Volume-2	Annexure-3, Clause 3.4.1.18 Global Load Balancer	116-117	Generic Query	Clarity required on the number of expected DNS Request per second, which would help in sizing the appliance.		50,000 DNS QPS
429	Volume-2	Annexure-3, Clause 3.4.1.18 Global Load Balancer	116-117	Clause 3.4.1.18 Global Load Balancer	"Must support resolution for A, AAAA, A6 ,CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, TXT and SRV queries as Internal DNS and Must support resolution for A, AAAA, MX, and NS queries as External DNS". Kindly Confirm.		Agreed.
430	Volume-2	Annexure-3, Clause 3.4.3.15 (26)	232	26) Support for VRRP, QoS and full OSPF routing protocol.	Please change it to as per the below mentioned as VRRP is gateway redundancy protocol and OSPF is a routing protocol. "Support for VRRP or equivalent protocols"		Agreed - VRRP or Equivalent Protocol
431	Volume-2	Annexure-3, Clause 3.4.3.18 (11)	242	11) RAM 64 GB	To support 30 Gbps throughput, while preventing OWASP Top 10 and SANS Top 25 attacks, significant memory is required for packet inspection, state tracking, and rule processing. 64 GB RAM may cause bottlenecks under high traffic or attack scenarios. At least		Agreed. 128 GB RAM.
432	Volume-2	Annexure-3, Clause 3.4.3.18 (14)	243	14) Network interface ports- 24, 4*40Gbps and	Clarity required. In a modern spine-leaf network, the emphasis is on high-speed links (e.g., 10/25/40/ Gbps) rather than a large number of ports. Efficient interconnections with aggregated uplinks reduce the need for devices with 24 ports. The architecture uses fewer, faster ports for scalability and performance, making excessive port counts unnecessary. **It should have** 2 x 100G/40G QSFP28/QSFP+ ports		The requirement for "24, 4×40" ports is indicative, not strict. A modern port mix with higher-speed interfaces (such as 25G/100G uplinks) that meets or exceeds the switching capacity and performance requirements is acceptable.
433	Volume-2	Annexure-3, Clause 3.4.3.10 (5)	204	5) Should support latency less than <75 microseconds and should be clearly documented in the data sheet.	The requirement for a fixed latency of <75 microseconds should be reconsidered, as latency is influenced by multiple factors beyond the hardware's capabilities, including network topology, connection		Already answered in S.No. 55
434	Volume-2	Annexure-3,Clause 3.4.3.10 (6)	204	6) SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	Module/appliance System should Mitigate encrypted attacks and should have 7000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key from day 1 and scalable upto 15K TPS."		Already answered in S.No. 55
435	Volume-2	Annexure-3, Clause 3.3.3.10 (2)	53	Lifecycle maintenance capabilities including definition, creation, security, monitoring and management	It is proposed to change to "The proposed solution shall provide API Lifecycle maintenance capabilities including definition, security monitoring and management."		Already answered in S.No. 308
436	Volume-2	Annexure-3,Clause 3.3.3.10 (3)	53	The proposed solution shall have API cataloguing capabilities along with mechanism to set up and externalize the APIs.	Please change it to **"The proposed solution shall have the capability to externalise APIs and should provide cataloguing capabilities with third party integrations."** because API cataloguing is not inherently a primary function of API gateway servers, as the core purpose of an API gateway is to manage, secure, and route API traffic. Their primary responsibility is to act as a central access point for APIs, handling authentication, load balancing, rate limiting, and request/response management. For advanced cataloguing capabilities such as detailed documentation, taxonomy management, or developer portal integration, leveraging third-		Already answered in S.No. 309

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
437	Volume-2	Annexure-3, Clause 3.2 (c)	3	In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave of Forrester Wave or Major Players in IDC MarketScape.	This is an ambiguous clause for Web Application Firewall Solution. Being a technology leading OEM for Web application Firewall, we seek some clarifications. It is important to note that recent third-party reports on Web Application Firewalls (WAF) now include a broader range of solutions, such as cloud-based services (WAAP-as-a-Service) OEMs in addition to traditional hardware OEMs. However, since the current requirement specifically pertains to hardware-based solutions, please clarify whether, for the purpose of evaluating the 4 distinct vendor criteria, Technology OEMs		Alreadt answered in S.No. 177
438	Volume-2	Annexure-3, Clause 3.2 (e)	4	In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of size, number of transactions, data and users handled iv)	Regarding the Load Balancer (ADC) category, we would like to clarify that the most recent Gartner report available was published in 2016. Additionally, there are currently no relevant reports available from IDC or Forrester for this category. In light of this, kindly advise whether: 1. We may submit a relevant customer use case instead, or 2. The 2016 Gartner report can still be considered valid for evaluation purposes.		Alreadt answered in S.No. 178
439	Volume-2	Annexure-3, Clause 3.4.3.10 (1)	204	1) DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. **Suggested Clause:** **The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).**		Already answered in S.No. 55
440	Volume-2	Annexure-3, Clause 3.4.3.10 (2)	204	2) Should have 4X10Gbps and 4X 40 Gbps SFP Interfaces. Interfaces should be populated with multi-mode fiber transceiver modules.	The proposed sizing appears to be misaligned with the other specified requirements like throughput which is only 1 Gbps scalable to 10 Gbps. 40G port will increase the size and overall cost of the solution. Hence, we request technical team to streamline sizing as per the requirement. **Suggested Clause :**		Already answered in S.No. 55
441	Volume-2	Annexure-3, Clause 3.4.3.10 (3)	204	3) System should have scalable inspection throughput of 5 Gbps scalable to 10 Gbps without additional hardware.	This clause is ambiguous as there are different throughput is asked. Generally DDoS Solution are sized on the basis of mitigation throughput and Legitimate throughput. Hence we recommend to amend the clause accordingly for ease of sizing. **Suggested Clause :** **System should have scalable mitigation throughput of 10 Gbps**		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
442	Volume-2	Annexure-3, Clause 3.4.3.10 (6)	204	6) SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. **Suggested Clause :** **SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card.** **Appliance should also support TLS 1.3 PFS Hardware Acceleration**		Already answered in S.No. 55
443	Volume-2	Annexure-3, Clause 3.4.3.10		New Clause	**Proposed Appliance should use real-time-signature creation technology to protect against DNS based DDoS Attack which should include but not limited to Packet Checksum, DNS FQDN, DNS Domain Name, Source IP address, Packet Size, DNS Query ID,**		Already answered in S.No. 55
444	Volume-2	Annexure-3, Clause 3.4.3.10		New Clause	**The proposed solution should have Geo Fencing/Geo Blocking to block the traffic or allow the traffic from specific Geo Location. Geo Fencing should also support Threshold based blocking based on configure PPS or Kbps value, to determine the rate of permitted traffic from the selected geolocations. Once any of the thresholds is reached, all traffic from the specified geolocations is**		Already answered in S.No. 55
445	Volume-2	Annexure-3, Clause 3.4.3.10		New Clause	**The proposed appliance should support Integration with OEM owned Cloud based Scrubbing Centers, in case of Bandwidth Saturation attacks, using the same technology, in case it is required by department with additional license.** **OEM Should have atleast once Cloud Scrubbing Centre in SAARC**		Already answered in S.No. 55
446	Volume-2	Annexure-3, Clause 3.4.3.18 (1)	242	1) The solution must be appliance based.	Appliance should be dedicated only, there should not have any option to import 3rd party OS on same hardware. **Suggested Clause:** **Application Delivery Controller shall be purpose built dedicated hardware appliance, there should not have any option to run 3rd**		Already answered in S.No. 196
447	Volume-2	Annexure-3, Clause 3.4.3.18 (9)	242	9) Should have a minimum set of rules defined to prevent OWASP Top 10 and SANS Top 25 attacks in default configuration	Every OEM has its own way of Handle OWASP TOP10/SANS 25 Attacks. Hence, we request to generalize the clause. **Suggested Clause:** **Should have rules to prevent OWASP Top 10 and SANS Top 25**		Already answered in S.No. 197
448	Volume-2	Annexure-3, Clause 3.4.3.18 (10)	242	10) Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	Solution can be oversized when considering the solution scalability. We request technical team to lower down the requirement a little to accommodate the solution. **Suggested Clause:** **Throughput minimum 30 Gbps from day 1 with scalability to upto**		Already answered in S.No. 46

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
449	Volume-2	Annexure-3, Clause 3.4.3.18 (12)	243	12) SSL transaction 10,000 CPS/TPS	From the provided specifications, it appears that support for ECC (Elliptic Curve Cryptography) and the TLS 1.3 protocol is currently missing. Modern applications increasingly rely on ECC for its lightweight performance and strong security, along with TLS 1.3 for enhanced privacy and reduced handshake latency. These are now considered best practices in securing web communications. We strongly recommend including support for ECC and TLS 1.3 in the specifications to ensure future readiness and compliance with modern security standards.		Already answered in S.No. 199
450	Volume-2	Annexure-3, Clause 3.4.3.18 (14)	243	14) Network interface ports – 24, 4*40Gbps and	Network interfaces requirement is not clear, may be some typo. Additional 40 Gbps is an over kill. Hence, request to amend this. **Suggested Clause:** **Network interface ports - 24*10 Gbps port (without use of**		Already answered in S.No. 200
451	Volume-2	Annexure-3, Clause 3.4.3.18 (15)	243	15) SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. **Suggested Clause:** **SSL throughput 10 Gbps scalable to 20Gbps.**		Already answered in S.no. 47
452	Volume-2	Annexure-3, Clause 3.4.3.18 (18)	243	18) Internet link connections supported by load balancer – 8191	We are talking about WAF here, so link doesn't not make sense. We request to add more related terms for reference to generalize the clause. **Suggested Clause :**		Already answered in S.No. 202
453	Volume-2	Annexure-3, Clause 3.4.3.18 (22)	243	22) Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. **Suggested Clause :**		Already answered in S.no. 48
454	Volume-2	Annexure-3, Clause 3.4.3.18 (31)	244	31) Proposed WAF Solution should Identify and limit / block suspicious clients, headless browsers and also mitigate client- side malware.	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause:** **Proposed WAF Solution should Identify and limit / block**		Already answered in S.No. 204
455	Volume-2	Annexure-3, Clause 3.4.3.18 (33)	244	33) Should provide encryption for user input fields to protect from browser-based malwares stealing users credentials	Malware is not a feature of a web application firewall. We request technical team to relax this clause. **Suggested Clause :** **Should support encrypted session between user and WAF (to protect against any data hijacking in transit) and should have provision to select between encrypted or decrypted traffic**		Already answered in S.No. 205
456	Volume-2	Annexure-3, Clause 3.4.3.18 (34)	244	34) On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address. For particularly destructive attacks, the Web application firewall should be able to block the user or the IP address for a configurable period of time.	Every OEM has its own way of Handling Attack packet.Hence, we request to generalize the clause. **Suggested Clause:** **On detecting an attack or any other unauthorized activity, the Web application firewall must be able to take the appropriate action. Supported actions should include the ability to drop requests and responses or block the TCP session or block the application user, or block the IP address. For particularly**		Already answered in S.No. 206

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
457	Volume-2	Annexure-3, Clause 3.4.3.18	244	New Clause	Appliance should support virtualization feature with option to create isolated environment from application and management perspective. 5 Virtual Instance from day1 and scalable upto 30 Virtual Instance Each instance should have dedicated: Resource, management, configuration and operating system. There should not have any		Already answered in S.No. 330
458	Volume-2	Annexure-3, Clause 3.4.3.18	244	New Clause	**The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No proprietary Protocol).**		Already answered in S.No. 331
459	Volume-2	Annexure-3, Clause 3.4.1.17 (1)	115	1) Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax and include more SLB based requirements : **Suggested Clause :** **Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, L4/L7 content**		Already answered in S.No. 207
460	Volume-2	Annexure-3, Clause 3.4.1.17 (11)	116	11) Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. **Suggested Clause :** **Solution should have VLAN Support.**		Already answered in S.No. 49
461	Volume-2	Annexure-3, Clause 3.4.1.17 (12)	116	12) Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : **Suggested Clause :** **Should have IPv6 Support for SLB, interfaces, routing.**		Already answered in S.No. 50
462	Volume-2	Annexure-3, Clause 3.4.1.17 (14)	116	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. **Suggested Clause:** **The solution should supports the following load balancing methods:** **a. Round-Robin** **b. Weighted Round-Robin** **c. Least Connections** **d. Fastest Response** **e. Hash,**		Already answered in S.No. 51

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
463	Volume-2	Annexure-3, Clause 3.4.1.17 (15)	116	Solutions should provide application & server health checks for well-known protocols like ICMP, TCP, TCP_ECHO, HTTP, HTTPS etc.	TCP_Echo is not the primary health check setting. Rather the solution should support Script Based Health check and Logical Expresssion Based Health check for Combining multiple rules. **Suggested Clause:** **The proposed solution should supports the following health check types:** **• Link Health Checks,** **• TCP Health Checks,** **• UDP Health Checks,** **• ICMP Health Checks,** **• HTTP/S Health Checks,** **• TCP and UDP-based DNS Health Checks,** **• WAP Gateway Health Checks,** **• Virtual Wire Health Checks,** **• DSSP Health Checks,**		Already answered in S.No. 211
464	Volume-2	Annexure-3, Clause 3.4.1.17	116	New Clause	In the specifications for Server Load Balancer, Sizing requiement is missing. Hence, we request technical committee to include mising sizing requirement . **Suggested Clause :** **Traffic Ports: 2 x 10 GE Fiber and 8 x 1G Copper from day1. Option for additional 8 x 1 GE Fiber and 8 x1G copper for future use (Break-Out should not be used)** **L4 Throughput: 20 Gbps and scalable upto 40 Gbps** **Layer 4 connection per second: 500,000** **RSA CPS(2K Key): 20,000** **ECC CPS (EC-P256): 12,000 with TLS1.3 Support** **The appliance should have dedicated 2x1G RJ45 Out-of-band**		Already answered in S.No. 337
465	Volume-2	Annexure-3, Clause 3.4.1.17	116	New Clause	**Virtualization is a very important feature in load balancers enables efficient resource utilization by allowing multiple virtual instances to run on a single physical device, enhancing scalability and flexibility. It also simplifies deployment and management in dynamic, multi-tenant environments covering different applications zones, critical applications, etc.** **VIRTUALIZATION:** 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 **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, **d) Operating System** The proposed device should support 5 Virtual Instance from Day 1 and support upto 10 Virtual Instances for future Scalability on the		Already answered in S.No. 338

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
466	Volume-2	Annexure-3, Clause 3.4.1.17	116	New Clause	**Bidder should propose Centralized Management & Reporting Solution from Day 1.** **Centralized management solution should provide:** **Application Dashboard** **Per Application Analytics** **SLA Breakdown (Network, per server)** **SSL Statistics (handshake and cypher breakdown, rejected handshake)** **SSL CPS** **System Dashboard** **Network Dashboard** **L4 Events**		Already answered in S.No. 339
467	Volume-2	Annexure-3, Clause 3.4.1.17	116	New Clause	**The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP**		Already answered in S.No. 340
468	Volume-2	Annexure-3, Clause 3.4.1.18	116-117	New Clause	In the specifications for Server Load Balancer, Sizing requiement is missing. Hence, we request technical committee to include mising sizing requirement . **Suggested Clause :** **Traffic Ports: 2 x 10 GE Fiber and 8 x 1G Copper from day1. (Break-Out should not be used)** **L4 Throughput: 6 Gbps and scalable upto 25 Gbps** **Layer 4 connection per second: 500,000**		Already answered in S.No. 341
469	Volume-2	Annexure-3, Clause 3.4.1.18	116-117	New Clause	**Virtualization is a very important feature in load balancers enables efficient resource utilization by allowing multiple virtual instances to run on a single physical device, enhancing scalability and flexibility. It also simplifies deployment and management in dynamic, multi-tenant environments covering different applications zones, critical applications, etc.** **VIRTUALIZATION:** 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 **Each Virtual Instance contains a complete and separated environment of the Following:** a) Resources, b) Configurations, c) Management, **d) Operating System** The proposed device should support 5 Virtual Instance from Day 1 and support upto 20 Virtual Instances for future Scalability on the		Already answered in S.No. 338
470	Volume-2	Annexure-3, Clause 3.4.1.18	116-117	New Clause	**The Solution should support native integration with Kubernetes Platforms and controller/connecter/plugin should operate within Kubernetes Cluster to automatically create service on Load Balancer. The controller/connecter/plugin should also support automatic creation, edition and deletion of service like VIP**		Already answered in S.No. 340

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
471	Volume-2	Annexure-3, Clause 3.4.1.18	116-117	New Clause	**The proposed device should support blelow GSLB Metrics:** **Least Connections** **Round Robin** **Response** **Geographical** **Network** **Availability** **QoS** **Minmisses** **Hash** **Local** **Always** **Remote** **Persistence** **Proximity** **Bandwidth**		Already answered in S.No. 344
472	Volume-2	Annexure-3, Clause 3.4.1.18	116-117	New Clause	**The proposed device should support standard VRRP (RFC - 2338) for High Availability purpose (No Propertary Protocol).**		Already answered in S.No. 331
473	Volume-2	Annexure-3, Clause 3.4.3.5 (1)	190	1) Proposed Web Solution should be an on premise having Proxy, URL filter Caching, SSL Inspection, Anti-Virus, Antimalware, multiple detection engines.	1.Kindly confirm whether the solution is required to be deployed on a physical hardware appliance, or if deployment on a virtual machine is acceptable. In the case of a virtual deployment, will the required infrastructure be provisioned by the SLUDI ?		Already answered in S.No. 346
474	Volume-2	Annexure-3, Clause 3.4.3.5 (4)	190	4) The Solution should integrate with SIEM, APT solution and the proposed/existing Ticket Management system for proactive detection and	Which exisiting SIEM/APT/Ticketing system SLUDI is using		Already answered in S.No. 347
475	Volume-2	Annexure-3, Clause 3.4.3.5 (8)	191	8) The solution must support different types of compression algorithms and should be able to scan encoded and compressed files.	The use of the clause is not clear. Please explain the use of the mentioned clause.		Already answered in S.No. 348
476	Volume-2	Annexure-3, Clause 3.4.3.5 (29)	193	29) The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to	These are either encrypted, non-HTTP-based or not inspectable using standard web proxy mechanisms. Kindly confirm if all these are mandatory or flexible based on actual use case.		Already answered in S.No. 349
477	Volume-2	Annexure-3, Clause 3.2 (e)	4	e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of size, number of transactions, data and users handled iv) details of the scenario for which the product is	We understand that in case the OEM whose product is not cited in the Gartner Quadrant / Forrester Wave / IDC MarketScape report will need to submit 1 case study of similar complexity and dimension where the same product is deployed, kindly confirm whether our understanding is correct. Furthermore, we interpret that solutions with comparable complexity and scale—such as those delivered for Telecom, Smart City, Safe City, large enterprise, Government, or PSU projects—shall be considered under this category, Kindly confirm.		Already answered in S.No. 350

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
478	Volume-2	Annexure-3, Clause 3.2 (a)	3	a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the	Mandating that the product be in the Leaders Quadrant of Gartner Magic Quadrant, Forrester Wave, or IDC MarketScape significantly restricts competition and may inadvertently exclude technically qualified OEMs whose solutions meet internationally recognized standards. Many capable vendors maintain rigorous certifications such as CMMI Level 3, ISO 27001, ISO 27034, and ISO 9001, demonstrating high-quality processes, robust security practices, and global compliance. Such restrictive criteria could: Reduce the pool of eligible bidders, Increase procurement costs,Limit innovation and technology diversity Thereby , to ensure a competitive procurement process, we request that eligibility be determined based on demonstrable capabilities		Already answered in S.No. 351
479	Volume-2	Annexure-3, Clause 3.2 (c)	3	c. In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave			Already answered in S.No. 352
480	Volume-2	Section VI, Clause 5.11.2.12 (iv) (b)	132	b. For IT Service Management, ITIL v3 is the chosen framework and ISO/IEC20000 is the chosen quality standard.	Please confirm our understanding that the latest version of ITIL, i.e., ITIL v4, shall be considered for IT Service Management compliance. Furthermore, ISO/IEC 20000-1 is a certification for a Service Management System (SMS) focused on process quality and continual improvement for trusted service delivery and support processes, Thereby we request that the ISO/IEC20000 certifications shall be considered as applicable from the OEM of the proposed		Already answered in S.No. 354
481	Volume-2	Section VI, Clause 5.1.3.1 (i)	33	(i) GoSL is seeking the capability to analyze large quantities of business data, transform the data into intelligence and insight, and deliver this intelligence and insight to the GoSL's processes and users. In a move aimed towards digital economy in Sri Lanka, the GoSL has taken up a Data Analytics and Business Intelligence initiative for SL-UDI Information System. SL-UDI Information System would help increase efficiency and availability of reliable data in a timely manner. GoSL desires to build enterprise-level DA and BI system with definition of Key Performance Indicators (KPIs) for SL-UDI Information System. The KPIs need to be viewed from a Division, Function,	Request clarification on the expected volumetrics to be considered for optimal estimation, sizing , and solution: 1. Data volume to be considered for the proposed solution, i.e., whether 20TB or 40TB ,100TB or higher, or higher 2. Tentative number of KPIs to be provided as part of the BI 3. Number of data sources to be integrated and type of integration format such as REST API, DB links etc. 4. Number of Reports and Dashboards required 5. Data retention duration.		Already answered in S.No. 355
482	Volume-2	Section VI, Clause 5.1.3.1 (ii)	33	(ii) The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of Data Analytics and Business Intelligence Solution for SL-UDI Information System. The MSI shall enable the system to provide comprehensive monitoring of enrolment	Request clarification on the number of data sources to be integrated with the proposed solution, along with details of the integration types or interfaces expected. This information will assist in accurate sizing and architectural planning of the solution.		Already answered in S.No. 356
483	Volume-2	Section VI, Clause 5.1.3.1 (vi)	33	(vi) The proposed product should preferably be an open-source solution along with Enterprise support.	We understand that the OEM of the proposed solution shall provide support for any open-source components utilized within their overall solution, as the ownership and responsibility for the complete solution rest with the OEM of the offered product line.		Already answered in S.No. 357
484	Volume-2	Section VI, Clause 5.1.3.1 (ix)	34	(ix) GoSL shall prescribe reports to be developed which will be identified at requirements stage as well as operations phase.	Request clarification on the expected number of reports required at both the requirements stage and the operational phase to assist the OEM in accurately sizing, estimating and designing the solution.		Already answered in S.No. 358
485	Volume-2	Section VI, Clause 5.1.3.1 (x)	34	(x) The Data Analytics system should allow GoSL to customize notification of certain indicator that GoSL is interested in to trigger activities/actions. The Data Analytics module should have a user interface to extract data based on the data required for self-analytics and report generation. The Data Analytics module should also allow for ad-hoc queries pertaining to the module for quick access to real time	We understand that the total requirement for BI users is five. Kindly also specify the expected number of concurrent application users for accurate solution sizing and capacity planning. Please also confirm the data retention duration.		Already answered in S.No. 359

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
486	Volume-2	Annexure-3, Clause 3.4.2.9	151	3.4.2.9 Enterprise Monitoring system	To optimize the sizing and Bill of Materials for the Enterprise Monitoring System, we request you to kindly share the total number of users and concurrent users required for proper capacity planning and proposing the optimal solution. Please also confirm		Already answered in S.No. 360
487	Volume-2	Annexure-3, Clause 3.4.2.11	160	3.4.2.11 IT Service Management	To optimize the sizing and Bill of Materials, we kindly request you to provide the number of end users, number of operators/technicians, and the number of concurrent users for accurate solution sizing and		Already answered in S.No. 361
488	Volume-2	Annexure-3, Clause 3.4.2.8 (4.3)	145	4.3) The proposed APM platform must support both Linux and Windows flavours for deployment of its core components (such as management server) and should not require any kind of "root access" or "root privilege" to deploy agents in the monitored applications.	Asking for deployment on both Windows and Linux OS restricts participation of capable OEMs, the focus should be to have a solution that runs on modern open technologies like docker/containers and microservices architecture to ensure scalability, flexibility and performance. Additionally Linux-based operating systems are widely recognized for their robust security architecture and are preferred platforms for most OEM solutions. Considering best practices and to encourage broader OEM participation, we request to update the clause as below,		Already answered in S.No. 362
489	Volume-2	Annexure-3, Clause 3.4.2.8 (4.21)	150	4.21) The platform should offer automatic Runtime Application Self- Protection (RASP) for modern applications, keeping both users and the digital business secure by detecting vulnerabilities at runtime and defending against attacks to prevent breaches on real time basis without having a need to deploy any extra agent. The module should offer following capabilities around application security: 1. Monitor common vulnerabilities in OWASP Top 10 along with providing the related CVE details of vulnerability detected in application runtime and provide recommendation related to remediation of these vulnerabilities.2. Harvest threat intelligence feeds from multiple sources including open source databases like NIST NVD and other OEM threat feeds assisting team in identifying any potential risks. 3. Flag any risk through API ecosystem and correlate these security context with business transactions through risk score helping team to prioritise and respond to security risks and reduce overall organisational risk profile. 4. Detects and block attacks on near real-time basis along with providing details around summary of attacks (like entry point, vulnerability used, attack type etc.) for an easy hand off between security and	The features specified in this clause pertain to security & vulnerability assessment solutions typically provided by security OEMs and are not integral to standard NMS/EMS frameworks. Inclusion of this feature may inadvertently Favor a particular OEM and limit broader participation. We request that this clause be removed for wider OEM participation.		Already answered in S.No. 363
490	Volume-2	Section VI, Clause 5.1.4.5	39	Generic Query	Please confirm the expected monthly transaction volume, number of services, and record growth (G2C/G2B) to size the system accurately.		Already answered in S.No. 364
491	Volume-2	Section VI, Clause 5.1.4.5 (c)	39	c. Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.	Please specify whether a central service catalogue need to be propsoed as part of the solution . If yes, kindly provide: 1. Specification of catalogue structure 2. Approval workflows		Already answered in S.No. 365

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
492	Volume-2	Section VI, Clause 5.1.4.5 (c)	39	Manage customer profile, metering and pricing configurations, invoicing and receivables, collections, notifications, reporting, etc.	Please confirm whether billing includes: 1. Subscription-based billing 2. Usage-based billing 3. Invoice-based billing		Already answered in S.No. 366
493	Volume-2	Section VI, Clause 5.1.4.5	39	Generic Query	The RFP states that SBS must integrate with multiple systems (Payment Gateway, SSO, portals, service delivery systems). Kindly provide: 1. List of systems & technology stack where integtrations are required 2. API specifications (SOAP/REST) and Expected number of API calls		Already answered in S.No. 367
494	Volume-2	Section VI, Clause 5.1.4.5	39	Generic Query	1. Please confirm the data retention policy: 2. How many years' invoices must be stored? 3. Cold storage vs hot storage requirements 4. Retrieval time expectations for archived invoices		Already answered in S.No. 368
495	Volume-2	Annexure-3, Clause 3.4.3.24 (1)	**261**	1) The proposed solution should detect web application, Host and Network vulnerabilities via crawl/application analysis, stack finger printing, universal translator, normalization, pre-attack analysis, attack, and generating reports after the scan runs.	Kindly Remove the Network parts as the heading of this requirements is for Web Application, Mobile Applications and APIs		The solution shall detect vulnerabilities in Web Applications, Mobile Applications, and APIs, including any application-exposed host or
496	Volume-2	Annexure-3, Clause 3.4.3.24 (38)	**267**	38) The proposed solution should have the ability to be programmed to test custom in-house web protocol. Describe how can the solution achieve that.	Kindly amend this points as Support HTTP/HTTPS		The solution shall fully support HTTP/HTTPS scanning and shall also provide the capability to programmatically test custom in-house web protocols. Bidders shall describe how this capability
497	Volume-2	Annexure-3, Clause 3.4.3.24 (41)	**267**	41) The proposed solution should have the ability for determining code coverage completeness of your testing solution - to understand and highlight areas of the application that were not covered with the testing.	Code coverage is not part of web application scanning. Its more of code quality testing. Kindly Remove this points		No change
498	Volume-2	Annexure-3, Clause 3.4.3.24 (56)	**270**	56) The proposed solution should produce logic-flow and data- flow analysis that could help find design flaws that cause security vulnerabilities. Describe the logic flaws analysis the solution detect.	data flow analysis is only possible when the code of the application is getting scanned. Kindly confirm whether our understanding is right.		No change
499	Volume-2	Annexure-3, Clause 3.4.3.24 (57)	**270**	57) The proposed solution should support data-flow analysis capability span applications that run on different platforms written in different languages. Describe how the solution achieves that.	Data flow analysis is only possible when the code of the application is getting scanned. Kindly confirm whether our understanding is right.		Already answered in S.No. 498
500	Volume-2	Annexure-3, Clause 3.4.3.24 (58)	**270**	58) The proposed solution shall provide Network based vulnerability assessment to perform automated, distributed or event driven probes of geographically dispersed network services, operating systems, routers/switches, mail servers, web servers, firewalls	AppScan detects only application related vulnerabilities and not related to networks. Kindly confirm whether our understanding is right.		Your understanding is right
501	Volume-2	Annexure-3, Clause 3.4.3.24 (60)	**270**	60) Network and Server Settings: a. Network Vulnerabilities b. OS Patches c. System Auditing d. Services e. File System and Directories f. File Attributes g. File Access h. Registry Permissions	These requirements are for network/infra vulnerability scanners. Kindly Remove		Agreed. Clause is deleted
502	Volume-2	Annexure-3, Clause 3.4.3.24 (82)	**273**	82) The proposed solution should have ability to scan even without on-premises scan engines installed by default.	The scan engines has to be installed on-premises unless the ask is for saaS based solution. Kindly change the requiremnt		Requirement is for On Premise Deployment. SaaS model is not required

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
503	Volume-2	Annexure-3, Clause 3.4.2.8 (4.21)	**150-151**	4.21 The platform should offer automatic Runtime Application Self Protection (RASP) for modern applications, keeping both users and the digital business secure by detecting vulnerabilities at runtime and defending against attacks to prevent breaches on real time basis without having a need to deploy any extra agent. The module should offer following capabilities around application security: 1. Monitor common vulnerabilities in OWASP Top 10 along with providing the related CVE details of vulnerability detected in application runtime and provide recommendation related to remediation of these vulnerabilities. 2. Harvest threat intelligence feeds from multiple sources including open source databases like NIST NVD and other OEM threat feeds assisting team in identifying any potential risks. 3. Flag any risk through API ecosystem and correlate these security context with business transactions through risk score helping team to prioritise and respond to security risks and reduce overall organisational risk profile. 4. Detects and block attacks on near real-time basis	Please confirm if Runtime Application Self-Protection (RASP) is expected to be delivered natively within the proposed platform or through integration with existing enterprise Application Security tools. Our solution focuses on Observability and APM capabilities (logs, metrics, traces, transactions), while runtime vulnerability detection and prevention as described is typically addressed by dedicated AppSec/RASP products. Kindly clarify if integration is acceptable.		The proposed APM and Observability platform shall support Runtime Application Security capabilities, including runtime detection of OWASP Top 10 and OWASP API Top 10 vulnerabilities, attack visibility, contextual risk scoring, and actionable remediation guidance. These capabilities shall be delivered either: Natively within the proposed platform, or Through tightly coupled integration with an enterprise-grade Runtime Application Self-Protection (RASP) or Application Security solution
504	Volume-2	Annexure-3, Clause 3.4.1.12 (6)	**102**	6) Application visibility using Deep Packet Inspection and also should provide visibility for known and custom applications along with SAAS based cloud applications.	Please clarify if Deep Packet Inspection (DPI) is mandatory under this requirement or if application visibility through flow records, SNMP counters, and system logs is acceptable. Our platform provides visibility into known, custom, and SaaS applications using flow and log-based telemetry. For full DPI capabilities, integration		Deep Packet Inspection (DPI) is mandatory under this requirement
505	Volume-2	Annexure-3, Clause 3.4.2.9 - Database Activity Monitoring (2)	**156**	The Solution should Provide SQL Response Time for Monitoring Custom Queries	Kindly clarify if direct SQL response time monitoring for custom queries is mandatory. Our solution monitors DB health, logs, blocking/deadlocks, replication, and performance counters. Native SQL query response time tracking is not supported, but integration with specialized DB monitoring tools can be explored if required.		direct SQL response time monitoring for custom queries is mandatory.
506	Volume-2	Annexure-3, Clause 3.4.2.9 - Database Activity Monitoring (3)	157	3) The Solution should provide response time Monitoring for custom queries through JDBC Mechanism to allow monitoring unsupported databases	Kindly clarify if JDBC-based response time monitoring for unsupported databases is mandatory. Our solution supports monitoring of DB metrics, health, and logs across multiple databases. JDBC-based custom query monitoring is not natively available but can be integrated via specialized DB monitoring solutions if required.		JDBC-based response time monitoring for unsupported databases is mandatory
507	Volume-2	Annexure-3, Clause 3.4.2.10 (5)	**159**	5) Bonus & Penalty: Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs. Support for Defining and Calculating service Bonuses based on clauses in SLAs	Kindly clarify if automated calculation of bonus is a mandatory requirement. Our solution natively supports SLA credit/penalty tracking, alerts, and reporting based on SLA clauses. However, bonus calculation workflows are generally handled at the commercial/contract management layer. Please confirm if		Automated calculation and reporting of SLA service credits and penalties based on defined SLA clauses shall be supported natively by the DAM solution.

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
508	Volume-2	Clause 5.11.2	**121**	MSI to operate & maintain hosting infra including **network monitoring**, event correlation, incident mgmt, SLA monitoring.	Please confirm the **scope split** between our EMS/NMS and any **existing OEM EMS** (e.g., for RAN, Core, DC). Do you expect **native** monitoring for all domains or **federation/integration** with existing tools?		GoSL does not have any existing EMS/ NMS etc. MSI will procure, supply, install, commission and test the various IT Components which includes Network and Security appliances as well. The
509	Volume-2	Clause 5.11.2	**121–129**	Server/virtual/storage operations activities tables	Can we **deploy host agents** on production servers/VMs where needed, or are there **agentless-only** zones? Any **bastion**/proxy constraints?		SLUDI infrastructure is a fresh deployment. Agent-based or agentless approaches for server, virtual, and storage operations may be proposed by the MSI, subject to compliance with security, performance, and
510	Volume-2	Clause 5.11.2 and Clause 5.12.4	**121, 141**	Automated SLA monitoring & reporting	Which **SLA definitions/KPIs** are in use today (availability, MTTR, latency, auth TPS, etc.) and their **authoritative sources** (NMS counters, APM, logs)?		Query not clear
511	Volume-2	Clause 5.11.2.11 and Clause 5.11.2.12	**132**	Event correlation and incident management called out	Do you already run a **correlation engine** (AIOps/SIEM/ITOM)? If yes, name/version and **integration pattern** (events in/out, dedup rules, identities).		Refer RFP 2 of 3 (Amended) and Annexure 3 - Minimum Technical Requirements (Amended) . Indicative BOQ is provided. The MSI has to propose the solution while meeting the RFP requirements and adhere to SLA
512	Volume-2	Clause 5.9.2 Table 29: Network Operations	**108–110**	Table 29: NOC operations	Please share the **NOC runbook**: current **thresholds**, **escalation matrix**, **ticketing categories** (P1/P2/P3), and **24x7 staffing** expectations.		NOC will be a de-novo implementation by the MSI. SLAs have to be met by the MSI. NOC runbook will be prepared by the MSI and approved by GoSL.
513	Volume-2	Clause 5.2.6	**54–56**	Network services & connectivity	Provide **L3/L2 inventories** (device make/model/OS), **SNMP versions** allowed (v1/v2c/v3), and **credentials strategy** (per device vs. shared/AAA).		The MSI has to propose the solution while meeting the RFP requirements and adhere to SLA & other requirements. It is once again made clear that GoSL will
514	Volume-2	Clause 5.11.2 and Clause 5.2.6	**121; 54–56**	Network monitoring responsibility	Is **ICMP** (for latency/jitter/loss) permitted across **all segments** (DC, DR, ministries, Internet edges)? Any **rate-limits** or **ACL** constraints?		The MSI has to propose the solution while meeting the RFP requirements and adhere to SLA
515	Volume-2	Clause 5.9.2	**108–110**	NOC operations and monitoring	Confirm **syslog & SNMP trap** architecture: central collectors in scope, **message volume/day**, **retention**, and **preferred severity**		Already answered in S.No. 512
516	Volume-2	Clause 5.1.3.1	**33–35**	Dashboards/reports/ad-hoc queries	Which **executive dashboards** are mandatory (weekly/monthly)? Please share sample **KPIs** and **report formats** for acceptance.		Requirement to be finalized at the time of implementation
517	Volume-2	Clause 5.11.2 (Change/Release/Patch Mgmt)	**121–134**	Release & patch mgmt part of O&M	Any **maintenance windows** and **freeze periods** (elections, fiscal closes)? Define **max outage** allowed for NMS/EMS upgrades.		Requirement to be finalized at the time of implementation
518	Volume-2	Clause 5.11.2 (API integrations) and Clause 5.1.7 (API gateway)	**121; 45–48**	API-first integrations	List **systems to integrate**: ITSM, CRM, SIEM/SOC, MOSIP telemetry, ABIS, IAM. Provide **API endpoints**, **auth method** (OAuth2, mTLS).		SLUDI system should be interoperable leveraging API and message based technologies. The Solution should be architected accordingly. Refer RFP Vol 2 of 3 and Annexure 3 - Minimum Tech requirement

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
519	Volume 2	Clause 5.11.2 (SLA & alerts) anc Clause 5.8.4 Support	**121; 97–105**	SLA alerts; helpdesk	For **auto-ticketing**, which **ITSM** is final (ServiceNow/Jira/Remedy)? Provide **incident templates**, **priority matrix**, and **routing rules**.		Already answered in S.No. 512
520	Volume 2	5.2.5 Server Services; 5.11.2 Ops tables	**53–55; 125–129**	Heterogeneous OS/virtual environments	Confirm **supported OS matrix** (Windows/Linux/Solaris/Unix), **hypervisors** (VMware/Hyper-V/KVM), and **versions** to monitor.		Already answered in S.No. 512
521	Volume 2	5.2.10 Virtual Environment Services	**58**	Virtual environment services	Do you expect **hypervisor-level** metrics via **vCenter/SCVMM** APIs and **guest OS** metrics both? Any **Air-gapped** clusters?		MSI to propose a solution based on RFP requirements and adhere to SLA requirements
522	Volume 2	5.2.8 Storage Services	**57–58**	Storage services	Please share **storage platforms** (NetApp/EMC/HPE/IBM), **mgmt APIs** available (REST/SMI-S/SNMP), and **multi-tenancy** expectations.		Already answered in S.No. 512
523	Volume 2	5.11.2 Ops & Admin (Backup/DR)	**121–131**	Backup/replication & RPO/RTO	Provide **RPO/RTO** targets for **NMS/EMS** themselves; confirm **DR topology** (active/active vs. active/standby) and **failover tests** cadence.		For RPO, RTO refer to RACI matrix : Annexure 16 . Please refer to 5.8.2.1
524	Volume 2	5.7 Performance Testing	**67–70**	Perf testing before Go-Live	Define **performance test goals** for NMS/EMS (events/sec, flows/sec, queries/min, dashboard concurrency) and **test data** availability.		Refer to Annexure 5: Demand capacity
525	Volume 2	5.8 Information Security	**73–85**	Security baseline, privacy by design	Confirm **on-prem only** hosting for NMS/EMS; list **network zones** (DMZ/Mgmt/Restricted), **mTLS/PKI** policy, **FIPS** cipher requirements.		on-prem only hosting for NMS/EMS. network zones (DMZ/Mgmt/Restricted) will be
526	Volume 2	5.11.2 (Config Mgmt)	**121–134**	Configuration & asset mgmt in O&M	Do you require **Golden-config templates**, **RMA workflows**, and **auto-reprovision** (firmware/config/licences) for replacements?		The NMS may optionally support the mentioned capabilities, which will be considered desirable
527	Volume 2	5.12.3 Incident & Issue Reporting	**140**	Incident and issue reporting	Share **report formats** (daily/weekly/monthly), **MTTA/MTTR** targets, and **KPI definitions** for NOC/EMS performance.		Already answered in S.No. 512
528	Volume 2	5.1.3.1 BI & Analytics; 5.12.5 Other Reports	**33–35; 141**	Scheduled & ad-hoc reporting	Who are **report consumers** (MoDE/DRP/ICTA)? Any **tri-language** reporting (Sinhala/Tamil/English) expectations?		Consumer - GoSL. Tri-language requirement will be decided at the time of implementation.
529	Volume 2	5.11.2 (Event Correlation)	**121–134**	Event correlation in Ops	Provide **noise-handling rules** (dedup, suppression, flapping windows), **P1/P2 policies**, and **business calendar** for SLA calc.		To be decided at the stage of implementation and further evolved during O&M
530	Volume 2	5.9.1 Security Operations; 5.9.2 NOC	**106–110**	SOC/NOC integration	Confirm **event sharing** between **NMS/EMS and SOC SIEM** (CEF/LEEF/JSON), and **who is source of truth** for major incidents.		The EDR, NDR, NMS, EMS, and APM solutions shall support event and alert forwarding to the SOC SIEM using industry-standard formats such as CEF, LEEF, or structured JSON, either natively or through supported integrations. For major security or operational incidents, the SOC SIEM shall be the system of record (source of

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
531	Volume 2	5.11.2 (Network Connectivity Mgmt)	**121–134**	Connectivity management & operations	Share **WAN topology** between DC/DR/field sites, **bandwidth**, **QoS policies**, **NAT/VPN** rules affecting telemetry collection.		Already answered in S.No. 512
532	Volume 2	5.6 Training & Capacity Building	**66**	Training plan and effectiveness	Define **user personas** (NOC L1/L2, EMS admins, DBAs, execs), **batch sizes**, **language** needs, and **UAT sign-off** criteria.		Refer Annexure 14 for List of Trainings. Batch size is limited to 10 per batch, for Techncial Training. It is further clarifed that for EO training three batches of
533	Volume 2	5.2.11 Container & OS Env Services	**59**	Container platform services	Should EMS/NMS **run containerized**? If yes, specify **K8s/OpenShift** versions, **ingress**, **persistent storage**, and **security context**.		Already answered in S.No. 512
534	Volume 2	5.11.2 (Patch/Change/Release Mgmt)	**121–134**	Patch & change mgmt	Confirm **CAB/CCB** process, **lead times**, **rollback policy**, **pre-prod** environments, and **blue/green** expectations.		Refer to 5.11.3.6 Change Control, RFP Volume 02 of 03
535	Volume 2	5.8.5 Support (Contact Center & Helpdesk)	**97–105**	Contact center & IT helpdesk	Confirm **auto-ticket** flow from EMS/NMS to **CRM/Helpdesk** (L1 triage), and whether **citizen-facing** issues must correlate to **NMS events**.		The EMS/NMS shall support automated ticket creation and updates in the CRM/Helpdesk for L1 triage, either natively or via integration. Where applicable, citizen-facing issues shall be correlated with NMS/EMS events to aid faster resolution.
536	Volume 2	5.2.3 Installation, Configuration & Testing	**52–53**	Install/config/testing responsibilities	Any **compliance hardening** (CIS benchmarks), **port whitelisting**, or **scan windows** we must comply with during rollout?		Deployments shall comply with SL-UDI security hardening, port-whitelisting, and approved scan/maintenance window policies, and with all applicable guidelines and provisions issued by the Government of Sri Lanka
537	Volume 2	5.1.7 Integration Middleware	**45–48**	API gateway & integration	Should we **publish northbound REST APIs** for partner systems (usage, rate limits, auth), and do you require a **developer portal**?		Requirements to be decided at the point of implementation
538	Volume 2	5.12.4 SLA Reporting	**141**	SLA reporting	Which **SLA views** are mandatory: **service-level**, **agency-level**, **site-level**, **device-level**, and **time-of-day** breakouts?		SLA are mandatory
539	Volume 2	5.2.10 Virtual Env Services; 5.2.8 Storage	**58; 57**	Virtual & storage services	Any **chargeback/showback** requirements for **resource usage** (compute/storage), to be surfaced in EMS dashboards?		The solution shall support showback for resource consumption visibility across compute and storage services.
540	Volume 2	5.7 Performance Testing	**67–70**	Performance & acceptance	What is the **expected daily event rate** (syslog+traps), **retention** (hot vs. cold), and **peak dashboards/users** for sizing?		GoSL will provided anonymised 1000 dummy dataset of all three modalities. MSI may use this dataset to create 8 million dummy records for performance

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
541	Volume 2	5.8 InfoSec; Annexure 2 NFR (referenced)	**73–85; Annexure**	Security, privacy, audit trails	Confirm **log retention** periods, **WORM**/immutability expectations, and **audit export** formats for regulator reviews.		All logs shall be retained in online for a minimum period of one (1) year, after which they shall be archived and retained permanently in accordance with GoSL policy. Archived logs shall support immutability (tamper-evident controls) to prevent unauthorized alteration or deletion and to meet audit, compliance, and
542	Volume 2	5.11.2; 5.12.1–5.12.5 Reporting	**121; 139–141**	ABIS/data quality/incident/SLA/other reports	Do you want **cross-correlation** (e.g., MOSIP auth errors vs. network faults) shown in **one executive report**? Share desired layout.		Cross correlation can be showed in one executive report.
543	Volume 2	5.2.6 Network Services	**54–56**	Network services	Provide **IPAM** details (addressing plan, subnets to scan, discovery windows), and whether **LLDP/CDP** discovery is permitted everywhere.		Already answered in S.No. 512
544	Volume 2	5.11.2 Ops	**121–134**	Ops responsibilities	For **RMA**: should EMS/NMS **auto-rehost config/firmware/licenses** to replacement devices and auto-update **NAC/Cert/NMS** entries?		The solution should preferably support RMA workflows where, upon replacement of a failed device, configuration, firmware, and licenses can be re-applied from centrally maintained
545	Volume 2	5.2.1 DC Site Setup; 5.2.2 Hosting Environments	**49–51**	DC/DR environments	Do you require **multi-DC active monitoring** with **HA** for NMS/EMS (clustering)? Define **failover RTO** for the tools themselves.		Requirements to be decided at the point of implementation
546	Volume 2	5.11.2 (Event correlation & incident)	**121–134**	Event correlation mentioned	Please provide **business calendars/holidays** that affect SLA calculations and **planned maintenance** exclusion policies.		Refer Annexure 9 : Service levels.
547	Volume 2	5.1.3.2 CRM	**34–36**	CRM integration	If citizen complaints are logged in CRM, should **relevant network/app telemetry** be **auto-linked** to tickets (context-enrichment)?		Yes. The solution should support context-enrichment of CRM tickets by linking relevant network and application telemetry from Network and Security Devices Such linkage shall be supported through secure, API-based integrations and may be automated or operator-assisted, based on defined correlation
548	NA	Generic	NA	Scope mentions integration with multiple existing monitoring, NOC, SOC, and ITSM tools.	Please share a full list (with versions) of all existing monitoring, observability, and ITSM tools that the APM solution must integrate		Already answered in S.No. 512
549	NA	Generic	NA	RFP covers multiple environments (Dev, UAT, Prod, DR) across data centers.	Please confirm the number of environments to be monitored, their physical/virtual location, and expected segregation of data.		Refer to 5.2.2 Hosting Environments , RFP Volume 02 of
550	NA	Generic	NA	RFP has strong SLA enforcement clauses.	Please confirm the SLA KPIs specific to APM monitoring (e.g., transaction latency thresholds, data freshness, alerting times) so		Refer to Annexure 9: Service levels
551	NA	Generic	NA	Multiple application types expected (Web, Mobile, Backend, API, DB, Container).	Please confirm the approximate count of each type in scope at Go-Live and expected growth in 3 years.		Requirments to be finalized at the time of implementation

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
552	NA	Generic	NA	Data retention and storage requirements for monitoring data are unclear.	Please confirm retention period for metrics, traces, logs, and whether raw or aggregated data storage is needed.		Data will be retained for a period of one year and thereafter archived. No data will be deleted/purged. The data
553	NA	Generic	NA	RFP demands security compliance (Data Protection Act, OWASP, etc.).	Please confirm if the APM platform must be independently audited/certified for security or if certification of the hosting environment is sufficient.		All items proposed should meet the required security standard. In addition, testing, including Security testing would be
554	NA	Generic	NA	RFP mentions integration with business KPI monitoring.	Please provide a list of business KPIs in scope for correlation with application performance data.		Query not clear
555	NA	Generic	NA	RFP lists predictive analytics.	Please confirm if AI/ML model training is expected to be done on-premises or if pre-trained vendor models are acceptable.		Already answered in S.No. 532
556	NA	Generic	NA	RFP scope covers API-based data exchange with multiple external systems.	Please confirm if any of these APIs are third-party paid services that we need to subscribe to or develop connectors for.		Bidders are expected to assess and propose the required APIs, integrations, and connectors, including identifying whether any such APIs are native, open, or third-party paid services, in order to meet the RFP requirements. Any dependency on third-party licensed or paid APIs, along with
557	NA	Generic	NA	RFP requires role-based access control (RBAC).	Please share the planned user roles and number of expected users per role in APM.		Refer Annexure 5 : Demand Capacity for users based on RBAC
558	NA	Generic	NA	Generic Query	Is the solution expected to be Active-Active and DR as well?		Refer to 5.8.2.1 Process/component wise
559	NA	Generic	NA	Generic Query	Is an Integration with LDAP Planned , if so , Name the type of Integration : OpenLDAP or AD or Open ID Connect Relay Protocol or IBM Directory Access Services ? Do you intend to use SSL for LDAP? Are there LDAP Failover Servers involved ? Do you intend to use		MSI to propose a solution based on RFP requirements and adhere to SLA requirements
560	NA	Generic	NA	Generic Query	How many Jobs would run on a daily basis on the Setup uniquely , count recursive jobs(running periodically) only once per day? Please provide a Breakup Environment wise for PROD , QA , DEV etc. ?(this		Jobs requirement to be finalized at the time of implementation. MSI to propose a solution based
561	NA	Generic	NA	Generic Query	HWA Lab Services team would conduct a Training of 40 hrs on the Product inclusive of Administration, Operations, Scheduling, is there		Already answered in S.No. 532
562	Volume-2	Bidding Document, SL-UDI Volume 2 of 3– Schedule of Requirements -21-28	NA	Generic Query	Is there an Integration with the SMS Server involved , if “YES” , Number of mail Server integrations? Type of Integration used(REST/SOAP/Message to messaging Service through SMTP)?		SMS gateway will be provided by GoSL. MSI to integrate.
563	NA	Generic	NA	Generic Query	Data retention period must comply with The National Records and Archive Authority - What's the number of days/months expected		Query not clear
564	Volume-2	Clause 5.1.3.1	**33–35**	Dashboards/reports/ad-hoc queries	Which **executive dashboards** are mandatory (weekly/monthly)? Please share sample **KPIs** and **report formats** for acceptance. Please confirm that PoE telemetry (per-port power usage) is		Executive dashboard and KPI - Already answered in S.No. 516. Refer to Amended Volume 02 of
565				General Queries	Number of users will use the DevOps Tool, Please confirm		MSI to propose a solution based on RFP requirements and adhere
566	Volume-2	Annexure-3, Clause 3.3.3.17 (General)	66	Clause 3.3.3.17 -Email Solution (General)	Please provide additional details like How Many Users will use Email Solution, What is the mode of access, How many Deployments, HA in DC and Single DR or HA in DC and DR. Deployment Details		Requirement of Email Solution has been dropped

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
567	Volume-2	Annexure-3, Clause 3.3.3.17 (General)	66	Clause 3.3.3.17 -Email Solution (General)	No mention has been made for Email on Mobile Devices. Does that need to considered. Also How many Mobile Devices.		Already answered in S.No. 566
568	Volume-2	Annexure-3, Clause 3.3.3.17 (3)	66	3) The email solution shall provide MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server	MAPI is an deprecated protocol. Can we provide our OEM supported Thick Client and also provide integration with MS Outlook if needed.		Already answered in S.No. 566
569	Volume-2	Annexure-3, Clause 3.3.3.17 (5)	66	It shall be able to provide access to the Mail server via IMAP (Internet Message Access Protocol) clients and POP (Post Office Protocol) clients, with the option to	Can we propose our own OEM supported Thick Client which will provide more secure access to mail rather than relying on Less Secure Protocols like IMAP / SMTP / POP3		Already answered in S.No. 566
570	Volume-2	Annexure-3, Clause 3.3.3.2 (5)	36	5) The portal should have the capability to integrate with enterprise document management system and Content	Do we assume that DMS and CMS will be provided or do we need to provide the same.		Refer Annexure 3- Minimum Tech Requirement, the specifications for DMS is provided there. MSI
571	Volume-2	Annexure-3, Clause 3.3.3.2	36	Portal Solution	Can you explain the actual usage and who will use the Portal. Is it for the Intranet or accessible from Intranet and Internet. Is it for the for the Citizens or for Internal Employee and Partner usage only.		Primary users of Portal would be citizens. However, it should be accessible from both Intranet and Internet.The portal design / workflow would be firmed up at
572	Volume-2	Annexure-3, Clause 3.3.3.3		Mobile Application	For Mobile Application what end user platform to consider will it be PWA or Native Mobile Application on iOS / Android.		Application should ensure compatibility with platforms such as Android and iOS.Kindly refer
573	NA	General	NA	Generic Query	Describe the intended primary deployment environment for the solution's servers. Is it On Premises/Private cloud		On premise.
574	NA	General	NA	Generic Query	Mail clustering required for mail file failover and load balancing in		Email soultion is dropped
575	NA	General	NA	Generic Query	Mail clustering required for mail file failover and load balancing in DR or Single Instance in DR / Passive DR, please confirm		Email soultion is dropped
576	NA	General	NA	Generic Query	High Availability needed for Mobile Devices in DC, please confirm		Refer to 5.8.2.1 Process/component wise
577	NA	General	NA	Generic Query	High Availability needed for Mobile Devices in DR, please confirm		Refer to 5.8.2.1 Process/component wise
578	NA	General	NA	Generic Query	Describe the primary use case for the traditional deployment: for instant Public Website (primarily anonymous, cacheable traffic) / Internal Employee Portal (primarily authenticated, dynamic traffic)		Query not clear
579	NA	General	NA	Generic Query	What is the anticipated volume of content and assets? In GB/TB please verify approx value		Query not clear. However, refer to Demand capacity : Annexure 5
580	NA	General	NA	Generic Query	Specify choice of DB Platform for Portal, Is DB2, Oracle, SQL or open source.		Prefereably : Open source with enterprise support. Final choice
581	NA	General	NA	Generic Query	Describe the intended primary deployment environment for the solution's servers. Is it On Premises/Private cloud		On premise.
582	NA	General	NA	Generic Query	What is the total number of named users (total accounts)		refer to Demand capacity :
583	NA	General	NA	Generic Query	Please provide a breakdown of this user base: Internal Employees: External Partners/Contractors: Public Customers (Authenticated): Public Customers (Anonymous):		refer to Demand capacity : Annexure 5
584	NA	General	NA	Generic Query	Describe the anticipated peak usage patterns (e.g., "9:00 AM - 10:00 AM Eastern Time," "End-of-quarter reporting," "Post-		Query not clear
585	Volume-2	Annexure 3, Clause 3.4.1.4 (15)	86	15) Solution shall consider rack awareness and failure domains while implementing	Please remove this clause **Justification** The object storage rack includes multiple PDUs to ensure redundancy and maintain failure domain isolation. Placing each node in a separate rack would significantly increase the rack		Already answered in S.No. 1

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
586	Volume-2	Annexure-3, Clause 3.4.1.4 (20)	86	20) Nodes shall be placed with Rack awareness	Please remove this clause **Justification** Object Storage RACK has multiple PDU for redundency and maitin failure domain.		Already answered in S.No. 1
587	Volume-2	Annexure-3, Clause 3.4.1.5 (8)	87	8) The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% availability with built-in redundancy and dynamic drive protection.	Please change it to "The proposed array shall have no single point of failure, with fully redundant and hot-swappable components. It must support non-disruptive hardware replacement, firmware upgrades, and guarantee 100% Data availability with built-in redundancy and dynamic drive protection." **Justification** 100% Data Availability ensures that data will be available for reading and writing. This guarantee is backed by integrated data		Already answered in S.No. 3
588	Volume-2	Annexure-3, Clause 3.4.1.5 (20)	89	20) The proposed storage solution should support snapshot capabilities, ensuring efficient data protection and recovery. It must include the necessary software licenses	Please change it to "The proposed storage solution should support snapshot capabilities upto 1000 snapshot per volume, ensuring efficient data protection and recovery. It must include the necessary software licenses" **Justification** Supporting large number of snapshot (up to 1000 per volume) supports finer-grained data recovery, enabling quicker restoration		Already answered in S.No. 4
589	Volume-2	Annexure-3, Clause 3.4.3.23 (32)	259	32) The solution must support log collection and retention.	What is the duration (in months/years) that logs should be retained?		Already answered in S.No. 373
590	Volume-2	Annexure-3, Clause 3.4.3.23	256	N/A	What is the number of endpoints to be considered for the solution? Please confirm		Already answered in S.No. 374
591	Volume-2	Annexure-3, Clause 3.4.3.15 (12)	233	12) Support hot swappable (1+1) field replaceable redundant power supply and fan module	While field replaceable power supplies are generlly available for the requested VPN gateway spec size, field replaceable fans are included in higher models, which will result in a much higher cost.		Already answered in S.No. 375
592	Volume-2	Annexure-3, Clause 3.4.3.15 (26)	235	26) Support for VRRP, QoS and full OSPF routing protocol.	VRRP is an open standard protocol used to provide high availability and fault tolerance for the solution. If the proposed solution includes it's own method to provide high availablity clustering		Already answered in S.No. 430
593	Volume-2	Annexure-3, Clause 3.4.3.17 (33)	241	33) All the proposed threat functions like IPS/vulnerability protection, Antivirus, C&C protection etc. should work in isolated environment without any need to connect	Threat protection functions such as IPS/vulnerability protection, Antivirus, C&C protection etc., require updates to be received on the firewall through the Internet to provide effective protection. Therefore, Is it acceptable to for the firewall to receive		Already answered in S.No. 377
594	Volume-2	Annexure-3, Clause 3.4.3.21 (3)	251	3) Solution should support multitenancy and provide a clear Architecture for function in multitenant environment.	Is it sufficient for the solution to support multitenant environment or should the solution include the required licensing to deploy a multitenant architecture? If licenses are required to be included, please provide following		Already answered in S.No. 378
595	Volume-2	Annexure-3, Clause 3.4.3.21 (36)	254	36) The proposed solution must allow case or task assignment in relation to a ticket or an incident to other team members or group.	Please indicate the number of users (analysts) that licensing should be included for with the provided solution. - Number of users will full access (read/write permissions) - Number of users with audit access (read-only permissions)		Already answered in S.No. 379
596	Volume-2	Annexure-3, Clause 3.4.3.21 (29)	254	29) Retaining the data of all multiple runs of SOAR playbooks ensure the retention of key artifacts especially with dynamic information such as threat	This clause refers to threat reputation information. Would like to know whether or not threat intel licenses should be included with the SOAR platform?		Already answered in S.No. 33
597	Volume-2	Annexure-3, Clause 3.4.3.21 (33)	254	33) The proposed solution must have ability to store attachment as part of the user manual workflow or as part of the automated playbook.	What is the required retention period for incidents?		Already answered in S.No. 381

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
598	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. b. Reports eligible for reference must be published within the last 3 years, i.e. calendar year 2021, 2022 and 2023	Requesting a change in the clause as Analyst like Gartner, Forester etc do not publish quadrants for mature technologies and deprecate the quadrants from time to time. With few product quadrants not been updated since last 7-8 years for products like IPS, GSLB, ADC, Rack Server, Blade Server etc. Thus requesting the following change ""Product Benchmarking: a. The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, AV Test, SE Labs for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory. In case quadrant are depreciated or not updated, alternate reputed analyst report to be provided along with 2 large deployment		Already answered in S.No. 41
599	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	3	Product Benchmarking: d. the Vendor has to mandatorily provide at least 2 case studies of similar complexity, sensitivity and scale where the proposed product is successfully implemented and is in operations for at least last two years i.e. calendar year 2022 and 2023. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario	Requesting a change in the clause as there no many similar projects rolled out. "d. the Vendor has to mandatorily provide at least 2 case studies of ~~similar~~ complex~~ity~~, Large scale, sensitivity and scale where the proposed product is successfully implemented and is in operations ~~for at least last two one years~~ ~~i.e. calendar year 2022 and 2023~~. The case study should provide i) name of the client ii) description of the solution iii) scale of the solution in terms of size, number of transactions, data and users being handled iv) details of the scenario		Already answered in S.No. 42
600	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.2	4	Product Benchmarking: e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of similar complexity and dimension where the proposed product is successfully implemented and has been in operation for at least two years as on March 2024. The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms of	Requesting a change in the clause as there no many similar projects rolled out. " e. In case Gartner Quadrant / Forrester Wave / IDC MarketScape report (for the product or product category) does not exist for a specific product or product category, the vendor must mandatory provide at least 1 case studies of ~~similar complexity~~ complex and ~~dimension~~ large scale where the proposed product is successfully implemented and has been in operation ~~for at least two years as on March 2024.~~ The case study should provide i) name of the customer ii) description of the solution iii) dimension of the solution in terms		Already answered in S.No. 43
601	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 1	204 of 361	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance.	There are a lot vendors who can offers DDoS Service over other solution like firewall, UTM, Load balancer, WAF or Application delivery Appliance. The problem with these appliances are these devices are stateful, meaning they track connections — which makes them vulnerable to state exhaustion attacks, a common DDoS tactic and become target itself rather protecting customers. The Solution should not limit on the attack concurrent session. Suggested Clause: The Proposed appliance should be a Dedicated appliance (NOT a part of or a service over Router,UTM, Application Delivery Controller,Proxy based architecture or any StateFul Appliance).		Already answered in S.No. 55

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
602	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.10 Anti-Distributed Denial of Service (DDoS) with High Availability Clause 6	204 of 361	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 4000 SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key.	HTTPS DDoS attacks are on the rise, with recent trends showing a sharp increase in frequency and complexity. These attacks target encrypted traffic, making them harder to detect and mitigate using traditional methods. The solution must offer robust capacity, advanced TLS inspection, and application-layer protection. Scalability and high bandwidth are critical to effectively absorb and neutralize modern HTTPS-based DDoS threats. The proposed solution must be capable of handling high-volume encrypted traffic without decrypting the SSL packet thereby reducing the latency. Suggested Clause : SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have 40K SSL CPS/TPS (1TPS = 1 CPS) with 2048 bit Key, with a Hardware based Acceleration card. Appliance should also support TLS 1.3 PFS Hardware Acceleration support along with RSA support. The Appliance should also support		Already answered in S.No. 55
603	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 10	242 of 361	Throughput minimum 30 Gbps from day 1 with scalability to upto 100Gbps without changing the hardware appliance	We request team to lower down the requirement a little to accommodate right filt solution with compliance and allow participation. Suggested Clause: Throughput minimum 30 Gbps from day 1 with scalability to upto 90Gbps without changing the hardware appliance		Already answered in S.No. 46
604	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 15	243 of 361	SSL throughput 2 GBPs	SSL throughput is not aligned with overall throughput. Hence, we request to align with the overall solution. Suggested Clause: SSL throughput 10 Gbps scalable to 20Gbps.		Already answered in S.No. 47
605	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.18 Web Application Firewall (WAF) with High Availability Clause 22	243 of 361	Compliance Certificates – RoHS, Compliant EU directive 2011/65/EU CE LVD EN 60950-1, CB-IEC60950-1, CCC, CTUVus CE EMC EU directive 2004/108/EC, FCCart 15B class A, ICES-003, VCCI, C-tick	The certificate mentioned are old certificate, we request to generalize this clause. Suggested Clause : Compliance Certificates – RoHS, Compliant EU, EN 60950-1, KCC, TUV FCC etc		Already answered in S.no. 48

SL No	Volume	Section	Page-Number	Original content from RFP	Queries	Justification (if any) (potential bidders)	Response (NISG)
606	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 11	116 of 361	Solution should have NVGRE and VXLAN Support	GRE is not very relevant for the solution like Load Balancers. Hence, we request to kindly relax this clause. Suggested Clause : Solution should have VXLAN and VLAN Support.		Already answered in S.No. 49
607	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 12	116 of 361	Should have IPv6 Support for SLB, interfaces, routing, and firewalling	L4 Firewall is a different solution asked in the RFP. Some of the Firewall vendors does offer Load balancing but it is not a integral part of Load Balancer. Hence we request to relax this clause : Suggested Clause : Should have IPv6 Support for SLB, interfaces, routing.		Already answered in S.No. 50
608	BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.1.17 Server Load Balancer Clause 14	116 of 361	The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Host f. Host Domain	This clause is restricting leading OEM from participation due to specific terminology.Request you to generalize the clause. Suggested Clause: The solution should supports the following load balancing methods: a. Round-Robin b. Weighted Round-Robin c. Least Connections d. Fastest Response e. Hash, f. Bandwidth, etc		Already answered in S.No. 51

RESPONSE TO QUERIES SET 3 OF NISG RFP NISG/SLUDI-2025

Response / Clarifications related to (a) SLUDI Project Components / Tech Stacks and (b) Changes / Clarifications on Specifications on SLUDI Project Tech Stack

A	**Product Benchmarking**	All components / stacks proposed by the MSI should meet the Product Benchmarking Requirements as specified in Sec 3.2, Annexure -3 Min Tech Requirements
B	**Clarifications Suggestions on Specifications on SLUDI products / componets**	All clarifications / suggestions / changes provided in respect to specifications to the various items through 'Response to Query Set 1, Set 2 & Query Set 3' and in subsequent clarification(s), if issued would be deemed relevant. The bidder can propose equivalent or higher specification to meet the RFP & SLA requirements.

Sl.No.	RFP Volume	Original Query Refernce#	Section	Page No.	Content of RFP Requires Clarification	Query	NISG Response
1	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3	3.2 Product Benchmarking	3	c. In case less than 4 distinct products that meet the solution, requirements are available in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Wave of Forrester Wave or Leader in IDC MarketScape, the vendor may offer products from the next category of these analyst reports, i.e. Challengers Quadrant of Gartner Magic Quadrant or Strong Performers Wave of Forrester Wave or Major Players in IDC MarketScape.	For the project management tool, can we propose an enterprise solution that is not listed as a Gartner or Forrester Leader, but meets all compliance requirements? This would be a TCS IP, Jile that has been successfully implemented in projects with similar complexity and scale, such as Sri Lanka UDI.	Yes, the MSI can propose a solution that is not listed as a Gartner or Forrester leader. The proposed tool should be open source with enterprise support. Refer Product Benchmarking, Sec 3.2, Annexure 3. It should have the option to allow GoSL to use this tool beyond the contract period with community support or purchase enterprise support
2	SL-UDI-Vol-2-of-Vol-3-protected_130126.		5.8.5.2 Deployment of Infrastructure for IT helpdesk	99	(ii) MSI shall be required to provide and maintain all IT required for successful operations of the IT helpdesk including, but not limited to, the following: c. Network Connectivity between IT helpdesk and DC, and IT helpdesk and DR	As per Annexure-16- RACI Matrix_130126, pg 4, SL. No 12 , the responsibility of Network Connectivity between IT helpdesk and DC, and IT helpdesk and DR lies with GoSL. Kindly remove this from MSI's SoW and ammend the clause.	Refer RFP Volume 2 of 3, Section 5.8.5.2 Deployment of Infrastructure for IT helpdesk, Item number (i) h – LAN connectivity – stands deleted. MSI will be responsible setting up of LAN Connectivity. RACI stays unchanged Network connectivity will be provided by GoSL, however, MSI will be responsible for integrating the network with the ITSM
3	SL-UDI-Vol-2-of-Vol-3-protected_130126.		5.8.5.4 Set up IT Infrastructure for Helpdesk Operations	100	MSI shall arrange for the associated hardware, software, and **network components** for operationalizing the IT Help Desk.	5.8.5.2 Deployment of Infrastructure for IT helpdesk, pg 99, states (i) GoSL will provide physical space for the IT helpdesk along with necessary IT, Electrical and Physical Infrastructure as follows: h. LAN connectivity As per above network components viz LAN Switches and LAN cabling will be provided by GoSL. Kindly remove network components from this clause.	GoSL will provide the network connectivity, however, all associated hardware such as Router, LAN Switches will be provided by MSI and LAN cabling will done by the MSI as well
4	Annexuure-3-minimum tech_130126		,3.4.3.19 Network Intrusion Detection System/ Intrusion Prevention System (NIPSIDS/IPS) with High Availability	244	Sl. No. 3, Minimum 50 Gbps with 8x10G and 8X100G interfaces at MZ and DMZ Zone	Kindly clarify whether NIPS is separately required for MZ and DMZ or same NIPS will be deployed for MZ and DMZ both.	MSI to propose solution as per the RFP
5	Response to query set-1, Sl. No 215.			39	Response (From NISG) The SL UDI system does not host heavy public-facing web applications that require application acceleration or SSL offload. The platform already uses an API Gateway and standard L7 load balancing, which provide the necessary routing and security. An ADC like F5 or Citrix would duplicate these functions and add unnecessary cost and complexity. **Therefore, a dedicated application delivery controller is not required for the UDI project.**	As per Annexuure-3-minimum tech_130126 , pg 115, 3.4.1.17 Server Load Balancer requirement is still mentioned. Please clarify whether this appliance is required to be quoted by the MSI or not as it conflicts with the response to queries. Kindly confirm.	Yes, Server Load Balancer is required however, clarification to the the specification as mentioned " Platform should provide application acceleration, reducing load on websites/Application and performing load balancing as well as other features (SSL offload, proxy/reverse proxy, content routing, L4/L7 firewalling and more)" was provided.
6	Response to query set-1, Sl. No 344.			69	Response (From NISG) All networking equipmemt at NOC, SOC will be provided by GoSL. However, routing networking equipment will be provided by MSI.	Kindly confirm whether GoSL will be providing the Routers at NOC, SOC, Helpdesk along with the WAN links?	Routers at NOC, SOC, Helpdesk will be provided by the MSI

7	Response to query Set 1		Query # 660		Performance testing environment is required. will be needed.	Query # 127 states that Performance testing shall be done in Production environment. This statement is contradictory to the referenced query response. Please allow MSI to use Production or Staging environment for Performance testing instead of provisioning a separate environment.	Refer RFP Vol 2 of 3, Sec 5.2.2 where the details of the environment required are mentioned. MSI will perform performance testing as per details provided in RFP Vol 2 of 3 Sec 5.7.1
8	Volume - 1		4.12.11	100	MS-Office	How many MS-Office licenses/subscriptions required and for how many years	All laptops and Desktops should be preloaded with basic MS Office (having MS Word, Excel and Powerpoint)
9	Volume - 2		7	160	Mobile Registration KITS	there are 15 line items given against the mobile registration kits. Do we need to supply all the items separately or can consider one integrated biometric enrolment kit having all the enrolment components complied with MOSIP ? Please confirm.	Refer Schedule of Requirements , Mobile registration KITS Page 156 (amended RFP Volume 02 of 03) for details.
10	Volume - 2		5	20	21. The proposed services/modules offered/interfaced to/with the public (eService interfaces) should be available in tri-languages (Sinhala, Tamil, and English).	As per MOSIP team, **the pilot was conducted using only the English language in Sri Lanka. Since the default MOSIP transliteration engine does not support Sinhala, Sinhala transliteration would need to be implemented as a country-specific customization.** Please confirm the transliteration libraries/tools required for sinhala language would be provided by GoSL to incorporate/customize MOSIP. In case, if it is a MOSIP core customization (L3) then it needs to be done MOSIP Engineering team as per the below RFP reference. 5.11.3.3 MOSIP Support (i)MSI shall be responsible for the first level and second level (L1 and L2) maintenance and management of the MOSIP application suite. (ii)MOSIP will provide maintenance and management support of MOSIP application suite at OEM Level which can be utilized by MSI on a need basis. MSI to work with MOSIP in regard to this. (iii)The process for escalation of support tickets will be specified in consultation with the GoSL. Please help with the clarification on the above.	Query Answered. Refer Response to Query Set 1, item no. 64.
11	Annexuure-3-minimum tech_130126		3.2	5	Messaging Platform - Publish/Subscribe Queues	This requirement has been dropped in the revised RFP shared. But MOSIP uses AMQ and Kafka for pub/sub messages & queues. In this case, Can we consider opensource community edition of Kafka & AMQ for MOSIP?. Please clarify.	All project components/tech stacks required for successful Project delivery should meet the Product Benchmarking as provided in Sec 3.2, Annexure 3
12	Response to query Set 2	Response to query Set 2	Query 30	5	The requirement is hereby clarified that the APT solution shall support a minimum effective throughput of 1 Gbps with all threat prevention features enabled, including IPS, anti-malware, sandboxing, and SSL/TLS inspection. The proposed solution must meet this	As per Volume 02 of 03 – Annexure 3: Minimum Technical Specifications, Section 3.4.3.2 (Anti-Advanced Persistent Threat), point no. 3, a minimum throughput of 30 Gbps is required. However, in the query response, it is mentioned that the minimum required throughput is 1 Gbps, which is contradictory. Request clarification.	All clarifications / suggestions / changes provided in respect to specifications to the various items through 'Response to Query Set 1 and Set 2' would be deemed relevant. The bidder can propose equivalent or higher specification to meet the RFP & SLA requirements.
13	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	Volume 02 of 03 - Annexure 3: Minimum Technical Specification	3.4.3.11 Security Information and Event Monitoring (SIEM) with High Availability	209	1.The solution should offer a single view of all the data captured from devices across all sites and the SIEM solution should be consistent in Gartner's Leaders Quadrant across last 5 years (2019-2024)	Please modify the clause "The solution should offer a single view of all the data captured from devices across all sites and the SIEM solution should be in Gartner's Leaders Quadrant in last 5 years"	The SIEM should meet the product requirements as laid down in Product Benchmarking, Annexure 3, Section 3.2
14	Response to query Set 2	Response to query Set 2	Query 34	5	Requirement of NDR is dropped.	As per the query response, the requirement for NDR has been dropped. However, in Volume 02 of 03 – Annexure 3: Minimum Technical Specifications, NDR is still listed as a compliance item. Please confirm whether NDR is required or not.	Requirement of NDR is not dropped.
15	Response to query Set 2	Response to query Set 2	Query 556		2022-2025	As per Query Response Set 1, the product cited must be in the Leaders Quadrant of Gartner Magic Quadrant, or the Leaders Quadrant of Forrester Wave, or a Leader in IDC MarketScape for their respective product categories. Submission of the relevant section of the analysis report along with the technical proposal is mandatory. The query response specifies that eligible reports must be published between 2022–2025. However, the RFP mentions the period as 2021–2024. This discrepancy is contradictory. Request clarification	Relevant years 2021 to 2024. Kindly refer Sec 3.2, Annexure -3

16	Annexure 3		3.2	3	The product cited must be in the Leaders Quadrant of Gartner Magic Quadrant or Leaders Quadrant of Forrester Wave or Leader in IDC MarketScape, for their product categories. Submission of a copy of the relevant section of the analysis report with the technical proposal is mandatory.	Is it acceptable to propose a product that isn't listed by Gartner or Forrester but has been used in projects of comparable complexity/ scale?	All project components/tech stacks required for successful Project delivery should meet the Product Benchmarking requirements as provided in Sec 3.2, Annexure 3
17	Annex 3 Technical Specifications		Page 288, 3.4.3.30 SOC / NOC – Monitor		There is a contridication between query and Technical specs, whether Monitor to be proposed or removed		As per RFP Vol 2, Sec 7- Schedule of Requirements and Annexure 3 - MinimumTech Requirements
18	Annex 3 Technical Specifications		Page No. 83 Point No.2		Blade enclosure should support all Intel or AMD latest-generation processors	Request you to mention either Intel or AMD so that there will be a fair comparision between the bidders. Since there is a commercial difference between Intel and AMD processor	Answered in earlier queries. No Response
19	Response to Query set 2		SL.No.11		Laptops for NOC/SOC resources Dropped	Please clarify whether its dropped ? Because Section 3.4.3.29 is still available in Annex 3 Technical specifications	Laptops are not required for NOC/SOC
20	Response to Query set 2		SL.No.13		IP Phones & IP PABX (SOC) Dropped	Please clarify whether its dropped ? Because Section 3.4.3.32 and 3.4.3.33 are still available in Annex 3 Technical specifications	IP Phones & IP PABX (SOC) are Dropped.
21	Response to Query set 1		3.4.3.5 Web Gateway with High Availability		2000 users for endpoints	We are seeing ambiguity in the user count . At few places we see as 2000 and at demand capacity is asked for 6000 and few other places we are seeing as 4000. Request to give us a firm clarity on the user count.	Please refer to Annexure 5 : Demand Capacity for user count
22	Response to Query set 2, Serial No. 30		3.4.3.2 Anti-Advanced Persistent Threat (APT) with High Availability		• Kindly clarify the basis or criteria used to derive the stated 1 Gbps throughput specification•	in Volume 2 of 3 Annex 3 - Technical spec document, still the value is shown as 30 Gbps. Kinldy give a clarity on the throughput spec	All clarifications / suggestions / changes provided in respect to specifications to the various items through 'Response to Query Set 1 and Set 2' would be deemed relevant. The bidder can propose equivalent or higher specification to meet the RFP & SLA requirements.
23	General		IDAM			How many useres to be created on Identity and Access Management system mentioned in Technical spec 3.4.3.8	Please refer to Annexure 5 : Demand Capacity
24	General		Mandatory Conditions		All Servers and Network devices shall be connected with 25GbE or higher.	For the requirement of SLUDI 10 Gig connectivity is more than sufficient. Also it can be achieved using Copper Interface. Once we plan for 25GbE overall sizing of all the hardware will be very high and the overall cost also will escalate. 25GbE can be acieved only using Optical (Fiber) Interfaces. Request to downsize this to 10 Gbps to have overall project cost under control	Clause remains unchanged
25	3.4.3.11 Security Information and Event Monitoring (SIEM) with High Availability				The solution must provide a field extraction wizard that is used to create parsers and allow testing and validation with existing live or historical data within the system from the web interface. Old data should be parsed with new parser without re-ingesting or re-indexing the data.	This is vendor specific please remove this	The requirement is functional and outcome-based, and does not mandate any specific vendor feature or implementation approach Equivalent mechanisms that achieve the same functional objective would be considered..
26	Annexuure-3-minimum tech_130126		3.5.2	299 - 329	Specifications for the components for Field infrastructure are different from the Mobile Enrollment Kit.	Can The secondary screen for Field infrastructure be same as the one considered for Mobile registration kit?	As per RFP
27	Annexuure-3-minimum tech_130126		3.5.2.7 #9	323	Scan Resolution - Minimum 300 dpi with TWAIN driver	Can TWAIN Drivers be eliminated? Since OCR is not required	No change
28	Annexuure-3-minimum tech_130126		3.5.2.7 #14	324	Light - LED Ring Light	Can Block light be considered instead of ring light? Ring Light is not suitable for Mobile registration kits due to its size constraints if not, can the Ring light be provided in a separate backpack?	No change
29	Annexure-10		10.2	36 & 38	Biometric – Implementation and Integration Engineer Manager - Biometric Job Descriptions • Actively implement Mass Communication programs as well as targeted communication programs to inform Residents of the processes and procedures for authentication and e-KYC	Please confirm if we have to provision any mass communication solution to meet the JD requirements. Please mention the frequency of the communication, volume and channels of communication	This will be decided in consultation with GoSL

30	Vol 2		5.3.1	59	Authentication Devices Authentication Devices should be from 3 different OEMs	only 100 devices each are required for authentication, Can the same be from a single OEM? 3 OEM for each device will require development of 9 SBIs and provisioning for 9 different models on the Device Management Server	Refer response to query set-1, item no. 654
31	Volume 02 of 03 - Annexure 3: Minimum Technical Specification		Section 3.4.1.1 Blade Servers	79	Blade server should be quoted with minimum 1024 1TB memory, expandable up to 8TB, 4800/5600 MHz DDR4/DDR5 DIMMS	Request you to change this clause to "Blade server should be quoted with minimum 1024 GB (1TB) memory, expandable to 6 TB or higher, 4800/5600 MHz DDR4/DDR5 DIMMS" Justification: This change would help in reducing the Total Cost of Ownership (TCO), while not affecting the performance. Currently from design standpoint the maximum memory that is generally deployed per server is 2 TB, with scalability of 6TB, there is head room for another 4 TB RAM extra per server depending on the CPU make selected. Currently the Spec does not allow a major CPU Vendor to participate in the RFP. With the requested change, in addition to allowing additional OEM, the solution can be designed such a way that the total number of servers can be reduced by about 40% to 50%. As a result, costs for software licenses (Hypervisor & Operating system), network switches, space, power, and cooling are lowered, which decreases the overall total cost of ownership (TCO).	1. Agreed. 2. CPU Clock Speed must be 2.7 GHz or Higher and must support hyperthreading (minimum 2 threads per core) and virtualization.
32	Volume 02 of 03 - Annexure 3: Minimum Technical Specification		Section 3.4.1.2 Blade Servers	81	Memory (RAM): Min. 1024 GB scalable up to 8TB of Memory with DDR5 memory DIMMS	Request you to change this clause to " Memory (RAM) Min. 1024 GB scalable up to 6 TB of Memory with DDR5 memory DIMMS" Justification: This change would help in reducing the Total Cost of Ownership (TCO), while not affecting the performance. Currently from design standpoint the maximum memory that is generally deployed per server is 2 TB, with scalability of 6TB, there is head room for another 4 TB RAM extra per server depending on the CPU make selected. Currently the Spec does not allow a major CPU Vendor to participate in the RFP. With the requested change, in addition to allowing additional OEM, the solution can be designed such a way that the total number of servers can be reduced by about 40% to 50%. As a result, costs for software licenses (Hypervisor & Operating system), network switches, space, power, and cooling are lowered, which decreases the overall total cost of ownership (TCO).	1. Agreed. 2. CPU Clock Speed must be 2.7 GHz or Higher and must support hyperthreading (minimum 2 threads per core) and virtualization.
33	Volume 02 of 03 - Annexure 3: Minimum Technical Specification		Section 3.6.2.2 Blade Server	347	Blade server should be quoted with minimum 512 GB memory, expandable up to 8TB, 4800/5600 MHz DDR4/DDR5 DIMMS and should support RAS features and memory mirroring	Request you to change this clause to "Blade server should be quoted with minimum 1024 GB (1TB) memory, expandable to 6 TB or higher, 4800/5600 MHz DDR4/DDR5 DIMMS" Justification: This change would help in reducing the Total Cost of Ownership (TCO), while not affecting the performance. Currently from design standpoint the maximum memory that is generally deployed per server is 2 TB, with scalability of 6TB, there is head room for another 4 TB RAM extra per server depending on the CPU make selected. Currently the Spec does not allow a major CPU Vendor to participate in the RFP. With the requested change, in addition to allowing additional OEM, the solution can be designed such a way that the total number of servers can be reduced by about 40% to 50%. As a result, costs for software licenses (Hypervisor & Operating system), network switches, space, power, and cooling are lowered, which decreases the overall total cost of ownership (TCO).	1. Agreed. 2. CPU Clock Speed must be 2.7 GHz or Higher and must support hyperthreading (minimum 2 threads per core) and virtualization.

34	Volume 02 of 03 - Annexure 3: Minimum Technical Specification		Section 3.6.2.3 Rack Server	349	Memory (RAM): Min. 512 GB scalable up to 8TB of Memory with DDR5 memory DIMMS	Request you to change this clause to "Memory (RAM): Min. 512 GB scalable up to 6 TB of Memory with DDR5 memory DIMMS" Justification: This change would help in reducing the Total Cost of Ownership (TCO), while not affecting the performance. Currently from design standpoint the maximum memory that is generally deployed per server is 2 TB, with scalability of 6TB, there is head room for another 4 TB RAM extra per server depending on the CPU make selected. Currently the Spec does not allow a major CPU Vendor to participate in the RFP. With the requested change, in addition to allowing additional OEM, the solution can be designed such a way that the total number of servers can be reduced by about 40% to 50%. As a result, costs for software licenses (Hypervisor & Operating system), network switches, space, power, and cooling are lowered, which decreases the overall total cost of ownership (TCO).	1. Agreed. 2. CPU Clock Speed must be 2.7 GHz or Higher and must support hyperthreading (minimum 2 threads per core) and virtualization.
35	Annexuure-3-minimum tech_130126		3.5.2.8	327	Management server: Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of SLUDI. The communication protocols between the MDS and the Management Server can be decided by the respective device provider. Such communication should be restricted to the above specified interactions only. No transactional information should be sent to this server	As per MOSIP specification as well as the technical requirement it is mentioned that the HSM for device management should be separate. Ideally it should be a separate one from the SLUDI HSM to prevent any kind of breach of Biometric data. However, the queries response mentions usage of shared HSM. Please confirm wether a sepatrate HSM is required for Device Management or not?	Responded in Query Set 1, Sl No. 79 & 464
36	Volume-2		Table 13: Volume of Biometric Capturing Device	62	Table 13: Volume of Biometric Capturing Device Note : MSI is required to provide the Virtual Device Manager (VDM) along with the biometric capture devices.	The Term VDM is not a MOSIP term. MOSIP refers to MOSIP Device Service (MDS) Please confirm that with VDM you are referring to MOSIP Device Service (MDS)	The term VDM may be understood as MOSIP Device Service (MDS) and should comply with MOSIP MDS specifications.
37	Vol 02		5.1.1 Table 6	31	Table shows Release_1 and Release_2 application lists including MOSIP apps + ABIS + support apps	For BI/Analytics, the RFP prefers open-source with enterprise support. Please confirm if GoSL has any preferred products/standards (PowerBI, Superset, Metabase, etc.) or MSI can propose freely.	Refer Sec 3.2, Annexure -3, Product Benchmarking
38	Vol 02		5.11.3 (Operations & Maintenance & Administration)	28-29	Operations include Network Monitoring, Security Management, Event Correlation, Incident Management, Patch Management, etc.	Centralized logging requirement is mentioned. Please confirm expected stack.	Refer RFP Vol, Sec 7 and Annexure3 - Min Tech Requirement. The proposed solution should meet RFP requirements and SLAs
39	Vol 02		5.1.7 Integration Overview	45-47	MSI should integrate MOSIP with other applications and security solutions.	Please confirm if GoSL expects an API Gateway product (e.g., Kong / Apigee / WSO2) and whether MSI must propose it.	Refer RFP Vol, Sec 7 and Annexure3 - Min Tech Requirement. The proposed solution should meet RFP requirements and SLAs
40	Vol 02		5.1.6 Solution Testing	43		During the O&M phase, vulnerability assessment and penetration testing will need to be conducted on a quarterly basis.	Refer Response to query Set 1, Sl No. 106
41	Vol 02		5.1.6 UAT Section 5.7	44		UAT testing will be carried out on datasets of 50,000 anonymized biometric data provided by GoSL + performance testing in both DC and DR	Refer Response to query Set 1, Sl No. 717
42	Vol 02		5.1.3.2 Customer Relationship Management	34	Customer Relationship Management	Please clarify on CRM System. For proposal, Should we propose COTS CRM with customization or Fully custom-developed CRM Open-source with enterprise support?	Refer RFP Vol 2, Section 5.1.3 where list of COTS products have been mentioned. Further peruse 5.1.3.2
43	Vol 02		5.1.3.1 Business Intelligence and Analytics	33	RFP states "preferably open-source solution along with Enterprise support"	Business Intelligence. Please clarify on if we can propose commercial BI tools Or strictly open-source only ?	Refer Sec 3.2, Annexure -3, Product Benchmarking. Bidder is at liberty to propose proprietary or Open Source Product. Preference is for Open Source with Enterprise Support
44	Vol 02		5.1.3.3 Document Management System (DMS)	35	Document Management System	Document Management System. Please clarify, Is DMS expected to be: COTS with customization or Fully custom-developed Open-source with support?	Refer RFP Vol 2, Section 5.1.3 where list of COTS products have been mentioned. Further peruse 5.1.3.3
45	Vol 02		5.1.4.4 Knowledge Management System	38	Knowledge Management System	Please clarify, Should KMS and LMS be Integrated single platform or Separate systems?	Bidder to propose either integrated or separate system. However, it should be interoperable and the functional needs should be met
46	Vol 02		5.7.1 Performance Testing	65	Performance Testing	Please clarify on Performance Test Data Volume. For benchmarking, how much data should be loaded?	Refer Response to Query Set 1, Sl No. 717

47	Vol 02		5.10.2.7 Payment Gateway	115	The MSI will be responsible for integration of the SL-UDI software system with multiple paymentgateways.	Please clarify on Payment Gateway. How many payment gateways to integrate? Are gateways already contracted by GoSL?	Refer Response to Query Set 1, Sl No. 735 and 740
48	Vol 02		5 Scope of Services	20	The MSI should integrate the foundation ID platform with Automated Biometric Identification Systems(ABIS), Card Printing Services, Biometric-SDK, Biometric devices, Device Management Services,HSM, Studio Application (ICAO Pics) , and COTS, etc.	Please clarify on ICAO Photo Studio Integration. Is this system already deployed? MSI responsibility is to only receive photos via API or Full integration with photo system?	Supply and integrate the photo system
49	Volume-1		SECTION IV, 4.4.2 Key Personnel Details	66	Summarize professional experience as specified in section **3.2.5.2**, in reverse chronological order. Indicate particular technical and managerial experience relevant to the project.	No Clause found in the tender document as 3.2.5.2	Refer Annexure 10- Manpower Requirements.
50	Volume-2		Annexure 10, Clause 10.2 Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Project Director)	6	**Key Professional Staff**: Project Director **Academic & Professional:** MBA/ME/M-Tech/BE/B-Tech or Equivalent Certifications: **Certification in Project Management (PMP, or Prince2 and related)** **Minimum Overall Experience**:20 years **Specific Qualifications / Requirements:** Experience in handling at least 5 (five) technology-led end-to- end projects of similar scale (scope, timeline, and budget) and out of this at least 1 (one) project should be in government sector. Experience of managing a portfolio of projects, and experience of periodic interaction with C-level of the organization **Experience of working in a multi-cultural and diverse environment in at least 3 countries.**	We Request 1) The Certifications requirements of "Certification in Project Management (PMP, or Prince2 and related)" may be considered as non-mandatory. 2) The Minimum Overall Experience maybe relaxed to **15 years**. 3) The experience in atleast **"one"** country may be accepted in place of **"three"** Countries	No Change
51	Volume-2		Annexure 10, Clause 10.1 Table 1: Key Professionals (Key Professional Staff: Technical Project Manager)	3	**Key Professional Staff:** Technical Project Manager **Deployment (Implementation Phase**): Full-Time Onsite	Full time onsite deployment during Implementation Phase is not required for Technical Project Manager as he/she shall work closely with the offshore project team as well. Hence, we request this requirement may be changed to "**onsite on-need basis**"	No Change
52	Volume-2		Annexure 10, Clause 10.2 Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Technical Project Manager)	7	**Key Professional Staff:** Technical Project Manager **Academic & Professional:** MBA/ME/M-Tech/BE/B-Tech or equivalent **Certifications:** **Desired – SCRUM Master** **Other Certification (PMP or Prince2) in Project Management**	We Request to kindly remove the certification requirement as specific experience is already asked regarding national identity project which itself satisfies the capability of the Key Professional Staff.	No Change

53	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Support and Operations Manager)	8	**Key Professional Staff**: Support and Operations Manager **Academic & Professional**: MTech / ME/B-Tech/BE or equivalent **Certifications: ITIL (Desired)** **Specific Qualifications/ Requirements**: Experience of at least 3 (three) technology-led projects as support manager role in a project of similar scale (scope, timeline, and budget) Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project in the government sector Experience in managing operations, maintenance, and support (L1, L2 and L3) aspects during O&M phase of a large project with multiple OEMs, ecosystem partners, sub-contractors, etc. **Experience is mandatory in a similar capacity on (a) biometric based projects, (b) DevSecOps, (c) Cloud Infrastructure, (d) Network and Security, and (e) Change Management**	We Request 1) Kindly remove the certification requirement as Support and Operations manager may have various other experience. In case SME support will be required against any specific technology/process, the same will be provided to Support and Operations Manager as per need basis.	Refer Response to Query Set 2, Sl No. 74. Certification ITIL is desired and not mandatory
54	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Chief Architect)	9 -10	**Key Professional Staff:** Chief Architect **Academic & Professiona**l: MS / MTech / ME / MCA/BE/B-Tech or equivalent **Certifications (Desired): TOGAF** **Specific Qualifications/ Requirements:** Experience in designing enterprise architecture for at least 3 (three) large scale technology-led projects of similar scale (scope, timeline, and budget) and out of this at least 1 (one) project should be in the government sector. **Experience is mandatory in a similar capacity on (a) biometric based projects, (b) DevSecOps, (c) Cloud Infrastructure, (d) Network and Security, (e) microservices, (f) enterprise architecture, server architecture, network architecture, database architecture, security architecture, deployment architecture etc.** Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	We Request to 1)Kindly remove the certification requirement as specific experience is already asked regarding National Identity Project which itself satisfies the capability of the Key Professional Staff. 2) Kindly remove "Experience is mandatory in a similar capacity on (a) biometric based projects, (b) DevSecOps, (c) Cloud Infrastructure, (d) Network and Security, (e) microservices, (f) enterprise architecture, server architecture, network architecture, database architecture, security architecture, deployment architecture etc." In case SME support will be required against any specific technology/process, the same will be provided to concerned Key Professional Staff as per need basis.	1. Certification is desired. 2. Refer Response to Query Set 2, Sl No. 73 and 74

55	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Software Architect (Application Architect))	10-11	**Key Professional Staff:** Software Architect (Application Architect) **Minimum Overall Experience:** 12 years **Specific Qualifications/ Requirements:** Experience in designing solution/application architecture for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) **Experience is mandatory in a similar capacity on (a) biometric based projects, (b) Agile methodology, (c) DevSecOps, (d) Microservices architecture, (e) software architecture (Docker based deployment, Hybrid Mobile Application Development, etc.), (f) integration architecture, and (g) quality engineering** Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable	We request to 1) The Minimum Overall Experience maybe relaxed to **8 years**. 2) Kindly remove "Experience is mandatory in a similar capacity on (a) biometric based projects, (b) Agile methodology, (c) DevSecOps, (d) Microservices architecture, (e) software architecture (Docker based deployment, Hybrid Mobile Application Development, etc.), (f) integration architecture, and (g) quality engineering" as specific experience is already asked regarding national identity project which itself satisfies the capability of the Key Professional Staff. In case SME support will be required against any specific technology/process, the same will be provided to concerned Key Professional Staff as per need basis.	1. No Chamge in minimum number of years of experience. 2. Refer response provided above
56	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Security and Network Architect)	11 - 13	**Key Professional Staff**: Security and Network Architect **Minimum Overall Experience:**12 years **Specific Qualifications / Requirements-** Experience in designing security architecture for at least 5 (give) large scale technology-led projects. **Experience is mandatory on** **(a) Biometric based projects,** **(b) DevSecOps,** **(c) establishing and managing security operation center,** **(d) governance, risk, and compliance,** **(e) authentication and authorization standard,** **(f) Information security products design and deployment and (g) business continuity planning** **Experience is mandatory in information technology security design, operations, encryption, information access, biometric security, and authentication processes.** Relevant experience in managing and reviewing the configuration of security devices and solutions such as IAM, DLP, WAF, firewall etc. **Experience of projects with ISO 27001 and ISO 22301 compliances** **Experience of National Identity project is mandatory**	We request to 1) Kindly change "Experience is mandatory on (a) Biometric based projects, (b) DevSecOps, (c) establishing and managing security operation center, (d) governance, risk, and compliance, (e) authentication and authorization standard, (f) Information security products design and deployment and (g) business continuity planning" to **"Experience is mandatory on** **(c) establishing and managing security operation center,** **(d) governance, risk, and compliance,** **(f) Information security products design and deployment and experience is desirable on** **(a) Biometric based projects,** **(b) DevSecOps,** **(e) authentication and authorization standard,** **and (g) business continuity planning".** 2) Kindly change "Experience is mandatory in information technology security design, operations, encryption, information access, biometric security, and authentication processes." to "**Experience is desirable in information technology security design, operations, encryption, information access, biometric security, and authentication processes.**" 3) Kindly change " Experience of projects with ISO 27001 and ISO 22301 compliances" to "**Experience is desirable of projects with ISO 27001 and ISO 22301 compliances**" 4)Kindly change "Experience of National Identity project is mandatory"	Refer Response to Query Set 2. Sl No. 73

57	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Infrastructure & Systems Architect)	14	**Key Professional Staff:** Infrastructure & Systems Architect **Academic & Professional:** MS / MTech / ME / MCA / BTech / BE or equivalent **Certifications: Cloud Architect (Desired)** **Minimum Overall Experience:** 12 years	We request 1) Kindly remove the certification requirement. 2) The Minimum Overall Experience maybe relaxed to **8 years**.	No Change
58	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Database Architect)	14 - 15	**Key Professional Staff:** Database Architect **Minimum Overall Experience:** 12 years **Academic & Professional:** MS / MTech / ME / MCA / BTech / BE or equivalent **Certifications: DBA (Desired)** Specific Qualifications / Requirements- Experience in designing database architecture for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) **Experience is mandatory in a similar capacity on (a) biometric based projects, (b) relational and non-relational database, (c) clustering and replication, (d) backup and restoration, (e) database optimization and tuning, (f) disaster recovery, (g) space management** **Experience in the architecture and design of population scale databases** **Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable**	We request to 1) Kindly remove the certification requirement. 2) The Minimum Overall Experience maybe relaxed to 8 years. 3) Kindly change " Experience is mandatory in a similar capacity on (a) biometric based projects, (b) relational and non-relational database, (c) clustering and replication, (d) backup and restoration, (e)database optimization and tuning, (f) disaster recovery, (g) space management" to **"Experience is desirable in a similar capacity on (a) biometric based projects, (b) relational and non-relational database, (c) clustering and replication, (d) backup and restoration, (e)database optimization and tuning, (f) disaster recovery, (g) space management"** 4) Kindly change "Experience of National Identity project is mandatory Experience or Knowledge of MOSIP is desirable" to "**Experience of National Identity project is desirable Experience or Knowledge of MOSIP is desirable.**"	No Change.
59	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Team Lead –UI/UX)	17	**Key Professional Staff**: Team Lead –UI/UX **Minimum Overall Experience**: 10 years	We request to 1) The Minimum Overall Experience maybe relaxed to **5 years.**	No Change
60	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Team Lead – Business Analyst)	18	**Key Professional Staff :** Team Lead – Business Analyst **Academic & Professional:** MBA / MS / MTech / ME / MCA / BE /BTech / BCA or equivalent **Certification: IIBA, PBA, CSPO** **Minimum Overall Experience:**10 years	We request to 1) Kindly remove the certification requirement. 2) The Minimum Overall Experience may be relaxed to **5 years**.	No Change

61	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Team Lead – Training and Certification)	20	**Key Professional Staff :** Team Lead – Training and Certification **Specific Qualifications/ Requirements:** Experience in leading the training as a master trainer under the train the trainer approach for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) out of which at least 1 (one) project should be in the government sector Experience of the establishing a certification program for a large-scale project **Should be able to fluently read and speak local languages (Sinhalese and Tamil) as well as English**	Due to requirement of multi-lingual capability, this requirement is very specific and can be fulfilled through sourcing the suitable Team Lead – Training and Certification on short-term/contractual or outsourcing basis in place of full-time employee. In this case CV of the Team Lead – Training and Certification can be shared once the contract is awarded to us. Kindly Approve.	No Change
62	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Data Centre Manager)	24 - 26	**Key Professional Staff :** Data Centre Manager **Specific Qualifications / Requirements:** **Note – This profile should be from the data center co-location provider in Sri Lanka.** Experience in leading the data center and/or cloud infrastructure tracks for at least 2 (two) large scale technology-led projects of similar scale (scope, timeline, and budget) Experience of Data Center for large scale technology-led projects in the government sector Experience in following is mandatory in a similar capacity (a) At least 5 years of experience as a Data Center Manager, managing all aspects of large infrastructure projects (b) At least 3 years of experience in the operations of data center in a highly scalable manner (c) Experience in the supervision and administration of DC infrastructure operations Experience in the design and management of structured cabling infrastructures and in-depth knowledge of cable distribution systems and industry standards	Since the Data Center Manager profile is to be provided by the data center co-location provider in Sri Lanka and does not fall under MSI's responsibility, we request the removal of the Data Center Manager profile from RFP to avoid any ambiguity during submission.	Refer Response to Query Set 1, Sl No. 204
63	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Track Lead – Systems Engineering)	26	**Key Professional Staff :** Track Lead – Systems Engineering **Minimum Overall Experience:** 10 years	We request 1) The Minimum Overall Experience maybe relaxed to **8 years**.	No Change

64	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Track Lead - Application Manager)	28	**Key Professional Staff :** Track Lead - Application Manager **Minimum Overall Experience:** 10 years	We request 1) The Minimum Overall Experience maybe relaxed to **8 years**.	No Change
65	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Infrastructure Engineer)	31	**Key Professional Staff :** Infrastructure Engineer **Academic & Professional:** BE / BTech / MSc / MCA / MTech or equivalent Certifications: ITIL or equivalent	We request to remove certification requirements	Refer Response to Query Set 2. Sl No. 70
66	Volume-3		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff : Infrastructure Engineer)	32	**Key Professional Staff :** Network Engineer **Academic & Professional:** BE / BTech / MSc / MCA / MTech or equivalent Certifications: CCNP	We request to make certification requirment non-mandatroy	Refer Response to Query Set 2. Sl No. 71
67	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: CRM Engineer)	33 - 34	**Key Professional Staff:** CRM Engineer	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	No Change. Profile to be submitted in the proposal
68			Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: IT Helpdesk Agents)	41	**Key Professional Staff:** Business Analysts	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	No Change

69	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: IT Helpdesk Agents)	42	**Key Professional Staff:** IT Helpdesk Agents	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	Refer Response to Query Set 2. Sl No. 66. Profile to be siubmitted in the proposal
70	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: NOC Agent)	43	**Key Professional Staff:** NOC Agent	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	Refer Response to Query Set 2. Sl No. 67. Profile to be submitted in the proposal
71	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: SOC Agent)	43	**Key Professional Staff:** SOC Agent	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	Refer Response to Query Set 2. Sl No. 68. Profile to be siubmitted in the proposal
72	Volume-2		Annexure 10, Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff (Key Professional Staff: Administrators (Server, Network, Storage, Database))	43 - 44	**Key Professional Staff:** Administrators (Server, Net	This profile requirement can be fulfilled through sourcing the suitable on short-term/contractual or outsourcing basis in place of full-time employee. Kindly approve for submssion of CV at later stage and not during technical submission.	No Change. Profile to be submitted in the proposal

73	Volume-2		Annexure 10, Clause 10.1 Table 1: Key Professionals (Key Professional Staff: Track Lead – Enrolment and Authentication) & Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff	4	**Key Professional Staff:** Track Lead – Enrolment and	Clause 10.2, Table 2: Minimum Qualifications of Key Professional Staff does not have the details for Track Lead – Enrolment and Authentication. Kindly provide the Minimum Qualification Criteria.	Minimum of 10 years of IT experience with at least 5 years in large-scale digital identity or biometric authentication systems, including leadership of enrolment, de-duplication, ABIS integration, and authentication platforms in national or state-level e-governance projects.
74	Volume-1		4.4 Key Personnel Details and CV Template	64	Bidders should provide the names of at least two candidates qualified to meet the specified requirements for each position. The data on their experience should be supplied on separate sheets using one form for each candidate.	As the project responsibility rest with bidder, the placement of suitable candidate on work profile will be ensured by Bidder. In this case it is requested to remove the necessity of submission for alternative names/CV for the Key roles specified in RFP and allow to submit only single CV against each role.	No Change in clause
75	Volume-2		General COTS Clarifications	33 - 34	The MSI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of Data Analytics and Business Intelligence Solution for SL-UDI Information System. The MSI shall enable the system to provide comprehensive monitoring of enrolment and authentication through Business Intelligence (Dashboards and reports) and Analytics.	1. Preferred Vendors: Is there a list of recommended or pre-approved COTS vendors for CRM, DMS, KMS etc or are we free to choose based on our experience and research? 2. Licensing Clarification: What are the acceptable licensing models (e.g., perpetual vs. subscription) for each COTS solution? 3. Integration APIs: Are there existing standards or APIs that MSI must conform to when integrating BI, CRM, IAM with other SL-UDI modules?	All the COTS products required for the solution as mentioned in the RFP have to be provided by MSI. Bidder is at liberty to propose the COTS while meeting Product Benchmarking requirements as specified in n Annexure 3 - Min Tech Requirements
76	Volume-2		Customer Relationship Management (CRM) Clause 5.1.3.2 Customer Relationship Management Clause 5.8.4 Support (Contact Center and Helpdesk) 5.8.4.1 Contact Center Setup and Administration (iv), (v) Clause 5.8.4.7 Key features of the proposed Contact Center, Table 24: key features of the proposed Contact Center	34 - 35 97 - 102	(iv)GoSL will be required to provide necessary IT (Hardware, Software, Network) and Non- IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialer, Telephones, Headsets, etc.). (v)MSI will be responsible for supplying and implementing Customer Relationship Management (CRM) software to support Contact Center Agents / GoSL Officials at the Contact Center. Features The Contact Center should include mechanism of calls, email, chat, chatbot, voice over IP (VoIP) and website support.	1. Integration endpoints: What external systems does the CRM need to integrate with (e.g., Contact Center telephony system, Helpdesk, MOSIP APIs)? Are there preferred integration mechanisms (REST/SOAP)? 2. Customisation extent: What is the expected level of customization for CRM—just UI/UX and workflows, or deeper functional development (custom modules, automations)? 3. Call center integration: Will the MSI be required to integrate the CRM with any IVR/ACD system for telephony support? If yes, please specify vendor/technology.	1. Refer Response to Query Set 1, Sl Nos. 630, 87

77	Volume-2		Clause 5.1.3.3 Document Management System (DMS)	35 - 36	The function of the Document Management Software is to handle file sharing, creation, manipulation, and storage. Documents would be indexed using various unique numbers (internal and external)	1. Document lifecycle: What types of documents (e.g., scanned forms, biometric captures, audit logs) will be stored in the DMS? Any specific classification or retention policies? 2. Volume and scale: Can you share the estimated volume (number of documents, average size) for the DMS? Will it store documents for the entire SL-UDI program lifecycle (20 years)? 3. Open-source tools: Is there a preference for any open-source DMS solution (e.g., Alfresco, Nuxeo, OpenKM)?	Refer Response to Query Set 1, Sl Nos, 28, 85, 90, 614, 616.
78	Volume-2		Clause 5.1.4.4 Knowledge Management System (iii)	38 - 39	(iii) The Knowledge Management System must be designed in a flexible manner so that additional categorization fields can be added in future, as and when required. Also, the system should be able to handle knowledge of any form, including different subjects, structures, and media.	1. LMS user base: What is the expected number of trainees and training modules in LMS? Will this be for DRP/government staff only or also external users? 2. Multilingual content: Should the LMS and Knowledge Management systems support Sinhala, Tamil, and English content natively?	1. Refer Response to Query Set 1, SL No. 36 and 121. Reference may also be made to RFP Vol 2 or 3, Sec 5.6. Further reference may be made to Annxure 14 - List of Indicative Trainings. 2. Refer Response to Query Set 1, Sl No. 66, & 720 (3).
79	Volume 2		Annexure 3, Clause 3.4.2.8 Application Performance Management(APM) and Full Stack Observability	142	Requirement for mobile application monitoring, including Real User Monitoring (RUM) and variation analysis by device, OS, carrier, etc.	Please confirm the number of mobile applications (iOS/Android) to be monitored.	Refer RFP 2 of 3 for Mobile Applications
80	Volume-2		Annexure 9, Clause 9.5 Service Levels for Biometric Solution	13-15	False Positive Identification Rate (FPIR) False Negative Identification Rate (FNIR) False Match Rate (FMR) False Non-Match Rate (FNMR) Response Time per De-duplication check Fine tuning of Biometric Solution	We understand that SLA measurement tool for the BSP will be provided by the customer, required to measure the Accuracy (FNIR/FPIR,FMR etc. mentioned in SLA) or MSI need to consider it as part of proposal. Please confirm.	Customer would not provide SLA measurement tool for the BSP. The MSI has to priovision for tool and mechanism for measurement of accuracy (FNIR/FMR etc).
81	Volume-3		SECTION VII, Clause 20	27	20.1 Appendix 3 (List of Approved Sub-Contractors) to the Contract specifies critical items of supply or services and a list of Sub- Contractors for each item that are considered acceptable by the Employer. If no Sub-Contractors are listed for an item, the Contractor shall prepare a list of Sub Contractors it considers qualified and wishes to be added to the list for such items, with the approval of the Employer. 20.2 The Contractor may from time to time propose additions to or deletions from any such list, only with the written concurrence of the Employer. Provided that the Contractor shall take steps to ensure and satisfy the Employer that a Sub-Contractor sought to be replaced would meet the same or equivalent expertise & experience of the Sub-Contractor being replaced. The Contractor shall submit any such list or any modification to the list to the Employer for its approval in sufficient time so as not to impede the progress of work on the System. The Employer shall not withhold such approval unreasonably, unless the Employer is not satisfied with the Sub-contractor. Such approval by the Employer of a Sub-Contractor(s) shall not relieve the Contractor from any of its obligations, duties, or responsibilities under the Contract. The Contractor shall not engage any Sub Contractor to which the Employer has objected in writing.	As Biometric Solution Provider (BSP) experience was required for pre-qualification, we had initially declared the sub-contractor for "Automated Biometric Identification System Solution" during the submission of pre-qualification bid. As per the Clause 20 of Volume-3, we understood that we can add more sub-contractors. Kindly Confirm if our understanding is correct? If yes, what are the documents required to declare the sub-contractors at TQ stage.	As per RFP

82	Vol-2		BIDDING DOCUMENT – SCHEDULE OF REQUIREMENTS Volume 02 of 03 1.6 Targeted Performance Parameters (Throughput , Accuracy, Availability, Integration	9	The SL-UDI should be designed considering the 20-year scale (2025 – 2045) i.e., population size of 33 million citizens. (Refer Annexure 5: Demand Capacity)	We request you kindly to confirm and clarify below points:- **A. Project duration vs. hardware lifecycle** The Project Term in the RFP is 4 years. Please confirm whether the MSI is expected to design, size and supply hardware/infrastructure to support a 20-year scale as noted in the RFP. Designing and supplying hardware to physically last 20 years is neither industry standard nor cost-effective (typical enterprise server/network refresh cycles are 5–7 years). If the intent is long-term scalability, please confirm whether NISG will accept: · *hardware supply sized for the contractual term (4 years) with documented capacity headroom and documented scaling paths (hot spare pools, cluster expansion, or cloud bursting), and* · *an option/obligation for periodic hardware refresh or capacity top-up after year 4 under a separate renewal/AMCschedule.* **B. Definition of "30 million unique records"** For sizing calculation of "30M unique records", please confirm NISG's definition: Option A: 30 million people (person-level unique identities) (each person may have multiple biometric modalities but counted once), or Option B: 30 million biometric records (each capture — e.g., fingerprints + face + iris per person — counted separately). Clarification is critical because Option B materially increases storage/compute/indexing requirements. Kindly confirm the above so MSI can submit an accurate, defensible hardware & cost proposal.	Refer answered in Response to Query Set 1 in Sl Nos 45, 707, 709
83	Vol-1		4.12.12 TABLE 9: ABIS Deduplication Services	101	Payment will be made monthly based on a successful de-duplication transaction that generates total SL-UDI in a single month until coverage of the "Target Population" is achieved. Thereafter, every month, the new registrations and deduplication transactions till the end of the contract period.	Kindly confirm whether the "Target Population" refers to: **The total population as of the effective date of the project, or the 30 million biometric records referenced in the RFP (for ABIS sizing and cost evaluation).** This clarification is essential to accurately size the system, estimate storage and compute requirements, and align the payment milestones and O&M activities with the intended coverage	Refer answered in Response to Query Set 1 in Sl No 707, 709
84	Response to query set-1		3.4.3.9 Hardware Security Module (HSM) with High Availability	95 and 15	Query no. 464- Total Three - 1 HSM that can be partitioned. 1 backup HSM. 1 for the authentication Query no. 79- HSM is not required seperatetly for the BSP setup. Common HSM cannot be leveraged for the whole setup.	The responses appear to be contradictory. Kindly clarify whether a separate HSM for Authentication/BSP is required.	Refer answered in Response to Query Set 1 in Sl No 79
85	Annexuure-3-minimum tech_130126		3.5.2.8	327	Management server: Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of SLUDI. The communication protocols between the MDS and the Management Server can be decided by the respective device provider. Such communication should be restricted to the above specified interactions only. No transactional information should be sent to this server	As per MOSIP specification as well as the technical requirement it is mentioned that the HSM for device management should be separate. Ideally it should be a separate one from the SLUDI HSM to prevent any kind of breach of Biometric data. However, the queries response mentions usage of shared HSM. Please confirm wether a sepatrate HSM is required for Device Management or not?	Refer answered in Response to Query Set 1 in Sl No 79
86	Annexuure-3-minimum tech_130126		3.5.2.8	327	Management server: Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration of the device with the Management Server. The Management Server is created and hosted by the device provider outside of SLUDI. The communication protocols between the MDS and the Management Server can be decided by the respective device provider. Such communication should be restricted to the above specified interactions only. No transactional information should be sent to this server	As per MOSIP specification as well as the technical requirement it is mentioned that the HSM for device management should be separate. Ideally it should be a separate one from the SLUDI HSM to prevent any kind of breach of Biometric data. However, the queries response mentions usage of shared HSM. Please confirm wether a sepatrate HSM is required for Device Management or not?	Refer answered in Response to Query Set 1 in Sl Nos 10, 11, 464, 465, 531, 666

87	Annexure-11, Volume-2	Decurity – Digital	46-48	The SL-UDI solution shall incorporate digital signing and certificate-based security mechanisms aligned to national standards and PKI policies.	As per the RFP requirements, most critical transactions are based on Public Key Infrastructure (PKI) and digital signature mechanisms. Integration of digital signatures across multiple solutions within the UID ecosystem is complex and critical. In such a scenario, switching the Certificate Authority (CA) within a short time frame poses significant operational and security challenges. Furthermore, digital certificates are issued with specific validity periods, which would require the regular renewal of approximately 5,000 certificates. This adds to administrative overhead and long-term maintenance challenges. To mitigate these issues and ensure long-term operational stability, we strongly recommend incorporating an in-house digital signature issuance infrastructure as part of the proposed solution. This approach would provide greater flexibility, reduce dependency on external CAs, and enable better control over certificate lifecycle management. Over and above this confirmation on whether a national Root CA/PKI service will be made available for SL-UDI. Additionally, please provide guidance on the required signing algorithms, key sizes, certificate policies, and any mandated certificate issuance workflows for system-generated documents and transactions. We request confirmation for Mandatory requirement of Own CA solution	The requirement for PKI is dropped. Query answered in Response to Query Set 1, Sl No. 742

C Further/ Revised Clarifications on - Amendment to "Response to Queries Set 1", Sl No.749, 750, 751, 752,753, 754 & 755

Sl No	Original Query Refernce#	Original Content from RFP	Queries	Justification	Amended Response
749	External Firewall	Firewall should support client-based ~~SSL/TLS as well as~~ IPSec VPN Tunnels.	Firewall should support client-based SSL/TLS or IPSec VPN Tunnels.	Since SSL/TLS has many vanuribilities in recent days vendors are moving to more secure protocal like IPSec for tunnel creation	The firewall shall support client-based VPN tunnels using TLS 1.2 or TLS 1.3 (preferred) and IPSec, with TLS configured using secure, industry-standard protocols and ciphers, implemented in accordance with OEM specifications, ISO/IEC 27001, and NIST guidelines.
750	External Firewall	Minimum Concurrent Sessions with Layer 7 NGFW and Application control enabled: 5Million (if as per bidder architecture they require more capacity they should plan for it)	Minimum Concurrent Sessions- 5Million	Since connection establishment occurs at Layer 4, concurrent session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The NGFW solution shall support a minimum of 5 million concurrent Layer-4 sessions and shall support Layer-7 NGFW and Application Control features at this session scale, in accordance with OEM-published specifications, sizing tools, and supported architecture.
751	External Firewall	Minimum New Connections per Second with Layer 7 NGFW and Application control enabled: 200K (if as per bidder architecture they require more capacity they should plan for it)	Minimum New Connections per Second- 200K	Since connection establishment occurs at Layer 4, New session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The NGFW solution shall support a minimum of 200,000 new Layer-4 connections per second (CPS). Layer-7 NGFW and Application Control features shall be supported at this connection rate in accordance with OEM-published specifications, sizing guidelines, and supported architecture.
752	Internal Firewall	The firewall appliance should not include any wireless, Bluetooth, or infrared interfaces or tunnelling mechanisms that allow unauthorized access. Each appliance must be equipped with redundant and hot-swappable power supplies, ~~fan modules/trays,~~ SSDs, and interface slots.	The firewall appliance should not include any wireless, Bluetooth, or infrared interfaces or tunneling mechanisms that allow unauthorized access. Each appliance must be equipped with redundant and hot-swappable power supplies and storage (SSDs).	Hardware redundancy implementation varies by firewall platform design. In many enterprise-grade appliances, cooling components and interface ports are designed as fixed or chassis-level elements while still meeting high availability and reliability requirements. Mandating hot-swappable fan modules and interface slots makes the requirement vendor-specific and may exclude compact, high-performance platforms that achieve redundancy through alternate architectural designs. Retaining redundancy requirements for critical components such as power supplies and storage sufficiently meets availability objectives.	The firewall appliance shall not include any wireless, Bluetooth, or infrared interfaces or tunneling mechanisms that allow unauthorized access. Each appliance shall be equipped with redundant and hot-swappable power supplies and storage (SSDs). Fan modules and interface slots shall be designed to meet high availability requirements in accordance with the OEM-supported architecture.

753	Internal Firewall	Minimum Concurrent Sessions with Layer 7 NGFW and Application contron enabled: 15Million (if as per bidder architecture they require more capacity they should plan for it)	Minimum Concurrent Sessions- 15Million	Since connection establishment occurs at Layer 4, concurrent session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The NGFW solution shall support a minimum of 15 million concurrent Layer-4 sessions and shall support Layer-7 NGFW and Application Control features at this session scale, in accordance with OEM-published specifications, sizing tools, and supported architecture.
754	Internal Firewall	Minimum new Connections per Second with Layer 7 NGFW and Application control enabled: 300K (if as per bidder architecture they require more capacity they should plan for it)	Minimum New Connections per Second- 300K	Since connection establishment occurs at Layer 4, New session capacity is fundamentally a Layer-4 performance metric driven by session architecture and platform resources. Requiring Layer-7 NGFW and application control enablement for this metric creates a vendor-specific condition, as among Gartner Magic Quadrant Leaders, only one vendor explicitly publishes this parameter with mandatory Layer-7 inspection in its datasheet, potentially limiting equitable comparison across vendors.	The NGFW solution shall support a minimum of 300,000 new Layer-4 connections per second (CPS). Layer-7 NGFW and Application Control features shall be supported at this connection rate in accordance with OEM-published specifications, sizing guidelines, and supported architecture.
755	Security Information and Event Monitoring (SIEM)	The solution should offer a single view of all the data captured from devices across all sites and the SIEM solution should be consistent in Gartner's Leaders Quadrant across last 5 years (2019-2024)	The solution should offer a single, centralized view of all data captured from devices across all sites, and the SIEM solution should be recognized by leading industry analysts such as Gartner.	1.Since this clause conflicts with the global clause defined in Volume 02 of 03 – Annexure 3: Minimum Technical Specifications (Page 3, Section 3.2: Product Benchmarking), we respectfully propose that this clause be removed to maintain consistency and avoid ambiguity in technical evaluation. 2.Mandating consistency in Gartner's Leaders Quadrant over a fixed multi-year period makes the requirement vendor-specific and commercially restrictive	The solution should offer a single view of all the data captured from devices across all sites and meet the product benchmarking requirements given in sec 3.2, Annexure 3