

REQUEST FOR PROPOSALS



FOR

**UP-GRADATION OF BIOMETRIC IDENTIFICATION SYSTEMS FOR
PASSPORT APPLICATION UNDER PSDP PROJECT-2023**

SINGLE STAGE TWO ENVELOPE PROCEDURE

F.No. 1/1/ABIS/26/LOG/PSDP/Re-1



Handwritten signature in blue ink

**DIRECTORATE GENERAL IMMIGRATION & PASSPORTS,
G-8/1, HEADQUARTER, ISLAMABAD**





Ph: +92-51-9107075

Email: logistics@dgip.gov.pk

Directorate General Immigration & Passports
G-8/I Mauve Area,
Islamabad

INVITATION OF BIDS

Tender Notice NO: 1/1/ABIS/26/LOG/PSDP/Re-1

Procurement of Up-gradation of Biometric Identification Systems for Passport application

Sealed Technical and Financial Proposals are invited for up-gradation of biometric identification systems for Passport application in accordance with the tender document that can be purchased from the Logistics Section (Room No. 207, 2nd Floor) of Directorate General (I&P) on a formal request and upon payment of non-refundable fee (in shape of pay order/demand draft/call deposit) of Rs.5,000/- in favor of Director General (I&P).

The Directorate General, Immigration & Passports (DGIP), Ministry of Interior, Government of Pakistan invites bids from authorized service providers or principals' authorized dealers based in Pakistan for up-gradation of biometric identification systems for Passport application. Detailed technical specifications and requirements are provided in Annexure-I of the bidding document.

Bidders must be registered with Federal Board of Revenue (FBR)/respective Revenue Boards for Income Tax and Sales Tax and must appear on Active Taxpayers List (ATL) for both taxes.

Background: This Invitation for Bids follows Tender Notice No. 1/1/ABIS/26/LOG/PSDP/Re-1 published on the PPRA website, DGIP website, and in two national daily newspapers regarding the up-gradation of Biometric Identification Systems for Passport application for DGIP (Headquarters), Islamabad, for the above-mentioned purpose.

Bid Security: All bids must be accompanied by a Bid Security amounting to Rs.12,000,000/-. The original bid security must be submitted to DGIP (HQ), Islamabad before the bid submission deadline, failing which the bid shall be rejected. The Bid Security shall be in the form of a Bank Guarantee, Banker's Cheque, Pay Order, or Bank Draft issued by a scheduled bank in Pakistan and must remain valid for thirty (30) days beyond the bid validity period.

Bidding Procedure: The bidding shall be conducted in accordance with the Single Stage Two-Envelope procedure as prescribed in the Public Procurement Rules, 2004, and any other applicable regulations or guidelines issued by PPRA.

Availability of Bidding Documents: Complete bidding documents, including Terms & Conditions, Scope of Work, Instructions to Bidders, Bid Evaluation Criteria, Bid Validity, submission requirements, and detailed specifications at Annexure-I, may be obtained from DGIP (HQ), Islamabad, Logistics Section during office hours. The documents are also available on the PPRA website and DGIP official website.

Submission and Opening of Bids: Bids must be submitted in sealed envelopes in accordance with the instructions provided in the bidding documents. The bids must be submitted to DGIP (HQ), Islamabad on or before **03:00 PM on 06-04-2026**. The bids will be opened on the same day at 03:30 PM in the presence of bidders or their authorized representatives who choose to attend.

Director (NW/ F & Logistics)

Directorate General Immigration & Passport, Mauve Area,

Sector G-8/1, Islamabad

Tel:+92+51+9107075



Handwritten signature

1) INTRODUCTION OF ORGANIZATION:-

The Directorate General of Immigration & Passports (DGIP), Islamabad, is an attached department of the Ministry of Interior, Government of Pakistan. It is mandated to manage and administer matters pertaining to the issuance of passports, visas, and Pakistan citizenship, as assigned under the relevant laws, rules, and governmental directives.

DGIP Headquarters is located in Sector G-8/1, Islamabad, and the department operates a nationwide network of 177 Regional Passport Offices (RPOs), including thirteen (13) Executive Passport Offices (EPOs) and above 40 Passport Processing Counters (PPCs). In addition, Machine Readable Passport (MRP) facilities have been established at ninety-two (92) Pakistan Missions abroad, ensuring global access to passport services for overseas Pakistanis.

2) OBJECTIVE:-

The Directorate General, Immigration & Passports (DGIP), Islamabad, through this invitation of bids intends, to procure IT Equipment, for "Up-gradation of Biometric Identification Systems for Passport application with all accessories for Directorate General, I&P Headquarter, Islamabad".

3) SCOPE OF WORK:-

- i. The successful bidder will be responsible for the supply, installation, integration and testing of equipment at Directorate General, I&P, Headquarter, G-8/1, Islamabad as per specifications attached at **Annexure-I**.
- ii. The successful bidder must ensure that the supplied equipment / items are fully operational, new, performs properly and meet the Technical Specifications as mentioned in **Annexure-I** of this tender document.
- iii. At the time of supply and testing of IT equipment, successful bidder must provide the brochure and **training** where required.
- iv. Successful bidder shall be responsible for minimum one year warranty services on site without any extra cost or hidden charges also responsible for 24/7/365 on site support.
- v. OEM Consistency and support: The virtualization hypervisor and its underlying servers must be from the same OEM. The backup software and purpose-built appliances must also be from the same OEM. All hardware and software must be backed by a minimum five (05) year, **24x7x365 OEM led warranty and support**, with a proven local presence in Pakistan (offices and warehouses in ISB, LHR & KHI).
- vi. The supplier shall bring the samples of the hardware, if required by the purchase committee at his own cost and expense.

4) BID SUBMISSION INSTRUCTION / REQUIREMENT:-

The purpose of these instructions is to guide bidders in preparing and submitting their bids strictly in accordance with the specifications and conditions provided in this Tender Document. All bidders are required to carefully review the Tender Document before preparing their proposals.

- i. Bidders must thoroughly read all terms and conditions and submit their proposals strictly in accordance with the requirements of this Tender Document. The Company Evaluation Sheet provided at **Annex-III** must be duly filled and uploaded..



Handwritten signature in blue ink.

- ii. The procurement shall be processed under the **Single Stage Two Envelope** procedure, as per the Public Procurement Rules, 2004.

Both Technical and Financial Proposals must be submitted electronically through EPADS only. No physical submission of bids, envelopes, or documents will be accepted under any circumstances.

- iii. At the bid opening stage, EPADS shall open only the "Technical Proposal" submitted by the bidders.
- iv. The "Financial Proposal" shall remain electronically locked and inaccessible to DGIP until completion of the technical evaluation.
- v. The Technical Proposals will be evaluated by the DGIP Procurement Committee strictly in accordance with the criteria and specifications prescribed in this Tender Document. **Any proposal failing to meet the Mandatory Eligibility Criteria shall be rejected.**
- vi. Only the Financial Proposals of the technically qualified bids will be opened electronically on EPADS within the bid validity period. Financial bids of technically non-responsive bidders shall remain locked and inaccessible.
- vii. The lowest evaluated Financial Bid among the technically qualified bidders shall be declared successful.
- viii. Bidders must upload a signed and stamped cover letter, as per the format provided at **Annex-IV**.
- ix. Bidders must upload valid Income Tax / Sales Tax Registration Certificates and a duly signed Affidavit of Non-Blacklisting.
- x. All Financial Proposals must be quoted in Pak Rupees (PKR) and must be inclusive of all applicable taxes.
- xi. Bidders must submit a Bid Security of **Rs. 12,000,000/-** in the form and manner specified in the Advertisement as under:
- xii. The original Bid Security instrument must be submitted physically to DGIP (HQ), Islamabad before the bid submission deadline, otherwise, the bid shall be rejected. **(Only the Bid Security is allowed to be submitted physically.)**
- xiii. DGIP reserves the right to reject any or all bids in accordance with the Public Procurement Rules, 2004.
- xiv. Any bid submitted after the deadline prescribed on EPADS shall not be entertained.
- xv. Complete Tender Documents are available only through EPADS. No physical issuance or purchase of tender documents is required.
- xvi. Any change in the information furnished by the bidder that may affect delivery, performance, or contract execution must be immediately communicated to DGIP. Failure to do so may lead to cancellation of the contract.
- xvii. Bidders providing false, misleading, or fraudulent information shall be disqualified.
- xviii. Although due care has been taken in preparing this document, inadvertent typographical or clerical errors may occur, for which DGIP shall not be held responsible.



(Handwritten mark)

(Handwritten signature)

- xix. Bidders must upload a complete copy of the Tender Enquiry along with signed Terms & Conditions and clearly typed rates. Rates must be legible, without overwriting or correction.
- xx. Conditional, incomplete, altered, or revised bids submitted after the deadline or in deviation from the Tender conditions shall be rejected.
- xxi. EPADS will open the bids through its electronic system. Bidders or their authorized representatives may attend the bid opening session virtually (if EPADS facilitates) or physically at DGIP (HQ), if allowed.

5) MANDATORY ELIGIBILITY CRITERIA:

Technical proposal must contain following documents. Preliminary scrutiny (initial screening) of technical bids will be done on the basis of following parameters which are pre-requisites for this tender. **NON COMPLIANCE OF ANY OF THE FOLLOWING CLAUSE SHALL DISQUALIFY THE VENDOR STRAIGHT AWAY.**

(Technical proposal must contain following documents)

- a) Company Profile and relevant brochures.
- b) Valid NTN, ATL, and GST registration. (*Upload copies of NTN/ATL certificates and Income/Sales Tax registration certificates.*)
- c) Proof of valid membership with a recognized Chamber of Commerce.
- d) Proof of valid SECP registration or registration with the Registrar of Firms.
- e) Details of the bidder's service/support mechanism, including a list of technical staff.
- f) Proof of minimum 05 years of experience of similar nature in I.T Industry, involving supply /installation /support of similar equipment's to Government / Semi Government departments./ Autonomous body of good repute (**Must provide copies of purchase order / work orders**).
- g) Financial soundness of the company of minimum 500 million PKR annual average turn over in **last three (03) years**, the bidder to provide audited accounts statements for last three years as evidence.
- h) Copies of at least ten (05) Work Orders/Purchase Orders/Contracts executed for IT-related supply/installation/services for Government, Semi-Government, Autonomous Bodies or private institutions in last three years valuing more than 1 Million USD each.
- i) Proof of relationship/partnership status with the OEM/Principal, including after-sales support capability, response time details, and local presence.
- j) Bidder must be registered with ISO 27001:2022 & ISO 9001:2015 certificates to be provided as evidence.
- k) Valid OEM ISO Certifications of the quoted brand for both the company and the product.
- l) An Affidavit on Rs. 100 Stamp Paper confirming that the bidder is:
 - Not blacklisted by any Government/Semi-Government/Autonomous Body; and
 - Not involved in litigation with any client.



Ant. Phobis

DIRECTORATE GENERAL, IMMIGRATION & PASSPORTS

- (If involved in any ongoing litigation, full details must be disclosed.)
- m) A written Certificate of Compliance confirming that all quoted equipment fully meets the Technical Specifications of **Annex-I**, is brand new, of good market repute, and not refurbished or used.
- n) Copy of Bid Bond / Earnest Money as specified in the Tender Document must be uploaded with the Technical Proposal. The original bid security shall be submitted physically at DGIP before the bid submission deadline.
- o) Reliability, warranty, and after-sales support certificates relevant to the quoted equipment.
- p) Joint Venture is allowed of maximum 02 number of firms, JV must be incorporated in SECP and registered with FBR, documentary evidence of SECP and FBR to be provided as evidence. In case of submission through JV the evaluation will be made based on combined resources and documentation.
- q) Bidders must quote all items as per **Annexure-I** and clearly specify the offered specifications for each item. The completed **Annexure-I** must be signed and stamped by the bidder.

Note:- All documents must be properly signed, stamped, and uploaded. Documentary evidence for every mandatory requirement is compulsory. Missing or incomplete documents will result in the bidder's disqualification.

6) BID SECURITY:

- i. All bids must be accompanied by a Bid Security amounting to **Rs 12,000,000/-**. The original bid security must be submitted to DGIP (HQ), Islamabad before the bid submission deadline, failing which the bid shall be rejected. The Bid Security shall be in the form of a Bank Guarantee, Banker's Cheque, Pay Order or Bank Draft, issued by a scheduled bank in Pakistan, and must remain valid for thirty (30) days beyond the bid validity period.
- ii. For submission on EPADS, bidders must upload a scanned copy of the Bid Security with the technical Proposal. In addition, the original Bid Security must be submitted physically along with the Tender Form to DGIP (HQ), Islamabad before the bid submission deadline.
- iii. Failure to submit the original Bid Security in time will result in rejection of the bid.
- iv. The Bid Security of the successful bidder shall be forfeited in case of any default, violation of tender conditions, withdrawal of the bid during validity, or refusal to accept the Purchase Order/Contract.
- v. The Bid Security shall be returned after submission of the required Performance Security as per Clause-12 of this Tender Document.
- vi. Any Financial Proposal not supported by the Bid Security (both scanned copy on EPADS and original instrument (BID Security) submitted physically) shall be rejected outright. Personal cheques or undertakings in lieu of Bid Security will not be accepted.

7) EVALUATION CRITERIA:

Only those bidders who meet all Mandatory Eligibility Criteria will be considered for Technical Evaluation. Bidders failing to meet any mandatory requirement shall be rejected and will not proceed to the technical evaluation stage.



Atul Phakar

- ii. The DGIP Technical Evaluation Committee shall examine all Technical Proposals submitted on EPADS, including the quoted equipment/items, to assess compliance with the technical specifications, standards, and requirements provided in this Tender Document. Evaluation shall be based solely on the documents uploaded on EPADS.
- iii. Only the bidders who are declared Technically Qualified shall be considered for the opening of their Financial Proposals on EPADS. Financial Proposals of technically non-responsive bidders shall remain unopened.
- iv. The contract shall be awarded to the bidder whose Financial Proposal is the Lowest Evaluated Bid (LEB) among the technically qualified bidders, in accordance with the Public Procurement Rules, 2004.

8) SAMPLE/PHYSICAL INSPECTION:

After the opening and evaluation of Technical Proposals, the technically responsive bidders may be requested to provide a demonstration or technical walkthrough of the quoted items regarding upgradation of Biometric Identification System, if required. The DGIP Internal Technical Evaluation Committee shall conduct and evaluate the demo/inspection to verify compliance with the specifications and performance requirements of the ABIS project.

9) INSPECTION AND TEST:

- i. After delivery of all equipment to DGIP Headquarters, the designated Supervision/Inspection Committee shall verify the quantity, quality, configuration, and technical specifications of the supplied items to ensure full compliance with the requirements of the Tender Document.
- ii. The Inspection Committee shall conduct a comprehensive physical and technical examination of the delivered equipment. Any item found non-compliant, defective, substandard, or not matching with the approved specifications may be rejected. In such cases, the vendor shall be required to replace the rejected item(s) at no additional cost to DGIP within seven (07) days of notification.

10) MODE OF PURCHASE ORDER / WORK ORDER:

- i. Upon finalization of the procurement process and approval of the Lowest Evaluated Bid, a Purchase Order / Work Order shall be issued to the successful bidders in accordance with the terms and conditions of this Tender Document.
- ii. DGIP reserves the right to increase, decrease, or partially award the quantities/items based on departmental requirements, storage capacity, or technical considerations. Any such adjustments shall be made within the bid validity period or any extended validity period agreed between DGIP and the bidder.

11) TERMS OF PAYMENT:

- i. The supplier shall submit the invoice in triplicate, along with the receipted delivery challan, to the Director (NW/F & Logistics), DGIP. Payment shall be processed by the DDO (PSDP) and DDO (B&R) DGIP, Islamabad, upon issuance of a satisfactory completion/inspection certificate by the relevant Technical Team, confirming that all supplied items conform to the required specifications and are in good working condition.



Handwritten signature

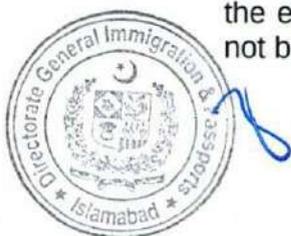
- ii. No advance payment shall be made to the firm under any circumstances.
- iii. Payment shall be made on completion of assignment as per work order, based on the successful delivery, installation, configuration, commissioning, and verification of each component/module and requisite site upgradation works.
- iv. Payment (up to 100%) shall be released upon completion of all deliverables and successful Acceptance Test Procedures (ATPs) carried out by the concerned Technical Wings of DGIP.
- v. All applicable Government taxes shall be deducted at source at the time of payment, in accordance with prevailing rules and regulations.

12) PERFORMANCE SECURITY:

- i. As per clause 39 of PPRA rules, the successful bidder shall submit a Performance Security equivalent to 5% of the total contract value, in the form of a Bank Guarantee (BG), Pay Order (PO), or Demand Draft (DD) from any scheduled bank in Pakistan, in favor of Director General, DG (Immigration & Passports), Islamabad.
- ii. The Performance Security must be submitted within 30 day from the date of signing of contract. Failure to submit the Performance Security within the stipulated time may result in cancellation of the award and forfeiture of the Bid Security.
- iii. The Performance Security shall remain valid for the entire warranty period, including any extended maintenance obligations, and shall cover all contractual obligations under this Tender.
- iv. The performance security in respect of procured items will be valid upto one year after successful completion / installation of the items.
- v. The Performance Security may be forfeited in full or in part in case the supplier fails to:
 - Comply with the terms and conditions of the contract,
 - Execute the supply, installation, commissioning, or integration as per specifications,
 - Honor warranty, maintenance, or after-sales obligations.
- vi. The Performance Security shall be released only after successful completion of all obligations, including the warranty period and final acceptance of all equipment and services by DGIP.

13) LIQUIDATED DAMAGES / PENALTIES:

1. In the event of delayed delivery, unsatisfactory performance, or non-compliance with the terms of the comprehensive warranty and after-sales service, the Performance Security / retention money may be forfeited, and DGIP reserves the right to refer the matter to the relevant authority for the possible blacklisting of the supplier.
2. A penalty of 2% of the total contract value shall be imposed for any delay in delivery of goods or services, calculated proportionally for part of the delay, if the stipulated delivery schedule is not met.
3. DGIP reserves the right to deduct such penalties directly from the supplier's invoices or any other dues payable under the contract.
4. Any request for exemption from penalties on account of force majeure or extraordinary circumstances must be submitted in writing at least 15 days prior to the expiry of the stipulated delivery period. Requests submitted after this period will not be entertained, and no exemption will be granted.



Handwritten signature in blue ink.

14) PRICE:

- i. All quoted prices must be unconditionally firm, final, and free from ambiguity, inclusive of all applicable taxes, duties, levies, and charges (including Sales Tax, Income Tax, and other statutory obligations) as applicable under the laws of Pakistan. All quoted prices must be in Pak Rupees only.
- ii. Bidders shall offer supply on a Free Delivery and Installation basis at DGIP Headquarters, Islamabad. All transportation, handling, and installation costs must be included in the quoted prices.
- iii. No request for price adjustment or escalation for any reason, including changes in taxes, duties, or exchange rates, shall be entertained during the contract period.
- iv. Quotations must be submitted in printed form on the official letterhead of the company/firm. Handwritten bids will not be accepted.
- v. Conditional bids, whether technical or financial, shall be considered non-responsive and shall be rejected outright.

15) SOFTWARE

- i. All software required for "Up-gradation of Biometric Identification Systems for Passport application with all accessories for Directorate General, I&P Headquarter, Islamabad must be genuinely licensed, with original license keys, certificates, and media provided to DGIP.
- ii. The software shall be procured through legal and authorized channels, with all applicable duties, taxes, and levies (if any) fully paid in accordance with the laws of Pakistan.

16) DELIVERY PERIOD:

- i. The supply, installation, and commissioning of all equipment and components for the subject equipment shall be completed within 12 to 16 weeks from the date of signing of the Contract.
- ii. The Director General, DGIP, reserves the right to extend or modify the delivery schedule as deemed necessary, based on operational requirements or other justifiable reasons.

17) REJECTED SUPPLY:

- i. Any equipment, materials, or components rejected by DGIP due to non-compliance with specifications, defects, or substandard quality shall be returned, transported, and replaced at the supplier's own risk and cost.
- ii. The supplier shall bear all expenses related to the handling, loading, unloading, and transportation of rejected items without any financial liability to DGIP.

18) FORCE MAJEURE:

- i. Force Majeure refers to any unforeseeable event or circumstance beyond the reasonable control of the Contractor or DGIP, including but not limited to government restrictions, war, hostilities, invasion, acts of foreign enemies, rebellion, revolution, riot, industrial disputes, civil commotion, natural disasters, or any other similar events that prevent the performance of contractual obligations.



Antal Chahar

- ii. The determination of the existence and applicability of Force Majeure conditions, including any extension of the delivery or performance schedule, shall be at the sole discretion of the Director General, DGIP, Islamabad.

19) WARRANTY:

- i. The supplier shall guarantee that all IT equipment supplied and installed under this Contract conforms to the specifications set forth in the Tender Document. Any item found to be defective, substandard, or non-functional **within a period of five (05) year** from the date of delivery/installation shall be replaced or repaired free of cost by the supplier, and a warranty certificate to this effect shall be provided.
- ii. The Contractor warrants that all goods supplied under this Contract shall be brand new, unused, of the latest or current models, and incorporate all recent improvements in design and materials, unless otherwise specified by DGIP. The Contractor further warrants that all goods shall be free from design, material, or workmanship defects (except as required by DGIP specifications) and shall perform reliably under normal operating conditions prevailing in Pakistan.
- iii. The Contractor shall provide a manufacturer's certificate confirming continuous backup support and after-sales service for all IT equipment and associated services for a **minimum period of five (05) years**.
- iv. DGIP shall promptly notify the Contractor in writing of any defects or issues covered under this warranty. Upon notification, the Contractor shall take immediate corrective action as per the warranty terms.

20) PROFESSIONAL TAX:

- i. The supplier shall provide valid National Tax Number (NTN) and Sales Tax Registration Number (GST) certificates.
- ii. In the event the supplier does not submit a valid Tax Exemption Certificate issued by the Federal Board of Revenue (FBR), all applicable taxes, duties, and levies as prescribed by the Government of Pakistan shall be deducted at source from the supplier's invoices/bills.

21) GENERAL TERMS AND CONDITIONS:

- a. In case of import of any items under this tender, the Contractor/Vendor shall be responsible for customs clearance of all goods through New Islamabad International Airport or Margalla Dry Port. All applicable customs duties, taxes, and charges arising from importation shall be borne by the Contractor/Vendor.
- b. Authorized agents nominated by the respective company must provide a letter of authority from their principal/manufacturer.
- c. DGIP, Islamabad, reserves the right to reject or accept any or all bids, in part or in full, without assigning any reason. DGIP may also distribute the tendered quantity among multiple bidders, and the lowest bidder shall have no claim to the full quantity.
- d. DGIP may waive any condition of the tender in the public interest.
- e. Suppliers must ensure that all supplies, installation, and commissioning strictly conform to the specifications provided in the tender document.

- f. DGIP shall not provide import licenses or any facility for the import or procurement of raw materials; the contractor shall be fully responsible for compliance.



(Handwritten signature)

- g. The decision of the Director General, DGIP shall be final and binding on all matters related to this tender.
- h. Bids that do not comply with the terms, conditions, and specifications of the tender shall be rejected.
- i. DGIP may request clarifications regarding submitted bids, but no change in price or substance of the bid shall be allowed after submission.
- j. Earnest money of unsuccessful bidders will be refunded upon submission of a written request after tender finalization.
- k. Incomplete or conditional bids shall not be entertained.
- l. All requests for clarification and responses must be in writing or via email; however, no alterations to price or substance will be permitted after bid submission.
- m. Any disputes arising after issuance of the work order shall be referred to the Director General, DGIP, whose decision shall be final and binding.
- n. Bids submitted via email/physical or fax shall not be accepted.
- o. In case of a public holiday on the bid opening date, bids will be opened on the next working day.
- p. The bidder must ensure the availability of spare parts and services for at least three (03) years for the quoted brand/model/solution.
- q. DGIP reserves the right to increase or decrease the quantity of items as per applicable rules.
- r. It is the bidder's responsibility to ensure that all bid documents are submitted through EPADs before the closing date and time. Late bids shall not be considered.
- s. The bidder shall be responsible for the supply, delivery, installation, and commissioning of new equipment.
- t. The delivery and installation of all items must be completed within 10 to 12 weeks from the date of signing the contract.
- u. Joint ventures or consortiums are not eligible for this tender.
- v. All decisions of DGIP shall be final, binding, and not challengeable in any forum or court of law.
- w. Bid Validity: Bids submitted under this tender shall remain **valid for 180 days** from the date of opening of Technical Proposals. DGIP may request an extension of bid validity for an **additional 90 days**, if deemed necessary.
- x. Bids must be submitted electronically through EPADS only. In accordance with instructions provided in the bidding document. The Original Bid security must be delivered to the address below on or before **03:00PM on April 06, 2026**. Electronic bids will be opened the same day at **03:30 PM through EPADs**.

22) SPECIAL CONSIDERATIONS FOR THE BIDDERS

- a. Bidders are strongly advised to visit and inspect the site of delivery and its surrounding areas to obtain, on their own responsibility, all information necessary for the preparation of their bids and for entering into a contract for the supply, installation, and commissioning of goods.
- b. All costs incurred in connection with such site visits, inspections, or information gathering shall be borne solely by the bidder.

Handwritten signature

Handwritten mark



23) CLARIFICATION:

- a. Any queries or requests for clarification regarding this Tender Document shall be submitted in writing to the Director (NW F&L), Directorate General, Immigration & Passports, Mauve Area, G-8/1, Islamabad.
- b. DGIP may provide clarifications or responses in writing to all prospective bidders, and such clarifications shall form an integral part of the Tender Document.

24) APPLICABLE LAW & DISPUTE RESOLUTION

In the event that any dispute arises between the procuring agency and the successful bidder in connection with the Agreement or services provided pursuant to the Agreement, the Parties shall attempt in good faith to resolve such dispute promptly by negotiation. If the matter has not been resolved within thirty (30) calendar days of a Party's request for negotiation, then all such dispute(s) shall be settled through arbitration by a sole arbitrator to be appointed with mutual consent of Parties. The arbitration shall be held under the provisions of the Arbitration Act 1940 as amended. The arbitration shall be held in Islamabad in English language. The award of the arbitration shall be binding on the Parties. As there is sole arbitrator fee will be paid by both the parties equally.

- i. Entry to DGIP Headquarters is strictly restricted for the general public. The successful bidder must submit full details of all personnel responsible for the delivery, installation, and commissioning of the goods prior to the issuance of the Purchase Order. Any subsequent changes in personnel must be promptly communicated to DGIP during the execution of the contract.
- ii. Access to the premises shall be granted only to authorized personnel whose details have been submitted and verified, and only during official working hours. Unscheduled or frequent visits without a valid purpose shall not be permitted.

**Director (NW/ F & LOGISTICS),
DG (I & P), Islamabad.**

I / We have carefully read and understood all the instructions, terms, and conditions outlined in this Tender Document and agree to fully comply with them in the submission and execution of this tender.

Signature of Proprietor / Authorized Agent / Owner: _____

Name of Firm: _____

Official Stamp / Seal: _____

Date: _____



Annexure-I

RFP Background: Enterprise Infrastructure Revamp and Modernization

1. Executive Summary

i. The Directorate General of Immigration & Passports (DGI&P) operates one of the most critical and security-sensitive IT environments in the country. Our systems manage the entire lifecycle of passport issuance and regulate all border entry and exit points, serving millions of citizens annually. The continuous availability, integrity, and confidentiality of the data processed by DGI&P are paramount to national security and public trust.

ii. To meet these mission-critical requirements, DGI&P invites proposals from established and reputable Original Equipment Manufacturers (OEMs) or their authorized partners for a comprehensive end-to-end revamp of our core IT infrastructure. This project aims to replace legacy, end-of-life systems with a modern, high-performance, resilient, and secure architecture. The solution must encompass RISC-based and x86 computing, all-flash storage, high-speed networking, a robust backup and disaster recovery framework including an air-gapped cyber-resilient vault, and a modern Virtual Desktop Infrastructure (VDI) to support our workforce.

2. Existing Environment & Business Challenges

i. DGI&P's current data center infrastructure, while having served its purpose, is now facing significant obsolescence and capacity constraints that pose a direct risk to business operations. The key challenges are outlined below:

ii. **End-of-Life Hardware:** A significant portion of the core RISC-based servers and associated storage arrays have reached their end-of-life and end-of-support milestones. This results in prohibitive maintenance costs, lack of firmware security updates, and increased risk of unplanned downtime.

iii. **Performance Bottlenecks:** The increasing digital adoption and data volume from passport applications and immigration transactions have outpaced the current storage and compute capacity. Existing systems struggle to maintain sub-millisecond latency required for real-time database transactions, leading to performance degradation during peak hours.

iv. **Inefficient Virtualization & Management:** The existing x86 virtualization environment is running on older hardware with limited resources, causing "VM sprawl" and inefficient resource utilization. Management overhead is high due to disparate, non-integrated tools for compute, storage, and networking.

v. **Inadequate Backup & Cyber Resilience:** The current backup infrastructure relies on an aging tape library and legacy software with insufficient capacity. Critically, there is no "air-gapped" or immutable copy of data to protect against sophisticated ransomware attacks, leaving the organization vulnerable to permanent data loss or extended downtime.

vi. **Scalability Limits:** The existing SAN fabric and storage arrays have reached their maximum scalability, preventing non-disruptive expansion to accommodate data growth. This limits our ability to onboard new digital services.

vii. **Legacy End-User Computing:** The current reliance on traditional desktop PCs creates challenges for secure remote access, endpoint management, and data security, particularly for a mobile workforce requiring flexible work options.

Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad



Handwritten signature



3. Strategic Objectives & Scope of Work

- i. To address the challenges above, DGI&P is seeking a holistic, "turnkey" solution that meets the following strategic objectives:
- ii. **Modernize Mission-Critical Compute:** Deploy a highly available, resilient, and scalable RISC-based architecture to host the core database and application workloads. This solution must provide advanced RAS (Reliability, Availability, Serviceability) features, including hardware-assisted virtualization, Live Partition Mobility, and Dynamic Logical Partitioning (DLPAR).
- iii. **Consolidate & Virtualize Workloads:** Refresh the x86 server estate with high-density, 6th-generation Xeon Gold/Platinum-based servers to create a robust virtualization cluster. This will host management servers (Jump Servers) and general-purpose virtualized applications, improving resource efficiency and manageability.
- iv. **Deploy High-Performance, Resilient Storage:** Procure Enterprise-Grade All-Flash NVMe-based storage arrays for both Production and Disaster Recovery (DR) sites. The storage must offer:
 - Guaranteed **3:1 data reduction** without performance impact.
 - Dual active/active controllers for high availability.
 - Support for block-level protocols (FC, iSCSI, NVMe/FC, NVMe/TCP).
 - Hardware-based ransomware threat detection and FIPS 140-2/3 compliance.
 - Native, non-disruptive data migration and federation across arrays.
- v. **Revamp Network Fabric:** Upgrade the data center network core and access layers with high-speed 25G/100G Top-of-Rack (TOR) switches and a dedicated Out-of-Band (OOB) management network. This includes deploying next-generation 32G Fibre Channel SAN switches to eliminate I/O bottlenecks and provide a low-latency, lossless fabric for storage traffic.
- vi. **Build a Cyber-Resilient Data Protection Framework:** Transform the backup and recovery landscape with a modern solution that includes:
- vii. **Software Licensing:** Upgrade the existing NetBackup environment with additional capacity and features.
- viii. **Purpose-Built Backup Appliances (PBBAs):** Deploy high-capacity appliances with inline deduplication at both primary and DR sites.
- ix. **Air-Gapped Cyber Vault:** Implement an isolated, ransomware-resistant environment with an immutable copy of critical data, incorporating anomaly detection and AI-based malware scanning.
- x. **Tape Library Expansion:** Scale the existing tape infrastructure with LTO-10 technology for long-term archival and compliance.
- xi. **Enable a Modern, Secure Workspace:** Implement a **Virtual Desktop Infrastructure (VDI) for 500 concurrent users**. The solution must provide a high-definition user experience with features like session roaming, multimedia optimization, and robust security controls, including watermarking, anti-screen capture, and integration with ADC/Gateways.

Directorate General, Immigration & Passports
Islamabad



4. Solution Architecture & High-Level Requirements

- i. The proposed solution must be architected to ensure zero downtime for critical services and seamless failover between the Primary and DR sites. Key architectural principles include:
- ii. **Redundancy & High Availability:** No single point of failure. All components, including servers, storage controllers, power supplies, fans, and network links, must be fully redundant and hot-swappable.
- iii. **Performance:** The solution must be engineered for high IOPS and low latency to support demanding database workloads. Specific performance metrics (e.g., >250,000 IOPS at sub-ms latency) are mandatory.
- iv. **Security-by-Design:** The infrastructure must incorporate security at every layer, from TPM 2.0 modules in servers to role-based access control (RBAC), encryption in-flight and at-rest, and compliance with standards like FIPS 140-2/3 and STIG.
- v. **Scalability:** All proposed hardware and software platforms must offer a clear, non-disruptive upgrade path to accommodate future growth (e.g., storage expandable to 1PB+, server cluster scalability to 256 nodes).
- vi. **OEM Consistency & Support:** The virtualization hypervisor and its underlying servers must be from the same OEM. The backup software and purpose-built appliances must also be from the same OEM. All hardware and software must be backed by a minimum 5-year, 24x7x365 OEM-led warranty and support, with a proven local presence in Pakistan (offices and warehouses in ISB, LHR & KHI).

5. Timelines & Commercial Terms

- i. The selected bidder must be capable of delivering, installing, and commissioning the entire solution within [Insert Number, e.g., 12-16] weeks from the date of the Purchase Order. The bidder will also be responsible for the seamless migration of data and workloads from the existing infrastructure to the new solution. All costs associated with migration, including any necessary hardware or software, must be borne by the bidder.

6. Proposal Submission Requirements

Bidders are required to submit a comprehensive proposal that includes:

- A detailed technical response using the Score-Based Compliance Matrix provided in this RFP, complete with page references to official datasheets.
- A high-level design (HLD) and low-level design (LLD) document.
- A project implementation and migration plan.
- Proof of OEM authorization and local support capabilities.
- A commercial bid with a detailed price breakdown in Pakistani Rupees (PKR).



TOR (Detailed Requirements)

1. CORE SERVER INFRASTRUCTURE (PRODUCTION)

(QTY:02)

Specification Category	Minimum Requirement
Form Factor	2U Rack Mount, 19" standard rack compatible Enterprise Grade RISC Architecture Machine
Architecture	64-bit RISC Architecture
Processor Sockets	Dual-socket configuration
Active Cores per Server	32 installed cores 24 Activated Cores per server
Virtualization Support	Hardware-assisted virtualization
Installed Memory	2 TB DDR5 ECC RAM
Memory Protection	Chipkill / ECC / Advanced RAS
Expandability	Expandable to system maximum supported
Internal Drive Bays	Minimum 8 hot-plug NVMe/SAS bays
Boot Device	Dual boot SSD (RAID1 preferred)
RAID Support	Enterprise RAID / NVMe HBA support
10G Ethernet	2x4x10GbE ports (SFP+ or RJ45)
Advanced Features	VLAN, LACP, Jumbo Frames, SR-IOV support
FC Ports	4 x 32Gb Fibre Channel Ports
HBA Type	PCIe 32G FC HBA (Dual-port cards allowed)
SAN Compatibility	Compatible with Brocade / Cisco MDS SAN
Power Supply	Dual Redundant Hot-Plug PSUs
Cooling	Redundant Hot-Plug Fans
Service Processor	Separate physical server for RISC-based server management
Hypervisor	OEM supported Hardware virtualization platform
Features	Live Partition Mobility, DLPAR, Micro-partitioning
OS Support	UNIX and LINUX on RISC platform supported
Warranty Period	Minimum 3 Years Onsite Support
Support Coverage	24x7 OEM Support
Firmware Updates	Included during warranty period

2. CORE SERVER INFRASTRUCTURE (DR)

(QTY:01)

Specification Category	Minimum Requirement
Form Factor	2U Rack Mount, 19" standard rack compatible Enterprise Grade RISC Architecture Machine
Architecture	64-bit RISC Architecture
Processor Sockets	Dual-socket configuration
Active Cores per Server	32 installed cores 24 Activated Cores per server
Virtualization Support	Hardware-assisted virtualization
Installed Memory	2 TB DDR5 ECC RAM
Memory Protection	Chipkill / ECC / Advanced RAS
Expandability	Expandable to system maximum supported



Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad

Ant Chahz



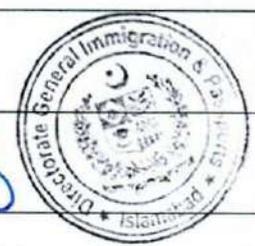
Internal Drive Bays	Minimum 8 hot-plug NVMe/SAS bays
Boot Device	Dual boot SSD (RAID1 preferred)
RAID Support	Enterprise RAID / NVMe HBA support
10G Ethernet	2 × 10GbE ports (SFP+ or RJ45)
Advanced Features	VLAN, LACP, Jumbo Frames, SR-IOV support
FC Ports	4 × 32Gb Fibre Channel Ports
HBA Type	PCIe 32G FC HBA (Dual-port cards allowed)
SAN Compatibility	Compatible with Brocade / Cisco MDS SAN
Power Supply	Dual Redundant Hot-Plug PSUs
Cooling	Redundant Hot-Plug Fans
Service Processor	Separate physical server for RISC-based server management
Hypervisor	OEM supported Hardware virtualization platform
Features	Live Partition Mobility, DLPAR, Micro-partitioning
OS Support	UNIX and LINUX on RISC platform supported
Warranty Period	Minimum 3 Years Onsite Support
Support Coverage	24×7 OEM Support
Firmware Updates	Included during warranty period

Handwritten signature in blue ink



3. Enterprise-Grade Block Storage NVMe-Based All-Flash (100TB Useable) PRODUCTION (QTY:01)

System Architecture:	
Form Factor:	Rackmount
Controllers:	Dual Active/Active Controllers
Power Redundancy:	Dual power supplies (independent operation)
Scalability:	Supports expansion to 1 PB or more via enclosures
Processor:	Minimum of 2 x Intel processors
Capacity & Drive Configuration	100 TB Useable post deduplication and compression including preferably 21x 9.6TB Modules
RAID:	RAID 10 for Pool 1, RAID-6 for Pool 2
Usable Capacity Pool 1:	100 TB or higher (Before Data Reduction)
Compression & Deduplication:	3:1 or better (guaranteed), without performance degradation preferably Hardware-based compression for no performance degradation of controller
Drive Type:	All-Flash NVMe SSD, hot-swappable
Drive Size (each):	9.6 TB or higher
Expansion:	Modular with support for additional enclosures
Cache:	1536 GiB per array (Maximum Memory bandwidth. Optimised for very high IOPs workloads in excess of 250,000 at sub-millisecond latency.)
PROTOCOLS, API SUPPORT, DATA SERVICES, AUTHENTICATION, SECURITY & ADVANCED FEATURES:	
Protocol:	Support Block Level Protocols (FC, iSCSI, NVMe/FC, NVMe/TCP etc)
Replication:	Synchronous for critical & asynchronous for non-critical workloads.
Snapshots & Cloning:	Space-efficient, Immutable, Writable clones for Dev/Test
Dynamic Storage Pooling:	Online expansion and reconfiguration
Data Tiering:	Hot/Cold auto-tiering
Virtualized Storage Pools:	Active/Active capability
Data Protection:	Maximize information security & minimize the risks of downtime, data loss/corruption, unauthorized access, & compliance failure
Cyber Resilience	Hardware-Based Ransomware Threat Detection
Compliance Standards:	TLS 1.2 (with TLS 1.0/1.1 disablement), FIPS 140-2/3, SHA-2 support, KMIP compliance
Directory Services:	LDAP, Active Directory
Secure Erase/Thin Provisioning/Data Shredding:	Required
Role-Based Access Control/Multi-Factor Authentication:	Required
Non-disruptive Data Migration (across volumes and pools):	Native, no third-party tools required



Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad

Handwritten signature



Clustering/Federation:	Across different models/generations
Monitoring, Management & Upgrade	
	Monitoring Dashboard: Centralized GUI, Real-time visibility with Capacity Forecasting & Trend Analytics.
	Online non-disruptive OS upgrade without reboot.
	OS Compatibility: Supports Microsoft Windows, Linux, Unix, & enterprise platforms.
	REST APIs for DevOps automation
Automation & Integration	
Automation Tools:	Ansible, PowerShell, OpenShift
Container Support:	OpenShift, CSI Driver, Docker or others
Licenses, Warranty & Support:	
	5 Years 24/7/365 OEM-led Warranty and technical support along with well-defined support matrix.
	Must include all necessary licenses: virtualization, snapshots, replication, compression, deduplication, etc. (single license bundle must include all features without per-feature/per TB licensing/vendor-specific add-ons.)

Handwritten signature in blue ink



4. Enterprise-Grade Block Storage NVMe-Based All-Flash (50TB Useable) DR (QTY:01)

System Architecture:	
Form Factor:	Rackmount
Controllers:	Dual Active/Active Controllers
Power Redundancy:	Dual power supplies (independent operation)
Scalability:	Supports expansion to 1 PB or more via enclosures
Processor:	Minimum of 2 x Intel processors
Capacity & Drive Configuration	50 TB Useable post deduplication and compression including preferably 9x 9.6TB Modules
RAID:	RAID 10 for Pool 1, RAID-6 for Pool 2
Usable Capacity Pool 1:	50 TB or higher (Before Data Reduction) 9x 9.6TB
Compression & Deduplication:	3:1 or better (guaranteed), without performance degradation preferably Hardware-based compression for no performance degradation of controller
Drive Type:	All-Flash NVMe SSD, hot-swappable
Drive Size (each):	9.6 TB or higher
Expansion:	Modular with support for additional enclosures
Cache:	512 GiB per array (Maximum Memory bandwidth. Optimised for very high IOPs workloads in excess of 250,000 at sub-millisecond latency.)
Protocols, API Support, Data Services, Authentication, Security & Advanced Features:	
Protocol:	Support Block Level Protocols (FC, iSCSI, NVMe/FC, NVMe/TCP etc)
Replication:	Synchronous for critical & asynchronous for non-critical workloads.
Snapshots & Cloning:	Space-efficient, Immutable, Writable clones for Dev/Test
Dynamic Storage Pooling:	Online expansion and reconfiguration
Data Tiering:	Hot/Cold auto-tiering
Virtualized Storage Pools:	Active/Active capability
Data Protection:	Maximize information security & minimize the risks of downtime, data loss/corruption, unauthorized access, & compliance failure
Cyber Resilience	Hardware-Based Ransomware Threat Detection
Compliance Standards:	TLS 1.2 (with TLS 1.0/1.1 disablement), FIPS 140-2/3, SHA-2 support, KMIP compliance
Directory Services:	LDAP, Active Directory
Secure Erase/Thin Provisioning/Data Shredding:	Required
Role-Based Access Control/Multi-Factor Authentication:	Required
Non-disruptive Data Migration (across volumes and pools):	Native, no third-party tools required
Clustering/Federation:	Across different models/generations
Monitoring, Management & Upgrade	



Handwritten signature in blue ink.



	Monitoring Dashboard: Centralized GUI, Real-time visibility with Capacity Forecasting & Trend Analytics.
	Online non-disruptive OS upgrade without reboot.
	OS Compatibility: Supports Microsoft Windows, Linux, Unix, & enterprise platforms.
	REST APIs for DevOps automation
Automation & Integration	
Automation Tools:	Ansible, PowerShell, OpenShift
Container Support:	OpenShift, CSI Driver, Docker or others
Licenses, Warranty & Support:	
	5 Years 24/7/365 OEM-led Warranty and technical support along with well-defined support matrix.
	Must include all necessary licenses: virtualization, snapshots, replication, compression, deduplication, etc. (single license bundle must include all features without per-feature/per TB licensing/vendor-specific add-ons.)

Handwritten signature in blue ink.



5. SAN Switch**(Qty:04)**

Form Factor:	1U rack-mountable or higher
Port Count:	48 x 32 Gbps Fibre Channel ports (36 active FC ports) or higher
Port Type:	for 32G FC
Backplane:	Throughput 1 Tbps or higher
Latency:	less than 900 nanoseconds (typical for 32G FC)
Switching Capacity:	0.77 Tbps or higher
Forwarding Rate:	Minimum 45 Mpps or higher
Operating Temp:	0° to 45°C
Allied Accessories:	Along with all allied necessary items, cabling, connectivity equipment to ensure redundant connectivity amongst 9 Servers and 1 Storage
Warranty & Support:	5 Years 24/7/365 OEM-led Warranty and technical support along with well-defined support matrix.

6. TOR Switch (Type-1): 25G Compute and Storage**(Qty: 08)**

1.	Switch must have
2.	- 24 x 25G SFP28 ports
3.	- 8x40GE/100GE QSFP28 Ports
4.	(Loaded with 6 x 25G SFP28 Optical Transceiver Module (Multi-Mode), 10 x 10G SFP+ Module(Multi-Mode), 8 x SFP+ 10GE Copper Interface Transceiver, 6 x 100G QSFP28 Optical Transceiver Module (Multi-Mode)).
5.	01 x Console Cable
6.	Note: SFPs must be of the same OEM Brand that of quoted Switch
7.	At least 5xfan tray slots
8.	Should have 4.8 Tbps or more box switching capacity
9.	Forwarding rate should be more than 1020 Mpps
10.	Should have 2.8Tbps or more port switching capacity
11.	Quoted switch must have redundant Power supplies
12.	Should be a Manageable Switch with Layer-3 features such as RIP, RIPng, OSPF & OSPFv3, BGP, Equal-cost multi-path routing (ECMP), IS-IS, PBR(Policy-based routing) and VRRP
13.	Switch CPU must be Quad core, 2GHz or higher
14.	Quoted switch must support L2, L3 VXLAN
15.	Quoted switch must support MPLS, MCE and MPLS VPN

7. TOR Switch (Type-2): Out of Band Management**(Qty: 06)**

1.	Should have 24 x 1G Ethernet Ports.
2.	Should have 4 x 10G SFP+ Ports (Loaded with 4 x SFP+ 10GE Module Multi-Mode)
3.	Note: SFPs must be of the same OEM Brand that of quoted Switch
4.	Should have 127 Gbps or more port switching capacity





5. Forwarding rate should be more than 95 Mpps
6. Should be a Manageable Switch with Layer-3 features such as RIP, RIPng, OSPF & OSPFv3
7. Should support Spanning Tree Protocol, 802.1D STP, 802.1W RSTP & 802.1S MSTP
8. Should support Stacking of local and remote devices through standard Ethernet interfaces. Should support stacking of 9 switches or more.
9. CPU speed, Dual Core, 1.2GHz or higher
10. Should Support Link Aggregation Protocol
11. Should have 4K or more VLANs support and 16K MAC address entries
12. Should be able to provide Access Port and Trunk Port
13. Broadcast, Multicast and Unicast Storm Control Support.
14. Port Mirroring, RSPAN or equivalent must be supported
15. Should support IPv4 routing entries 3000 or higher

Handwritten signature in blue ink.

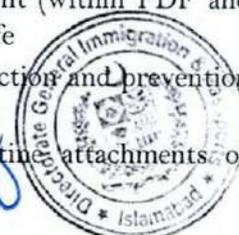




8. Firewall for Primary Site Network Data Protection

(Qty:02)

- The proposed product shall support robust GUI configurations of both IPv4 and IPv6 firewall policies.
- The proposed products should have onboard SSD internal storage for storage of logs, event etc.
- The proposed product must be based on hardware architecture for Security features inspection (NG Firewalling, SSL/TLS inspection, IPS, Antimalware etc) in the hardware.
- The proposed product must be recognized as a Leaders in the latest Gartner Magic Quadrant for Enterprise Network Firewalls.
- The proposed system shall minimally provide management access through:
 - GUI using HTTP or HTTPS access
 - CLI console using console port, SSHv2, telnet or from GUI console
- The administrator authentication shall be facilitated by a local database, PKI & remote services such as Radius, LDAP and TACACS+.
- The proposed product should be able to facilitate administration audits by logging detailed activities to event log - management access and also configuration changes.
- The proposed product shall have the ability to interconnect discrete security solutions into an integrated whole to detect, monitor, block, and remediate attacks across the entire attack surface.
- Administrators shall be able to configure both IPv4 and IPv6 DHCP service on an interface of the proposed product.
- Administrators shall be able to configure multiple loopback interfaces on the proposed product.
- Administrators shall be able to group interfaces, both physical and virtual, into zones that simplifies the creation of security policies.
- The proposed product shall support static routing and policy-based routing
- The proposed product shall support Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) for both IPv4 and IPv6.
- The proposed product must support active-passive (failover HA), active-active (load balancing HA) and Clustering.
- The proposed product shall support the upgrade of the firmware without interrupting communication through the cluster
- The proposed product shall support various QoS (quality of service) techniques, including Traffic policing, Traffic shaping and Queuing
- The proposed product shall support clientless and client-based SSL Remote Access VPNs.
- The proposed product shall support IPsec based Remote Access VPNs.
- The proposed product shall support both Route based and policy-based site to site IPsec VPNs.
- The proposed product shall provide Secure sockets layer (SSL) content scanning and inspection abilities that allow organizations to apply antivirus scanning, application control, web/URL filtering, and IPS inspection to encrypted traffic
- The proposed product shall provide the ability to exempt web sites from SSL scanning by site reputation, address, category, or using a whitelist.
- The proposed product shall support file sanitization feature where exploitable content (within PDF and Microsoft Office files) can be removed and replaced with content that is known to be safe
- The proposed product shall support Advanced Malware Protection for proactive detection and prevention against known and unknown threats.
- The proposed product shall provide ability to allow/monitor, block and quarantine attachments or downloads after malware detection using various technologies:
 - Malware signature database



[Handwritten signature]

Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad



- External file analysis with integration with on-prem or cloud-based sandbox service.
- File checksums query using cloud-based malware database.
- The proposed product shall be capable of blocking Botnet server communications.
- The proposed product shall also be able to block graywares and mobile malwares.
- The proposed product shall support category based dynamic web filtering by querying real-time cloud-based categorization database.
- The proposed product shall provide ability to use local categories (that override the cloud-based database rating) and remote categories (external URL list) as part of the URL rating function.
- The proposed product shall detect over 4,000+ applications for Application visibility and Control.
- The proposed product shall support custom application detection and control.
- The proposed product's IPS engine shall offer:
 - Signature based detection using real time updated database
 - Anomaly based detection that is based on thresholds
- The proposed product's IPS database shall have over 10,000+ up-to-date signatures and should support custom IPS signatures. A signature can be selected by searching for its corresponding CVE-ID (if applicable).
- The proposed product shall provide the ability to apply DNS category filtering to control user access to web resources.
- The proposed product shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.
- The proposed product shall support virtual firewalls that divide the Firewall into two or more virtual units that function independently.
- The proposed system shall provide explicit web proxy capabilities for proxying IPv4 and IPv6 HTTP and HTTPS traffic. Security components such as AV scanning, web filtering, IPS, application control, DLP and SSL/SSH inspection can be applied to proxied traffic within the system itself.
- The proposed product shall allow configuration of virtual systems resource limiting and management.
- The proposed product shall support Virtual routing and forwarding (VRF).
- The proposed product shall support various logging facilities:
 - Local memory
 - Local Storage
 - Multiple concurrent syslog servers.

Handwritten signature in blue ink



Require Hardware based firewall with following performance specs: (To be modified as required)

(Qty: 02)

Firewall throughput	195 Gbps
IPsec/SSL VPN throughput	52 Gbps
IPS throughput	20 Gbps
NGFW throughput	16 Gbps
Threat Protection throughput	14 Gbps
SSL inspection throughput	12 Gbps
Application Control throughput	32 Gbps
Concurrent TCP sessions	12 million
New TCP sessions/sec	750,000
Virtual Firewall/Router/Domains	10
Interfaces	4x 100 GE QSFP28, 12x 25 GE SFP28, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45
Local Storage	240 GB
Licenses with 5 years OEM support	Firewall, Anti-Malware, Application Control, IPS, URL Filtering

Abdul Wahid





9. Management / Jump Server – PRODUCTION (Qty:1)

1.Processor: 2 * Xeon Gold/Platinum 2.4GHz/24Cores/144MB Processor 6th-generation with a maximum power consumption of 210 watts or better
2. Form Factor: 2 U Rack Mount
3. RAM: At least 16 * 64GB DDR5 6400MHz (2Rx4) RDIMM
4. Memory Supported: Up to 4TB
5. 1 x 2U Front 8SFF Drive Backplane Module
6. HDD Required: 3* 960GB Read Intensive SATA 6Gb SSD,4* 7.68TB PCIe4.0 NVMe 2.5in RI SSD
7. Raid controller: Raid Controller 0,1,5 supported with 4 GB Cache
8. Network Adapters: 2 x Dual Port 10G SFP+ with 4 x 10G SFP+ Module (850nm,300m, LC), 1 GB Quad Port OCP 3.0 Adapter
9. 2 x Dual Port 32Gb PCIe Fibre Channel Host Bus Adapter (with Two FC SFP+ Transceiver)
10. Security Features: Support for Chassis security bezel, administrator's password, Root of Trust module supporting TPM 2.0
11. PCI Slots: Should support minimum 10x PCIe slots
12. Operating System Supported: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CAS, Ubuntu Server
13. Management Software: Remote Server License Included
14. Rack Mount Kit: Ball Bearing Rail Kit with Cable Management Arm
15. Power Supply: Redundant Power Supply
16. Warranty: 3 Years NBD ON-SITE with parts replacement

10. Virtualization Servers – PRODUCTION (Qty:4)

1.Processor: 2 * Xeon Gold/Platinum 2.4GHz/24Cores/144MB Processor 6th-generation with a maximum power consumption of 210 watts or better
2. Form Factor: 2 U Rack Mount
3. RAM: At least 16 * 64GB DDR5 6400MHz (2Rx4) RDIMM
4. Memory Supported: Up to 4TB
5. 1 x 2U Front 8SFF Drive Backplane Module
6. HDD Required: 3* 960GB Read Intensive SATA 6Gb SSD,4* 7.68TB PCIe4.0 NVMe 2.5in RI SSD
7. Raid controller: Raid Controller 0,1,5 supported with 4 GB Cache
8. Network Adapters: 2 x Dual Port 10G SFP+ with 4 x 10G SFP+ Module (850nm,300m, LC), 1 GB Quad Port OCP 3.0 Adapter
9. 2 x Dual Port 32Gb PCIe Fibre Channel Host Bus Adapter (with Two FC SFP+ Transceiver)
10. Security Features: Support for Chassis security bezel, administrator's password, Root of Trust module supporting TPM 2.0
11. PCI Slots: Should support minimum 10x PCIe slots
12. Operating System Supported: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CAS, Ubuntu Server
13. Management Software: Remote Server License Included
14. Rack Mount Kit: Ball Bearing Rail Kit with Cable Management Arm
15. Power Supply: Redundant Power Supply
16. Warranty: 3 Years NBD ON-SITE with parts replacement



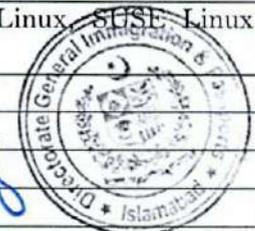
Signature

11. Management / Jump Server – DR site**(Qty:1)**

1. Processor: 2 * Xeon Gold/Platinum 2.4GHz/24Cores/144MB Processor 6th-generation with a maximum power consumption of 210 watts or better
2. Form Factor: 2 U Rack Mount
3. RAM: At least 16 * 64GB DDR5 6400MHz (2Rx4) RDIMM
4. Memory Supported: Up to 4TB
5. 1 x 2U Front 8SFF Drive Backplane Module
6. HDD Required: 3* 960GB Read Intensive SATA 6Gb SSD, 4* 7.68TB PCIe4.0 NVMe 2.5in RI SSD
7. Raid controller: Raid Controller 0,1,5 supported with 4 GB Cache
8. Network Adapters: 2 x Dual Port 10G SFP+ with 4 x 10G SFP+ Module (850nm,300m, LC), 1 GB Quad Port OCP 3.0 Adapter
9. 2 x Dual Port 32Gb PCIe Fibre Channel Host Bus Adapter (with Two FC SFP+ Transceiver)
10. Security Features: Support for Chassis security bezel, administrator's password, Root of Trust module supporting TPM 2.0
11. PCI Slots: Should support minimum 10x PCIe slots
12. Operating System Supported: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CAS, Ubuntu Server
13. Management Software: Remote Server License Included
14. Rack Mount Kit: Ball Bearing Rail Kit with Cable Management Arm
15. Power Supply: Redundant Power Supply
16. Warranty: 3 Years NBD ON-SITE with parts replacement

12. Virtualization Servers – DR Site**(Qty:2)**

1. Processor: 2 * Xeon Gold/Platinum 2.4GHz/24Cores/144MB Processor 6th-generation with a maximum power consumption of 210 watts or better
2. Form Factor: 2 U Rack Mount
3. RAM: At least 16 * 64GB DDR5 6400MHz (2Rx4) RDIMM
4. Memory Supported: Up to 4TB
5. 1 x 2U Front 8SFF Drive Backplane Module
6. HDD Required: 3* 960GB Read Intensive SATA 6Gb SSD, 4* 7.68TB PCIe4.0 NVMe 2.5in RI SSD
7. Raid controller: Raid Controller 0,1,5 supported with 4 GB Cache
8. Network Adapters: 2 x Dual Port 10G SFP+ with 4 x 10G SFP+ Module (850nm,300m, LC), 1 GB Quad Port OCP 3.0 Adapter
9. 2 x Dual Port 32Gb PCIe Fibre Channel Host Bus Adapter (with Two FC SFP+ Transceiver)
10. Security Features: Support for Chassis security bezel, administrator's password, Root of Trust module supporting TPM 2.0
11. PCI Slots: Should support minimum 10x PCIe slots
12. Operating System Supported: Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CAS, Ubuntu Server
13. Management Software: Remote Server License Included
14. Rack Mount Kit: Ball Bearing Rail Kit with Cable Management Arm
15. Power Supply: Redundant Power Supply
16. Warranty: 3 Years NBD ON-SITE with parts replacement



Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad



13. Hypervisor Solution– PRODUCTION (10 Sockets Perpetual Licensing)

1. Fully licensed with quoted hardware solution, with 03 Years OEM support
2. Virtualization Hypervisor and Servers should be from same OEM.
3. Proposed hypervisor must be provided along with replication licenses for 25 VMs.
4. Should have features like High availability, Live & Seamless VM Migration (host & storage), Snapshot, Cloning, Template creation, real time monitoring and analytics.
5. Support features like increasing capacity by adding Memory, CPU and virtual NIC to virtual machines on an as needed basis without any disruption in working or downtime for the virtual machines
6. Proposed Solution must provide High Availability
7. Proposed Solution should be highly redundant providing capability for the VMs to restart on another node in case of any Node failure in the Cluster
8. Proposed Solution must provide capability to scale up to 256 nodes or higher
9. Proposed Solution must support to create and manage local Users with Role Based Access and Permission Control
10. Proposed Solution must provide VM Snapshot capability to revert to previous point in time in case a failure or system error occurs
11. Proposed Solution must provide VM Clone capability for creating cloned instances from source VM for testing or any other purposes
12. Proposed Solution must provide automated Resource Scheduling and Load Balancing capability for balanced performance on all nodes across the cluster.
13. Due to the critical nature of customer business, proposed Solution must support cluster dynamic resource scheduling, which can dynamically schedule resources for VMs based on host CPU usage, memory usage, disk I/O, disk usage, disk requests, and network traffic. (Provide screenshot as proof)
14. Due to the critical nature of customer business, proposed Solution must support self-managed host system. When the virtualization management platform fails, hosts and VMs on the hosts can be managed from the self-managed host system. (Provide screenshot as proof)
15. Due to the critical nature of customer business, proposed Solution must support monitoring the running status of VM application processes, and support restarting the applications or VMs in the event of a fault to minimize downtime.
16. Due to the critical nature of customer business, proposed Solution must provide Distributed Switch capability to configure and administer switching for the entire Cluster. (Provide screenshot as proof)
17. Due to the critical nature of customer business, proposed Solution must support viewing the services and port numbers used by a host, and setting the IP range for access to prevent unauthorized access and attacks. (Provide screenshot as proof)
18. Due to the critical nature of customer business, proposed Solution must support viewing, starting, deleting, bulk starting, and bulk deleting VMs that have not been used for a long time and are in a shutdown state at one click. (Provide screenshot as proof)
19. Due to the critical nature of customer business, proposed Solution must support analyzing invalid image files on the back-end storage at one click. (Provide screenshot as proof)
20. Due to the critical nature of customer business, proposed Solution must support bulk editing VM configuration, including CPU scheduling priority, number of CPUs, memory size, I/O priority, boot priority, auto migration. (Provide screenshot as proof)
21. Due to the critical nature of customer business, the virtualization platform must provide graphical display of vSwitch port. (Provide screenshot as proof)



Signature

22. Due to the critical nature of customer business, proposed Solution must support memory swapping, using intelligent scheduling algorithms. (Provide screenshot as proof)
23. Proposed Solution must support encrypted disk creation for VMs by using the
24. AES encryption algorithm.
25. Proposed Solution must provide capability to display Virtual Datacenter Network Topology for easy Management and Troubleshooting
26. Proposed Solution must provide capability to manage Switching and Routing of Internal workloads by providing Virtual Switches.
27. Proposed Solution must support to configure Internal Virtual Storage, External LAN/SAN or NAS to be Backup repository for Storing Virtual Machine Backups
28. Proposed Solution must support Industry's common storage protocols such as iSCSI, FC or Network File Sharing (NFS)

14. Hypervisor Solution-DR

(06 Sockets Perpetual Licensing)

1. Fully licensed with quoted hardware solution, with 03 Years OEM support
2. Virtualization Hypervisor and Servers should be from same OEM.
3. Proposed hypervisor must be provided along with replication licenses for 25 VMs.
4. Should have features like High availability, Live & Seamless VM Migration (host & storage), Snapshot, Cloning, Template creation, real time monitoring and analytics.
5. Support features like increasing capacity by adding Memory, CPU and virtual NIC to virtual machines on an as needed basis without any disruption in working or downtime for the virtual machines
6. Proposed Solution must provide High Availability
7. Proposed Solution should be highly redundant providing capability for the VMs to restart on another node in case of any Node failure in the Cluster
8. Proposed Solution must provide capability to scale up to 256 nodes or higher
9. Proposed Solution must support to create and manage local Users with Role Based Access and Permission Control
10. Proposed Solution must provide VM Snapshot capability to revert to previous point in time in case a failure or system error occurs
11. Proposed Solution must provide VM Clone capability for creating cloned instances from source VM for testing or any other purposes
12. Proposed Solution must provide automated Resource Scheduling and Load Balancing capability for balanced performance on all nodes across the cluster.
13. Due to the critical nature of customer business, proposed Solution must support cluster dynamic resource scheduling, which can dynamically schedule resources for VMs based on host CPU usage, memory usage, disk I/O, disk usage, disk requests, and network traffic. (Provide screenshot as proof)
14. Due to the critical nature of customer business, proposed Solution must support self-managed host system. When the virtualization management platform fails, hosts and VMs on the hosts can be managed from the self-managed host system. (Provide screenshot as proof)
15. Due to the critical nature of customer business, proposed Solution must support monitoring the running status of VM application processes, and support restarting the applications or VMs in the event of a fault to minimize downtime.
16. Due to the critical nature of customer business, proposed Solution must provide Distributed Switch capability to configure and administer switching for the entire Cluster. (Provide screenshot as proof)

Ant Chelz



17. Due to the critical nature of customer business, proposed Solution must support viewing the services and port numbers used by a host, and setting the IP range for access to prevent unauthorized access and attacks. (Provide screenshot as proof)
18. Due to the critical nature of customer business, proposed Solution must support viewing, starting, deleting, bulk starting, and bulk deleting VMs that have not been used for a long time and are in a shutdown state at one click. (Provide screenshot as proof)
19. Due to the critical nature of customer business, proposed Solution must support analyzing invalid image files on the back-end storage at one click. (Provide screenshot as proof)
20. Due to the critical nature of customer business, proposed Solution must support bulk editing VM configuration, including CPU scheduling priority, number of CPUs, memory size, I/O priority, boot priority, auto migration. (Provide screenshot as proof)
21. Due to the critical nature of customer business, the virtualization platform must provide graphical display of vSwitch port. (Provide screenshot as proof)
22. Due to the critical nature of customer business, proposed Solution must support memory swapping, using intelligent scheduling algorithms. (Provide screenshot as proof)
23. Proposed Solution must support encrypted disk creation for VMs by using the
24. AES encryption algorithm.
25. Proposed Solution must provide capability to display Virtual Datacenter Network Topology for easy Management and Troubleshooting
26. Proposed Solution must provide capability to manage Switching and Routing of Internal workloads by providing Virtual Switches.
27. Proposed Solution must support to configure Internal Virtual Storage, External LAN/SAN or NAS to be Backup repository for Storing Virtual Machine Backups
28. Proposed Solution must support Industry's common storage protocols such as iSCSI, FC or Network File Sharing (NFS)

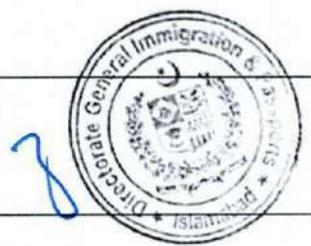
Handwritten signature in blue ink.



15. Enterprise-Grade Block Storage NVMe-Based All-Flash (50TB Useable)
PRODUCTION QTY:01

System Architecture:	
Form Factor:	Rackmount
Controllers:	Dual Active/Active Controllers
Power Redundancy:	Dual power supplies (independent operation)
Scalability:	Supports expansion to 1 PB or more via enclosures
Processor:	Minimum of 2 x Intel processors
Capacity & Drive Configuration	50 TB Useable post deduplication and compression including preferably 9x 9.6TB Modules
RAID:	RAID 10 for Pool 1, RAID-6 for Pool 2
Usable Capacity Pool 1:	50 TB or higher (Before Data Reduction) 9x 9.6TB
Compression & Deduplication:	3:1 or better (guaranteed), without performance degradation preferably Hardware-based compression for no performance degradation of controller
Drive Type:	All-Flash NVMe SSD, hot-swappable
Drive Size (each):	9.6 TB or higher
Expansion:	Modular with support for additional enclosures
Cache:	512 GiB per array (Maximum Memory bandwidth. Optimised for very high IOPs workloads in excess of 250,000 at sub-millisecond latency.)
Protocols, API Support, Data Services, Authentication, Security & Advanced Features:	
Protocol:	Support Block Level Protocols (FC, iSCSI, NVMe/FC, NVMe/TCP etc)
Replication:	Synchronous for critical & asynchronous for non-critical workloads.
Snapshots & Cloning:	Space-efficient, Immutable, Writable clones for Dev/Test
Dynamic Storage Pooling:	Online expansion and reconfiguration
Data Tiering:	Hot/Cold auto-tiering
Virtualized Storage Pools:	Active/Active capability
Data Protection:	Maximize information security & minimize the risks of downtime, data loss/corruption, unauthorized access, & compliance failure
Cyber Resilience	Hardware-Based Ransomware Threat Detection
Compliance Standards:	TLS 1.2 (with TLS 1.0/1.1 disablement), FIPS 140-2/3, SHA-2 support, KMIP compliance
Directory Services:	LDAP, Active Directory
Secure Erase/Thin Provisioning/Data Shredding:	Required
Role-Based Access Control/Multi-Factor Authentication	Required

Ant Alchaher

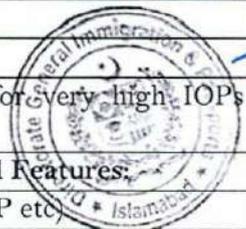




Non-disruptive Data Migration (across volumes and pools):	Native, no third-party tools required
Clustering/Federation:	Across different models/generations
Monitoring, Management & Upgrade	
	Monitoring Dashboard: Centralized GUI, Real-time visibility with Capacity Forecasting & Trend Analytics.
	Online non-disruptive OS upgrade without reboot.
	OS Compatibility: Supports Microsoft Windows, Linux, Unix, & enterprise platforms.
	REST APIs for DevOps automation
Automation & Integration	
Automation Tools:	Ansible, PowerShell, OpenShift
Container Support:	OpenShift, CSI Driver, Docker or others
Licenses, Warranty & Support:	
	5 Years 24/7/365 OEM-led Warranty and technical support along with well-defined support matrix.
	Must include all necessary licenses: virtualization, snapshots, replication, compression, deduplication, etc. (single license bundle must include all features without per-feature/per TB licensing/vendor-specific add-ons.)

16. Enterprise-Grade Block Storage NVMe-Based All-Flash (50TB Useable) DR QTY:01

System Architecture:	
Form Factor:	Rackmount
Controllers:	Dual Active/Active Controllers
Power Redundancy:	Dual power supplies (independent operation)
Scalability:	Supports expansion to 1 PB or more via enclosures
Processor:	Minimum of 2 x Intel processors
Capacity & Drive Configuration	50 TB Useable post deduplication and compression including preferably 9x 9.6TB Modules
RAID:	RAID 10 for Pool 1, RAID-6 for Pool 2
Usable Capacity Pool 1:	50 TB or higher (Before Data Reduction) 9x 9.6TB
Compression & Deduplication:	3:1 or better (guaranteed), without performance degradation preferably Hardware-based compression for no performance degradation of controller
Drive Type:	All-Flash NVMe SSD, hot-swappable
Drive Size (each):	9.6 TB or higher
Expansion:	Modular with support for additional enclosures
Cache:	512 GiB per array (Maximum Memory bandwidth. Optimised for Very high IOPs workloads in excess of 250,000 at sub-millisecond latency.)
Protocols, API Support, Data Services, Authentication, Security & Advanced Features:	
Protocol:	Support Block Level Protocols (FC, iSCSI, NVMe/FC, NVMe/TCP etc)



Handwritten signature



Replication:	Synchronous for critical & asynchronous for non-critical workloads.
Snapshots & Cloning:	Space-efficient, Immutable, Writable clones for Dev/Test
Dynamic Storage Pooling:	Online expansion and reconfiguration
Data Tiering:	Hot/Cold auto-tiering
Virtualized Storage Pools:	Active/Active capability
Data Protection:	Maximize information security & minimize the risks of downtime, data loss/corruption, unauthorized access, & compliance failure
Cyber Resilience	Hardware-Based Ransomware Threat Detection
Compliance Standards:	TLS 1.2 (with TLS 1.0/1.1 disablement), FIPS 140-2/3, SHA-2 support, KMIP compliance
Directory Services:	LDAP, Active Directory
Secure Erase/Thin Provisioning/Data Shredding:	Required
Role-Based Access Control/Multi-Factor Authentication:	Required
Non-disruptive Data Migration (across volumes and pools):	Native, no third-party tools required
Clustering/Federation:	Across different models/generations
Monitoring, Management & Upgrade	
	Monitoring Dashboard: Centralized GUI, Real-time visibility with Capacity Forecasting & Trend Analytics.
	Online non-disruptive OS upgrade without reboot.
	OS Compatibility: Supports Microsoft Windows, Linux, Unix, & enterprise platforms.
	REST APIs for DevOps automation
Automation & Integration	
Automation Tools:	Ansible, PowerShell, OpenShift
Container Support:	OpenShift, CSI Driver, Docker or others
Licenses, Warranty & Support:	
	5 Years 24/7/365 OEM-led Warranty and technical support along with well-defined support matrix.
	Must include all necessary licenses: virtualization, snapshots, replication, compression, deduplication, etc. (single license bundle must include all features without per-feature/per TB licensing/vendor-specific add-ons.)

Handwritten signature



Backup Solution Upgradation & Modernization

Proposed data backup & recovery software (Existing NetBackup Software) additional 20TB (Data size) front-end capacity-based license with Five (05) years 24x7x365 support, which also include entitlement for DR site for same capacity and all required features.
Two (02) purpose build backup appliance having at-least 75TB (post-RAID capacity without dedupe factor) useable storage space of same OEM (whose backup software is proposed above) for storing data backups at Primary and DR Site with Five (05) years 24x7x365 support
One (01) purpose build backup appliance having at-least 75TB (post-RAID capacity without dedupe factor) useable storage space of same OEM (whose backup software is proposed above) for Air Gap (isolated ransomware protected) Environment for storing critical data having front end capacity license of 140TB for Air Gap environment with all allied hardware and software for Air Gap environment having Five (05) years 24x7x365 support
Backup appliances should have complete redundant power supply and fans, support hot swappable disk replacement,
Proposed backup appliance should have at least 4x 10/25GB Ethernet SFP ports and 4 x 32GB FC ports.
Proposed backup appliance should have option of storage expandability at least up to 400TB.
Backup appliance must support Inline block level dedupe across all datasets.
The solution must have built-in (or provided separately) IDS/IPS software and other ransomware protection (e.g. anomaly detection, malware scanning)
Backup appliance and master server role must support Linux Operating System with security hardened configurations as per standards like CIS relevant benchmarks or STIG
Backup software should be capable of automated catalogue recovery
Solution must support Active/Active Backup Server implementation across main and DR site, with replicated catalogue information to ensure business continuity.
Ability to scale up and scale out the implementation seamlessly to accommodate more policies, clients, and storage
Offer choice of deduplication - source based, target based in-line process deduplication to meet the varying needs of physical and virtual environments, natively from the same deduplication appliance
Offer bandwidth (WAN) optimized replication across sites to enhance disaster recovery option
Tape-out should be integrated with the Disk Backup Policy, one policy should manage the "backup image" across Main site, DR site and Tape out Facility in DR
Backup appliance must support direct connectivity with Tape library to eliminate proxy tape servers
Provide a flexible solution that scales to the growing needs of the environment.
Offer Granular Recovery for VMware and Hyper-V at file level in a single step backup, without the need to copy, duplicate or restore the backup image to a different location.
Should be able to protect Oracle, MS-SQL, DB2 backups without Manual Scripts (Including Archive redo Log Truncation)
Should be capable of Guided Application recovery for Oracle. RMAN catalogue should be synchronized with all database backup image copies available within the data lifecycle.
Backup software should be able to utilize the backup appliance as a storage location of all RMAN-directed operations, via a NFS share.
Backup software should provide "incremental forever" backup method by leveraging Oracle® Incremental Merge technology without scripting. Space-optimized full back up images should be automatically synthesized to prepare for fast recovery
Oracle DBA should be able to see all backup copies across the entire lifecycle within the Oracle RMAN recovery catalogue. All subsequent copies made by Backup software must be synchronized with Oracle.
Backup software should be capable of configuring Multiple Schedules per Backup Policy with multiple client targets
Backup and Recovery Audit Trail is required with Roles Based Authentication security
Backup appliance Lockdown using an industry standard security software is needed

[Handwritten Signature]

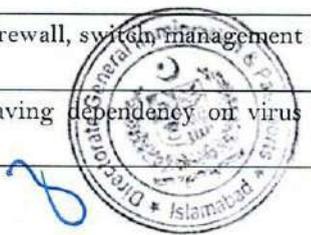
Directorate General, Immigration & Passports (Hqrs)
Room No 207 2nd Floor Mauve Area G-8/1 Islamabad





Backups over LAN should support 1Gbit/sec, 10Gbit/sec and 25Gbit/sec network ports, 10 G must be supplied
Support backup to physical Tape library, backup appliance should have FC connectivity for tape libraries
Backup appliance should support backup over SAN, appliance should have FC connectivity to receive backup data on SAN
Full support for Windows, Linux (Red Hat Enterprise, SUSE, etc.) and other systems, with support for open file backups
Backup software should have the ability to generate an inline optimized synthetic FULL backup from Incremental backups, thus allowing incremental backups forever. VMware, Hyper-V and File System backup (including NDMP) should support this functionality over LAN or SAN & the proposed OEM shall be the leader in Gartner Magic Quadrant for last 7 consecutive years.
The management of the backup software and deduplication appliance must be from the same management console.
The appliance must offer multiple levels of deduplication optimizations, including application aligned deduplication, together with CPU and memory optimization.
Appliance must be capable of deduplication complex data types (such as databases). Must integrate with native database backup mechanisms such as RMAN and provide advanced multiple stream-based duplicated backup. Must support MSSQL, Oracle, Postgres, MySQL and other databases.
The dedupe license should be independent of hardware so replacing hardware should not incur new software license cost and is not tied to a specific hardware vendor, providing greater flexibility and reducing the risk of vendor lock-in.
The deduplication appliance must support one-to-one, many-to-one, one-to-many, many-to-many replication topologies including catalogue together replication capability for true DR Readiness. Support replication of backup data between backup appliances over Ethernet / FC SAN network.
The deduplication appliance must support 256bit (or more) encryption algorithm for both data during transfer (on the wire) and for data at rest (in the appliance) without the need for any additional licenses.
Proposed solution should be in compliance with SEC 17a-4(f), ISO 15489-1, FDA 21 CFR Part 11 and FIPS 140-2 standards, STIG Compliance implementation, DISA Security Control implementation or Industry standards
The deduplication appliance must be capable of reporting in the event of a failure. Must have standard SNMP/SMTP support and Call Home capability.
Backup Software should provide self-services, where-in clients can run their own backups and restores of Virtual Machines.
Backup software must be certified with modern workloads such as Kubernetes, Red Hat Open Shift, Docker container backup integration. Must able to support legacy workloads on Unix, Linux, Windows as well as modern workloads and hyper converged infrastructure.
The backup software must provide Operational Resiliency, Security and Compliance. Should allow creating a separate user for SQL admin, Oracle administrator, etc.
The backup software must support integration with external certificate authority. Must support 2048 bit (or more) keys for backup certificate authority.
The Backup software must support unified single server deduplication for both dedupe to local disk or object storage or cloud storage.
The backup software must support single click fail over or rehearsal operation to club of VMs. DR Orchestration must support IP and DNS customization. DR Orchestration should not require extra license. Implementation of resiliency group might be required for future use case as part of DR plan.
The solution must support Oracle RAC integration with parallel node writing/reading simultaneously for backup & recovery.
Solution must support encryption in-flight and at-rest.
Proposed solution must offer key features for providing ultra-secure copies of backups to recover from a cyber-attack/ransomware attack including; Automated Isolation / Air Gap, Data Immutability, behavioural based anomaly detection
All required infrastructure components for building cyber recovery site / IRE (e.g. compute, firewall, switch, management software) must be included in the proposed solution
Solution should have an intelligent/AI based mechanism and machine learning without having dependency on virus signatures for detecting malicious activity/malware/ransomware.

Handwritten signature





Solution must pause data protection (backup, duplication and Expiration) activities for the protected asset when an infection in a backup image is detected.
Solution must support parallel malware scanning.
Solution support backup Web UI and/or Java UI integration with 2FA/MFA, MPA, SAML for enhanced secure login for backup and recovery software and backup appliances.
Solution must support integration with industry leading SOAR/XDR and SIEM Platform.
Five (05) years OEM back-to-back warranty and support of all hardware and software included in the Solution
OEM resource participation will be required during installation and configuration of complete solution (if required).
Bidder will submit a plan and perform backup data migration from existing backup solution software to newly supplied backup software and backup appliance. If any hardware or software is required for migration then bidder will bear the cost of such hardware and software
Bidder will need to provide onsite engineering support through at least one professional level certified and experienced resource on deployed hardware and software.

17. Tape Library at PR & DR Site (QTY:02)

Parameter	Minimum Requirement
Library Type	Enterprise-class modular and scalable tape library
Form Factor	3U base module with modular expansion capability
Scalability	Minimum 7 modules scalability without forklift upgrade
Cartridge Slots (Base Module)	≥ 40 slots
Cartridge Slots (Expansion Module)	≥ 40 slots
Total Slots (After Expansion)	≥ 80 slots usable
Drive Bays per Module	Minimum 3 drive bays per module
Robotics	Single robotic mechanism with intelligent slot management
Barcode Reader	Integrated standard
Control Panel	Front LCD/Touch control panel
Online Expansion	Supported without downtime
LTO-10 Full Height Fibre Channel Tape Drive	40TB Native, FC Interface

Handwritten signature



Solution must pause data protection (backup, duplication and Expiration) activities for the protected asset when an infection in a backup image is detected.
Solution must support parallel malware scanning.
Solution support backup Web UI and/or Java UI integration with 2FA/MFA, MPA, SAML for enhanced secure login for backup and recovery software and backup appliances.
Solution must support integration with industry leading SOAR/XDR and SIEM Platform.
Five (05) years OEM back-to-back warranty and support of all hardware and software included in the Solution
OEM resource participation will be required during installation and configuration of complete solution (if required).
Bidder will submit a plan and perform backup data migration from existing backup solution software to newly supplied backup software and backup appliance. If any hardware or software is required for migration then bidder will bear the cost of such hardware and software
Bidder will need to provide onsite engineering support through at least one professional level certified and experienced resource on deployed hardware and software.

17. Tape Library at PR & DR Site (QTY:02)

Parameter	Minimum Requirement
Library Type	Enterprise-class modular and scalable tape library
Form Factor	3U base module with modular expansion capability
Scalability	Minimum 7 modules scalability without forklift upgrade
Cartridge Slots (Base Module)	≥ 40 slots
Cartridge Slots (Expansion Module)	≥ 40 slots
Total Slots (After Expansion)	≥ 80 slots usable
Drive Bays per Module	Minimum 3 drive bays per module
Robotics	Single robotic mechanism with intelligent slot management
Barcode Reader	Integrated standard
Control Panel	Front LCD/Touch control panel
Online Expansion	Supported without downtime
LTO-10 Full Height Fibre Channel Tape Drive	40TB Native, FC Interface

Handwritten signature in blue ink.





18. Virtual Desktop Infrastructure for 500 users

VDI Licensing	
	Provide license for 500 users
	Must be able to support deployment for on premise, public cloud or hybrid
	Must provide Cloud Management & Monitoring Plane as a Service without additional cost
	Must come with ADC, Endpoint Management, App Protection, Hypervisor, Secure OS & Monitoring Agent licenses bundled
App and Desktop Resources	
Session-based desktop	A shared desktop is hosted on a virtual server OS, such as Windows Server and delivered to the user as a virtual desktop over a remote presentation ICA HDX protocol.
Session-based apps	Individual applications are hosted on a virtual server OS, such as Windows Server, and delivered to the user as a published application over a remote presentation ICA HDX protocol.
Mixed desktop/app deployment	A server OS can simultaneously deliver desktops and apps.
Management	
System and logon messages	Messaging can be used to keep remote desktop clients more informed. System messages can be used to inform users of upcoming server downtimes. Logon messages can be used to display legal information that the remote user must acknowledge before starting a session.
Policy based Application Publishing for groups of servers	Provide a centralized mechanism for publishing applications to groups of servers simply by adding or removing servers from a group.
Reboot management	Policy defined schedule, built within the administrator console, allowing for a daily or weekly schedule for rebooting servers, allowing an administrator to define specific groups of servers and warning messages to users.
Centralized Power Function Management	Ability to manage restart or shutdown RDS host servers and VDI VMs from the management console.
Centralized Publishing	Allows administrators to easily deliver server resources – such as applications, content, and server desktops – from hundreds to tens of thousands of users from a single wizard-driven console.
Automated Client Installation	A web-based process walks the user through the process of automatically detecting the needed client software and then automatically installs the appropriate client software for the platform used.
Role-based management tools	Support and management tools designed to align with the common tasks associated with different support roles.
Deliver a High Definition User Experience	
Auto-resize user desktop	As a user changes end point devices with different resolutions or the user resizes the virtual desktop window, the interface and application automatically resize for the new resolution.
Session Roaming	Provides seamless roaming of the user's session across devices.
Folder management	Allows applications to be grouped within folders for easier organization

Handwritten signature

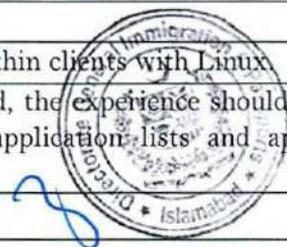


	for multiple user groups.
Disconnect or Close All Applications	A single button provides a means for the user to suspend or exit all running applications without having to perform this action in each individual application. This functionality works regardless of how many server sessions the user has established. This is especially useful for situations where the user wants to switch devices such as when leaving the office to go home.
Support for video conferencing in hosted sessions	Provides the ability to use video conferencing applications within server hosted sessions.
Seamless applications	Enables applications running on the server to look and feel as if they are running locally
Connection resiliency	Automatically reconnects user sessions when the network connection is temporarily lost.
USB device support	Enables users to remotely access USB devices such as USB printers, USB storage, and USB Webcam devices connected to their client device
Session pre-launch	A session is automatically created when a user logs onto their endpoint. When the user launches an application or desktop, 80% of the session instantiation was already completed, providing a much faster logon time and user experience.
Session linger	When a user closes their last hosted application, the session remains active for a period of time in the event the user launches a new application. As the session is still active, the user does not have to go through the logon process again.
Auto enrolled apps	The app or desktop will have an automatic subscription for a user without the user being required to manually subscribe. The user can still unsubscribe.
Featured apps	Provides an administrator to highlight an app or desktop. This feature is often used when there are hundreds of apps published for a single user and is used for the most widely used apps.
Preferred apps	Allows an administrator to set conditions that a local application on the end point should be used if the same app exists as a hosted application.
App store branding	Allows an organization to add a corporate brand with the application store without requiring extensive coding expertise.
Multi-launch prevention	Many times, due to the few seconds it takes between the selection of a resource until the launch window is seen, users tend to click multiple times, which could launch a single application 5+ times. Multi-launch prevention prevents this accidental and resource intensive behavior.
Session reliability	When a network connection issue occurs, the application window remains visible on the end point and the session continues to accept keystrokes and mouse movement from the user while session re-connection is attempted in the background. For transient network issues, such as where users roam between wireless "hot spots", the user may not even know connectivity was lost.
User self-service for application subscription	Users are provided self-service control of which applications are integrated within their desktop environment through a simple application subscription store front. Without this, users might see a list of over 100 applications, many not relevant to their job.

Handwritten signature



Automatic Reconnection	Configurable option allowing users to automatically reconnect to all disconnected sessions at logon without user interaction.
Multimedia and Traffic Optimization	
High resolution graphics	If a bitmap looks as if it is photographic or highly detailed, an extra level of lossy JPEG compression is added to reduce the bandwidth required to transmit the image to the client.
Visually lossless	Remoting ICA HDX protocol dynamically adjusts visual quality based on the network link conditions, degrading image quality to save bandwidth without the user being aware.
Multimedia playback	Supports audio and video playback on the client device for audio streams from the server session.
Adaptive Display	Multiple encoding schemes are utilized within a single session for different portions of the screen.
Enlightened Data Transport	A transport layer protocol that combines much of the resiliency of TCP with the performance gains of UDP over High-bandwidth, high-latency WAN links.
Adaptive Transport	The ability to automatically switch the transport layer of a user's session between multiple transport options in order to compensate for dynamic network conditions.
Bandwidth limit	Allows an administrator to set the maximum bandwidth limit for audio, video, client drives and USB devices to reduce the likelihood that a print job could disrupt the user experience.
Web browser performance optimizations	Provides a combination of features that can automatically disable GIF animations, intercept images and pass them on before being uncompressed, dynamically re-compress JPEG images, deliver images in the background, and cache images on the client.
Hypervisor & Cloud Support	
Hypervisors	Supports Microsoft Hyper-V, Citrix XenServer, VMWare vSphere, Nutanix Acropolis
Hybrid deployment	A single installation can manage resources available onsite in the data center as well as hosted on a cloud provider.
Multi-Cloud deployment	A single control plane installation can manage resources located in multiple datacenter and multiple cloud infrastructures (i.e. AWS EC2, Microsoft Azure, and On-Prem VMware ESX) simultaneously.
Client Endpoint Device OS	
Windows	Support access from Windows Desktop/Server OS devices
Macintosh	Support access from MacOS devices
iOS	Support access from iOS devices
Android	Support access from Android devices
HTML5	Provides HTML5 web based browser support, no additional client installation required for simple and fast access.
Chromebooks	Native support, not via HTML5
Linux	Access from Linux based OS including thin clients with Linux
Seamless end point agent experience	Regardless of the end point device used, the experience should look the same, which includes the interface, application lists and application favorites.





Security	
Delegated Administration	Allows different administrators to manage different aspects of the solution including: images, delivery groups, catalogs, infrastructure, and monitoring tools.
Centralized Access Policies	Administrators can configure settings for user sessions as policies that can be applied to sessions based on username, group, server name, server management container, client IP address or subnet, zone, or client name (or partial name). Priorities can be applied to these policies depending on specific user session situations.
Secured Access to Server Applications	Provides SSL/TLS encryption and multifactor authentication to provide authorized application access to appropriate users.
Device Redirection Enforcement	Device redirection enforcement helps prevent malicious code on remote clients from overriding security policies set by an administrator.
User or group based policy enforcement	User and security policies are applied based on the user or group name.
OU based policy enforcement	User and security policies are applied based on the Active Directory organizational unit name.
Clipboard Security	Users are permitted, denied or partially denied usage of copying text and images from the server to the client or from the client to the server via the clipboard (copy/paste)
Watermark	Able to include critical information to identify any potential data leak via mobile camera
Anti Screen Capture	Block attempts of local endpoint device from performing screen capture by showing only black/white/grey screen
Anti Keylogger	Blocks keylogger from capturing keyboard inputs by scrambling inputs
Anti DLL Injection	Blocks connection to apps or desktops when detecting client app DLL files has been tampered with
Session Management and Recording	Provide native session recording capabilities without requiring 3rd party licenses. Session Management and Recording features include automatic session recording triggered by predefined events and detailed monitoring of the user's final network segment for enhanced troubleshooting.
Integration	
ADC/Gateway	VDI solution must be able to integrate with ADC/Gateway from same vendor without additional licenses cost
Performance	Integration must be native without performance impact, Must support ICA/HDX protocol natively.

Handwritten signature in blue ink



Annexure-II Evaluation of Bid

DIRECTORATE GENERAL, IMMIGRATION & PASSPORTS COMPANY EVALUATION PROFORMA

Total Marks		100				
Minimum Qualifying marks		70				
S.No	Criteria for evaluation	Total Marks	Detail parameter	Detail to be provided by the bidder	Marks awarded	
1	Company Age: Age of Company as per SECP incorporation at the time of bid submission	10	10 Years or above = 10 Marks 5 to 9 Years = 5 Marks Less than 5 Years = 0 Marks	Copy of SECP Incorporation to be provided by bidder		
2	Financial Strength: Annual Average Turn over for the last 03 years of the company at the time of bid submission	25	PKR 3 Billion or above = 25 Marks PKR 2 Billion or above 15 Marks PKR 1 Billion or above = 05 Marks Less than 500 Million = 0 Marks	Audited Accounts for Last Three financial years to be provided		
3	Technical Strength: Number of Technical resources employee in company at the time of bid submission.	10	100 or more employees = 10 Marks 50 to 99 employees = 5 Marks 25 to 49 employees = 3 Marks Less than 25 = 0 Marks	Company Payroll or EOBI List or similar document.		
4	OEM MAF/MAL: Bidder should provide Maf/Mal from OEM at the time of bid submission	5	0 Marks = If Not provided	MAF/MAL to be provided		
5	ISO Registration: ISO 27001:2022	10	0 Marks = if not ISO 27001:2022	Copy of Registration to be provided		
6	ISO Registration: ISO 9001:2015	5	0 Marks = if not ISO 9001:2015	Copy of Registration to be provided		
7	Technical Expertise IT Services: The Bidder has secured at least 01 project worth USD 5 Million	10	0 Marks = if no project	Copy of Purchase order/Contract to be provided		
8	Technical Expertise IT Infrastructure:	15	3 or more PO/Contract = 15 Marks	Copies of Purchase		



Handwritten signature

9	The Bidder has secured IT Infrastructure projects valuing more than 03 Million USD Each	10	1 to 2 POI/Contract = 05 Marks	order/Contracts to be provided
			No POI/Contract = 0 Marks	
9	Presence: The bidder has offices in all three major cities in Pakistan including Karachi, Islamabad & Lahore	10	Three cities = 10 Marks	Copy of Rent Agreements to be provided
			Two Cities = 05 Marks	
			One City = 0 Marks	
Note: Registered JV for a maximum of 02 companies together is allowed to participate, the evaluation of JV shall be based on combined criteria for evaluation and individual firms do not require to fulfill all the requirements independently				
Total Marks		100	Qualification Score	70 Marks
Signature of Owner / Authorized representative				

Financial Evaluation

Financial bids shall be evaluated of only Technically Qualified bidders. While doing financial evaluation, total bid value shall be considered provided the financial bid includes all the costs involved in the project as per the requirements set forth in this document, and strictly following the format given in BoQ.	Financial Score weightage of overall bid 30%
Method of calculation	Lowest Bidder Price score 30 Mark 30 % of (Lowest Bidder Price Divided by Highest Bidder Price) x 100

Overall qualification

Total Qualifying score from Technical Bid (Administrative Score + Technical) should be more than 70% for the bidder to qualify for participation in Financial Opening Evaluation Method 70% Technical Score + 30 % Score from financial Bid.

Most Advantageous bid

Most advantageous bid scoring highest score shall be considered as successful



[Handwritten signature]

[Handwritten signature]

ANNEXURE - III

PROPOSAL SUBMISSION FORM

To:

The Director (NW F & Logistics)
Directorate General, Immigration & Passports,
G-8/1, Mauve Area, Islamabad.

Subject: Submission of Proposal for "Up-gradation of Biometric Identification Systems for Passport application with all accessories

Dear Sir,

We, the undersigned, hereby submit our proposal to provide Data Center-Related I.T. Equipment to the Directorate General, Immigration & Passports, Islamabad, in strict accordance with your tender document dated 31-03-2026. We are submitting our Technical Proposal along with the Financial Proposal, each sealed in separate envelopes as specified in the tender document.

We have also enclosed a Bid Bond / Earnest Money of **Rs. 12,000,000 /-**, as required under the tender terms, along with our financial proposal.

We understand that the Directorate General, I&P, Islamabad, is not bound to accept any proposal received and reserves the right to accept or reject any offer, or to annul the bidding process, without assigning any reason.

We acknowledge that the decision of the Evaluation Committee shall be final, binding, and cannot be challenged in any forum. The Evaluation Committee shall not be liable for any loss or damage to any party acting in reliance on the evaluation process.

We remain,

Your's sincerely

Authorized Signature:
Name and Title of Signatory:
Name of Firm / Company:
Address



ANNEXURE-V FINANCIAL PROPOSAL

Price Schedule / Financial Cost Sheet (separately for each lot)

Item #	Item/Equipment / Work Description	Quantity	Unit Price (without Tax)	Unit Price with Taxes (if any, also mention tax type and percentage)	Total price with taxes (if any)
1.					
2.					
3.					
4.					
5.					
Grant Total					

NOTE:-

- i. Vendor will determine the total bid cost for all items ~~under each lot.~~
- ii. Prices must be quoted for all items under each lot.
- iii. Hardware quoted must be legally imported in Pakistan after paying all taxes.
- iv. DG I&P reserves exclusive rights to increase / decrease the quantities of the tender.

Total Cost (in words) Rs. _____

Date:- _____

**Signature of the Authorized person
Name:-**

(Company Seal)

**In the capacity of
Duly authority by**

Note:- No cutting or overwriting is allowed. Any cutting or overwriting will lead to rejection of the financial bid.

Handwritten signature



Annexure VIForm of Performance Security

To:

Directorate General Immigration & Passports Headquarters,
Sector G-8/1, Mauve Area,
Islamabad.

Subject: B/G AND DATE FOR _____ ON BEHALF OF _____ FOR DUE AND FAITHFUL PERFORMANCE OF CONTRACT NO. 1/1/ABIS/26/LOG/PSDP/Re-1 DATED _____

Whereas M/s _____ (hereinafter called the Contractor) have requested us to furnish a Bank Guarantee in your favour in the sum of Rs. _____ (Rupees _____ (IN WORDS) as Performance Security against Contract / Agreement No. _____ dated _____ to be concluded between the Contractor and Directorate General Immigration & Passports (hereinafter called the DG I & P).

WE HEREBY AGREE AND UNDERTAKE:

- i. To make an un-conditional payment of Rs. _____ (Rupees _____) to you on demand, without any further question or reference to the Contractor, upon failure of the Contractor to perform the Contract of which you shall be the sole judge.
- ii. To keep this guarantee valid and in full force and effect from this date up to the time of the due and faithful completion of the Contract under reference (the schedule of implementation shall be as described in the Contract and its subsequent amendments) or till _____ whichever date is later. The faithful completion of the Contract by the Contractor shall be intimated by the DG I & P.
- iii. To extend the period of the enforceability of this guarantee if such extension be necessary due to late issuance of Clearance Certificate from Pakistan Customs or desired by you of us. All claims hereunder must be submitted to us on or before the expiry date mentioned in this guarantee or the date mentioned in any extensions issued from time to time, after which this guarantee shall become null and void and should be returned to us. Irrespective of its return, we shall consider ourselves fully discharged from any obligation there under after the said expiry date.

Dated This Day of _____, 2026.

Signature: _____
A Signatory Authorized To Sign Contract on
Behalf of Contractor.

Witness: _____

Sworn & Sign before me
This day of2026

By: _____

Ant Arshad



Annexure VI **Integrity Pact**

_____ [the Seller/Supplier] hereby declares its intention not to obtain or induce the procurement of any contract, right, interest, privilege or other obligation or benefit from Government of Pakistan or any administrative subdivision or agency thereof or any other entity owned or controlled by it (GoP) through any corrupt business practice.

Without limiting the generality of the foregoing, [the Seller/Supplier] represents and warrants that it has fully declared the brokerage, commission, fees etc. Paid or payable to anyone and not given or agreed to give and shall not give or agree to give to anyone within or outside Pakistan either directly or indirectly through any natural or juridical person, including its affiliate, agent, associate, broker, consultant, director, promoter, shareholder, sponsor or subsidiary, any commission, gratification, bribe, finder's fee or kickback, whether described as consultation fee or otherwise, with the object of obtaining or inducing the procurement of a contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP, except that which has been expressly declared pursuant hereto.

[the Seller/Supplier] certifies that it has made and shall make full disclosure of all agreements and arrangements with all persons in respect of or related to the transaction with GoP and has not taken any action or shall not take any action to circumvent the above declaration, representation or warranty.

[the Seller/Supplier] accepts full responsibility and strict liability for making any false declaration, not making full disclosure, misrepresenting facts or taking any action likely to defeat the purpose of this declaration, representation and warranty. It agrees that any contract, right, interest, privilege or other obligation or benefit obtained or procured as aforesaid shall, without prejudice to any other rights and remedies available to GoP under any law, contract or other instrument, be void at the option of GoP.

Notwithstanding any rights and remedies exercised by GoP in this regard, [the Seller/Supplier] agrees to indemnify GoP for any loss or damage incurred by it on account of its corrupt business practices and further pay compensation to GoP in an amount equivalent to ten times the sum of any commission, gratification, bribe, finder's fee or kickback given by [the Seller/Supplier] as aforesaid for the purpose of obtaining or inducing the procurement for any contract, right, interest, privilege or other obligation or benefit in whatsoever form from GoP.



