Request for Proposal

No. EA/02-51-2023

For Provisioning of MFA Solution

1. Bids are invited from potential Companies for Provisioning of Multi Factor Authentication (MFA) Solution as per RFP Annexure. This bid Document is also available in Etisalat website (www.etisalat.af, Tenders).

2. RFP Deadline is **26-September-2023**. The bids shall be submitted though email (snabizada@etisalat.af) and marked clearly with **RFP name, number.**

Note: If you submit your commercial part of proposal by email, please provide it in **password protected document/format**. We will request the password once here the concerned committee started the bid's commercial evaluation.

3. Bid received after the above deadline shall not be accepted.

4. Local and international firms can send their offer via email to snabizada@etisalat.af and copy Ihsanullah@etisalat.af.

5. Etisalat Afghanistan reserves the right to accept or reject any or all bids and to annul the bidding process at any time, without thereby incurring any liability to the affected bidder(s) or any obligations to inform the affected bidder(s) of the grounds for Etisalat Afghanistan action.

6. Bidder should be registered with Etisalat Afghanistan in Vendor Registration List. If any interested bidder **is not registered**, first they should fill the attached Vendor Registration Form and provide following documents before tender deadline and submission of bid. Bidder's offer will not be considered without registration process**.**

1- Company Profile

2- Business License

3- President and Vice President ID Cards/Tazkira Copies

4- Article of Association (نامه اساس)

3. Past Performance:

Firm must describe past performance on similar public and or private agency contracts,

including past performance on similar works for any other telecom company.

7. All correspondence on the subject may address to Shoaib Nabizada, Sr. Analyst Procurement & Contracts, and Etisalat Afghanistan. Email snabizada@etisalat.af and Phone No. 0781204113.

Ihsanullah Zirak
Director Supply Chain
Ihsan Plaza, Shar-e-Naw, Kabul, Etisalat Afghanistan
E-mail**:** ihsanullah@etisalat.af

Request for Proposal

(RFP)

For

Provisioning of Multi Factor Authentication (MFA) Solution

1. DEFINITIONS

In this document, the following terms and meanings shall be interpreted as indicated:

1.1 Terms.

"Acceptance Test(s) "means the test(s) specified in the Technical Specifications to be carried out to ascertain whether the Goods, Equipment, System, Material, Items or a specified part thereof is able to attain the Performance Level specified in the Technical Specifications in accordance with the provisions of the Contract.

"Acceptance Test Procedures" means test procedures specified in the technical specifications and/or by the supplier and approved by EA as it is or with modifications.

"Approved" or "approval" means approved in writing.

"BoQ " stands for Bill of Quantities of each job/work as mentioned in this contract and its annexes according to which the contractor shall supply equipment & services and subject to change by agreement of both parties.

"Bidding" means a formal procurement procedure under which sealed bids are invited, received, opened, examined and evaluated for the purpose of awarding a contract.

"Bid/Tender Document" means the Bid/Tender documents issued by EA for invitation of Bids/Offers along with subsequent amendments and clarifications.

"CIF" means "Cost Insurance Freight" as specified in INCOTERM 2010.

"Competent Authority" means the staff or functionary authorized by EA to deal finally with the matter in issue.

"Completion Date" means the date by which the Contractor is required to complete the Contract.

"Country of Origin" means the countries and territories eligible under the rules elaborated in the "Instruction to Bidders ".

"Contract" means the Contract between Etisalat Afghanistan (EA) and the Contractor and comprising documents.

"Contractor" means the individual or firm(s) ultimately responsible for supplying all the Goods/Equipment/Systems/Material/Items on time and to cost under this contract to EA.

"Contractor's Representative" means the person nominated by the contractor and named as such in the contract and approved by EA in the manner provided in the contract.

"Contract Documents" means the documents listed in Article (Contract Documents) of the Form of

Contract (including any amendments thereto) or in any other article in this contract.

"Contract Price" means the price payable to the Contractor under the Contract for the full and proper performance of its contractual obligations.

"Day" means calendar day of the Gregorian calendar.

"Delivery charges" means local transportation, handling, insurance and other charges incidental to the delivery of Goods to their final destination.

"D.D.P" means Delivered Duty Paid as defined in the Incoterms 2010 including the unloading responsibility of bidder/seller.

"Effective Date" means the date the Contract shall take effect as mentioned in the Contract.

"Etisalat Afghanistan (EA)" means the company registered under the Laws of Islamic republic of Afghanistan and having office at Ihsan Plaza Charahi Shaheed Kabul in person or any person dully authorised by it for the specific purpose for the specific task within the Contract and notified to contractor in writing.

"Final Acceptance Certificate" means the certificate issued by EA after successful completion of warranty and removal of defects as intimated by EA.

"Force Majeure" means Acts of God, Government restrictions, financial hardships, war and hostilities, invasion, act of foreign enemies, rebellion, revolution, riot, industrial disputes, commotion, natural disasters and other similar risks that are outside of Contractor's and EA's control.

"Goods Receipt Certificate" means certificate issued by the consignee certifying receipt of Goods in good order and condition.

"Liquidated Damages" mean the monetary damages imposed upon the contractor and the money payable to EA by the contractor on account of late delivery of the whole or part of the Goods.

"**L.o.A**" means Letter of Award issued by EA to successful bidder with regard to the award of tender.

"Month" means calendar month of the Gregorian calendar.

"Offer" means the quotation/bid and all subsequent clarifications submitted by the Bidder and accepted by EA in response to and in relation with the Bid Documents.

"Origin" means the place where the Goods are mined, grown or produced from which the ancillary services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembling of components, a commercially recognized product results that is substantially different in basic characteristics or in purpose or utility from its components.

"EA's Representative" shall mean the representative to be appointed by EA to act for and on behalf of EA with respect to this Contract.

"Specifications" means the specifications, provided in the Contract and its annexure and in EA Tender Specifications and where the Contract is silent and in cases of conflicting specifications appearing in the documents, based on the latest version of ITU-T recommendations.

"Supplier/Vendor" (used interchangeably) means the individual or firm ultimately responsible for supplying all the Goods on time and to cost under this Contract acting individually alone or as a "prime contractor" for a consortium.

"Supplier's Representative" means the person nominated by the Contractor and named as such in the Contract and approved by EA in the manner provided in the Contract.

"Warranty Period" shall mean the period of 12 months or any extended period starting from the acceptance of the delivered Goods in good order and conditions at consignee's certified by EA authorized representative (s).

2. INTRODUCTION TO WORK.

2.1 Bids are invited for Provisioning of Multi Factor Authentication (MFA) Solution in accordance with Etisalat specifications as per Annexure A.

3. Scope of Work

As per Annexure –A

4. Validity of Offers

The Tenders must be valid for a minimum of 90 days from the Tender closing date, or as may be specified by Purchaser in the Tender documents.

5. Price:

5.1 International Bidders can quote CIP Kabul and Local Bidders shall quote DDP Kabul prices accordingly.

5.2 DDP Prices shall be inclusive of Custom Duties and all Taxes as applicable in Afghanistan as per Islamic Republic of Afghanistan Tax Laws.

6. Payment Terms.

6.1 Payment mode:

6.1.1 75% of Payment will be made to the Contractor after Software delivery and installation.

61.2 25% of Payment will be made to the Contractor after RFS.

6.2 Payment shall be made by bank transfer after receipt of original Hardcopy of invoice.

6.3 Advance payment will be not made to contractor.

6.4 EA shall make prompt payment, within thirty days of submission of an invoice/claim by the contractor subject to availability of pre requisite documents specified under the contract and adjustment of penalty (if any) on account of late delivery and/or defective Goods replacement after confirmation from Project Director.

6.5 Payments are subject to deduction of income tax at prevalent rate from the relevant invoices of the contractor and paid to the Tax Authorities, except those especially exempted by the authorities. EA will issue certificate of deductions to the contractor to enable him to settle tax returns with the concerned authorities.

6.6 "Etisalat Afghanistan has full right to issue the PO/Contract payments via mHawala (mobile financial services) system to your mHawala account".

7. Penalty:

7.1 If the contractor fails to complete the said job on or before the Completion Date, the Contractor shall pay to the Purchaser as and by way of Penalty resulting from the delay, the aggregate sum of one percent (1%) of Total Contract price of the delayed services for each week and pro-rata for parts of week, for delay beyond the specified date, subject to a maximum of ten percent (10%) of the Total Contract Price of the service(s). In the event that delay is only in respect of small items which do not affect the effective utilization of the system, penalty shall be chargeable only on the value of such delayed items.

7.2 Any penalty chargeable to the Contractor shall be deducted from the invoice amounts submitted by the Contractor for payment, without prejudice to the Purchaser's rights

8. Construction of Contract:

The Contract shall he deemed to have been concluded in the Islamic Republic of Afghanistan and shall be governed by and construed in accordance with Islamic Republic Afghanistan Law.

9. Termination of the Contract:

9.1 If during the course of the Contract, the Contractor shall be in breach of the Contract and the Purchaser shall so inform the Contractor by notice in writing, and should the breach continue for more than seven days (or such longer period as may be specified by the Purchaser) after such notice then the Purchaser may immediately terminate the Contract by notice in writing to the Contractor.

9.2 Upon termination of the Contract the Purchaser may at his option continue work either by himself or by sub-contracting to a third party. The Contractor shall if so required by the Purchaser within 14 days of the date of termination assign to the Purchaser without payment the benefit to any agreement for services and/or the execution of any work for the purposes of this Contract. In the event of the services/jobs being completed and ready for utilization by the Purchaser or a third party and the total cost incurred by the Purchaser in so completing the required services/jobs being greater than which would have been incurred had the Contract not been terminated then the Contractor shall pay such excess to the Purchaser.

9.3 The Contractor shall not have the right to terminate or abandon the Contract except for reasons of force majeure.

10. Local Taxes, Dues and Levies:

10.1 The Contractor shall be responsible for all government related taxes, dues and levies, including personal income tax, which may be payable in the Afghanistan or elsewhere.

10.2 Withholding tax (if applicable) shall be deducted on local portion only as per prevailing rates as notified Islamic republic of Afghanistan. The amount of withholding Tax(s) is 2% of all project cost for local/registered companies who have Afghanistan Government Official Work License and 7% for International/ nonregistered companies.

Annexure-A

Scope of Work:

Table of Contents

Project Overview:

The project entails the implementation of Multi-Factor Authentication (MFA) on all our portals, operating systems, and databases. This initiative aims to bolster security by introducing an additional layer of authentication beyond traditional username and password methods.

Scope of Work:

We are seeking a comprehensive Technical Statement of Work (SOW) that includes the following components:

Assessment Phase:

Evaluate existing portals, operating systems, and databases to determine compatibility with MFA solutions.

Identify potential challenges and risks associated with the implementation process.

Solution Design:

Propose suitable MFA solutions meet to our organization's requirements. Design a solution architecture that integrates seamlessly with our existing infrastructure. Additionally, we prefer cloud-based solution architecture.

Implementation and Integration:

Deploy MFA solutions across all relevant platforms, ensuring minimal disruption to ongoing operations. Integrate the MFA solution with our current authentication processes.

Testing and Quality Assurance:

Conduct thorough testing of the implemented MFA solution to validate its effectiveness and stability.

Address any issues or discrepancies identified during the testing phase.

Training and Documentation:

Provide training sessions to our technical team for the proper management and administration of the MFA solution.

Create comprehensive documentation outlining the configuration, management, and troubleshooting procedures.

Post-Implementation Support:

Offer ongoing support for the implemented MFA solution, including troubleshooting and updates as needed.

Proposal Submission:

We kindly request that you submit a detailed Technical Statement of Work (SOW) encompassing the above scope along with the following details:

Proposed MFA solution(s) with relevant specifications.

General Solution Questions

Question	***Answer***
The proposed solution must be offered as add-on license for the MFA setup	
The solution must have the option to be deployed as cloud, On-premise, Hybrid or full SaaS with no change to the license.	
Emergency access token code function must be offered to be available for offline situations.	
Proposed solution should offer separate web interface to segregate between day-to-day and maintenance activities	
Solution must be compliant with NCA & SAMA regulations.	
The technology vendor must be ISO9001:2015	

compliant.	
The technology vendor must be FedRAMP compliant	
The proposed vendor must be identified as an overall leader Identity Fabrics at Kuppinger Cole report for the last 4 years.	
Technology vendor must be able to offer IAM solution as a future enhancement.	
There must be no direct connectivity between critical resources like "AD, DNS, DHCP" and the cloud services	
The solution radius interface must be cloud or on premise.	
Password-less authentication must be supported	
Air gaped network authentication support is a must	
Built in radius server, no additional server should be deployed for radius authentication	
FIPS 140-2 compliant cryptography and TLS v1.2 must be applied to secure data in transit and at rest	
Proposed vendor must offer variety of authentication option biometrics, Push notifications, OTP & SMS under the proposed license	
Technology vendor must be able to offer SSO solution as part of the license	
Solution must be able to integrate with Outlook Web Access	
Solution must be able to integrate with Fortinet SSLVPN & ZTNA	
Solution must be able to integrate with Windows RDP	

SAML, Rest-full API and Radius must be supported as integration protocols	
Windows offline authentication must be supported with no disruption in the user experience	
Self-service console must be part of the proposed solution to manage the tokens lifecycle	
MFA application seeding process must be completed using QR code.	
Proposed solution must be able to enable multi-factor authentication for virtual desktop (VDI), Citrix, BYOD, or mobile solutions where LAN, VPN, and Internet-based access to secure resources may occur	
Proposed solution must offer automatic update	
proposed solution must offer IPsec support for VPN connections.	
Users should be able to choose their own security question and answer for forgotten passwords?	
Solution must be scalable to fit the entire business. Please identify where you had a situation where you served customers with multiple independent AD's and how you immediately provided security improvements to these customers by leveraging the investment made from the corporate level but being able to provide additional security to these desktops regardless of network or AD integration.	
Solution must be widely adopted globally, Describe the largest customer production implementation of your solution and its performance.	

Solution Engineering

Question	Answer
Solution performance must be scalable and support high number of concurrent authentications.	
It is preferred that the solution be cloud-based	
Solution must be based on Linux OS, Windows based solutions will not be accepted	
Solution must be including internal DB	
The proposed solution must be offered as OVA ready image	
Solution must be designed to be highly available and survive a disaster with zero RTO/RPO.	

High Level Requirements

Question	Answer
System must be able to populate its user list from Microsoft Active Directory.	
System should be able to populate its user list via AD groups.	

System should be able to query multiple OUs to populate its user list.	
System must be able to populate user lists with other directories via LDAPS.	
System administrative console should be a web application.	
System infrastructure must provide for fail-over clustering over multiple locations	
System infrastructure must provide for load-balancing clustering.	
The system must be compatible with Fortinet VPN clients.	

Software Token Mobile Application

Question	***Answer***
Software application must be available to be downloaded on IOS, Android, MacOS, and Windows devices	
Proposed solution SW application must support Disabling screen sharing	
Proposed solution SW application must support Secure enrolment of the device using certificate pinning	
Proposed solution SW application must support Detection of jailbroken devices	
SW application Credential secrets must be stored in the device secure element and cannot be extracted or copied	
Proposed solution SW application must offer Encryption of locally stored sensitive data	

Annexure – B

General Security Requirements:

1. Vendor must ensure their operating systems are up to date and is not End of Life/End of Support.
2. Vendor must ensure proper patch management of their servers in alignment with EA IT and Cybersecurity policies.
3. Vendor must ensure a licensed and standard AV solution is installed in all of their operating systems.
4. Vendor must ensure full cooperation and coordination with EA Cybersecurity team whenever required.
5. Vendor must not install any application without proper coordination and agreement of EA SOC Team.
6. The use of insecure cryptographic algorithms and protocols are strictly prohibited and all integrations and system communication must be based on secure and strong cryptographic algorithms.
7. Vendor must ensure strong protection of EA data stored on vendor's cloud.
8. Vendor must align all of their services and configurations in accordance to EA Information Security policies and standards.
9. Vendor must use and install only licensed applications.
10. The installation and Integration of servers must be aligned with IT and Cybersecurity requirements.
11. Vendor must not use/install any application/service that is not required.
12. Vendor must communicate any software installation with EA Cybersecurity team in advance.
13. Vendor must align their changes according to EA Change Management Policy.
14. Vendor must ensure all their operating systems are fully patched with the latest OS/Software updates.

15. Vendor must not use any OS that is/will be End of Life / End of Support in less than 3 year.
16. Only secure and strong cryptographic algorithms are allowed to be used in the vendor platforms.
17. System must support Role Based Access Control, and Rule Based Access Control
18. System must provide Strong authentication and authorization mechanisms
19. System must be capable of advanced logging mechanisms to ensure user activities are logged for audit and security purposes and the log must include all of the following at minimum.
    - Failed and successful logins
    - Modification of security settings
    - Privileged use or escalation of privileges
    - System events
    - Modification of system-level objects
    - Session activity
    - Account management activities including password changes, account creation, modification…
    - Event logs must contain the following details:
    - Date and time of activity
    - Source and Destination IP for the related activity
    - Identification of user performing activity
    - Description of an attempted or completed activity.
20. The system must support live log retention of 1 Year and backup up to 3 years.
21. System must be capable of encrypting the log files to ensure user does not modify or change the logs.
22. System must provide cryptographic algorithms such as AES 128/256 Bit, SHA 256/384/512 bits.
23. System must be secure against well-known attacks including but not limited to SQL Injection, XSS, CSRF, SSRF, Code Execution and other attacks.

24. Vendor system's password configuration must be aligned with EA Information security policies.
25. System must support integration with LDAP, IAM "Identity and Access Management" and PAM "Privileged Access Management" Solutions.
26. System must support external log synchronization mechanisms to push logs to another system for analysis such as SIEM and centralized log server.
27. The database must support the encryption of admin user's information with algorithms such as PBKDF2 and SHA256/384/512 bits.
28. The database platforms "if any" must support the encryption of data in-transit and at rest.

Important Note:

Bidders, vendors, and any concerned party shall fill all the fields in the below table, any missing or non-compliant item may cause disqualifying the proposed system from the Etisalat Security side.

S. No.	Description	Compliance (YES/NO/NA)	Comments
1	**Etisalat Security Requirements**		
1.1	The Contractor/Supplier/vendor to sign Non-Disclosure Agreement (NDA) with Etisalat before finalizing RFx/contract/POC agreement as per Etisalat NDA process.		
1.2	Contractor/Supplier/vendor equipment's (e.g. Servers, PCs, etc.) that are connected to Etisalat network must be securely wiped before taking out of Etisalat premises.		
1.3	The proposed/contracted system shall pass Etisalat Security Audit (Vulnerability Assessment/Penetration Testing) before go-live/service acceptance by Etisalat.		

	Contractor/Supplier/vendor shall provide SLA for fixing Security gaps based on severity.		
1.4	Contractor/Supplier/vendor shall fix all security issues identified and reported by ETISALAT and/or Third Party Contracted to do the testing, with no additional cost		
1.5	Contractor/Supplier/vendor confirms that its products/solution are tested for weaknesses via methods such as Vulnerability Assessment, penetration testing, red teaming exercises and scans that check for compliance against the baseline security standards or security best practices, before the new product or any of its releases is delivered to ETISALAT. The Contractor/Supplier/vendor shall provide evidence/report of the security assessment/audit of the proposed solution.		
2	**Security Architecture**		
2.1	The Contractor/Supplier/vendor shall ensure that proposed solution shall comply with the applicable IT and Telecom Security standards (such as Afg. NESA (SIA) IA V2, Afg. DESC (ISR), Afg. TRA, 3GPP, ETSI, ENISA, CSA, NIST, PCI, ISO, GDPR etc.) The Contractor/Supplier/vendor shall confirm the applicable standard.		
2.2	The proposed solution shall support the latest operating systems and application versions. Contractor/Supplier/vendor to ensure		

	proposed solutions will run the latest stable software, operating system, and firmware.		
2.3	The solution shall be designed with multi-tier architecture, (Demilitarized Zone (DMZ), middleware, and private network). Any system accessible from the Internet shall be on the DMZ and access to internal sensitive data shall be secured through the middle tier application proxy.		
2.4	The proposed solution shall not impact or relax existing Etisalat security control or posture.		
2.5	The performance of the proposed system shall meet the business requirements without disabling or removing any existing security control		
2.6	The Contractor/Supplier/vendor shall provide only secure methods of communication such as HTTPS, SFTP, SCP, TLS1.3, IPSEC, SRTP, SSH v2, SNMPv3 between the proposed nodes. Non-secure protocols such as Telnet, HTTP and FTP shall not be used.		
3	**Password Security**		
3.1	All Operating Systems (e.g. Linux and Windows) shall be hardened according to well-known standards such as, but not limited to NIST, CIS security benchmark, and NSA.		
3.2	The proposed system includes password management module that supports the		

	following features:		
3.3	Setting the minimum password length		
3.4	Password complexity, and not accepting blank passwords		
3.5	Maximum password age and password history		
3.6	Account lockout		
3.7	Enforce changing password after first login		
3.8	Prompt / notify for the old password on password changes		
3.9	The password shall be saved in hashed format (i.e. irreversible encryption)		
3.10	Forgetting or resetting password function shall support using OTP or email for verification		
4	**Authentication**		
4.1	The proposed system shall not provide access without valid username and password.		
4.2	All user access to the proposed system shall support Privilege account Management (PAM) integration.		
4.3	For public web applications, the proposed system supports and uses CAPTCHA or OTP to prevent password dictionary attacks		
4.4	For mobile applications, the proposed system shall support and uses fingerprint authentication method		
4.5	The proposed system supports and uses		

	secure authentication protocols, like Kerberos, LDAP-S, NTLM V2 and above, HTTPs (for web applications)		
4.6	The proposed system will not use insecure authentication protocols, like NTLM v1, HTTP (for web applications)		
4.7	The proposed system shall support session timeout settings		
4.8	The proposed solution shall support secure API architecture to integrate systems to exchange data where deemed necessary.		
5	**Authorization**		
5.1	The proposed solution shall support role-based access controls that includes access profiles or security matrix (i.e. Role Name VS. Access Permissions)		
5.2	The proposed system supports role-based access permissions, i.e. Administrator, Operator, Viewer, User…		
6	**Software Security**		
6.1	The software development and testing will not run on the production systems, and will be running in an isolated environment		
6.2	The software source code will not include clear-text passwords		
6.3	The software code will not include insecure protocols, like FTP, telnet …etc.		
6.4	The software testing will not use live/production sensitive or PII data unless it's		

	masked as Etisalat security policy		
6.5	The proposed system enforces input and output validation to prevent security attacks, like SQL Injection, Buffer Overflow…etc.		
6.6	For web portals, the proposed system includes all security controls to prevent / protect from OWASP Top 10 security attacks and risks		
6.7	For mobile application, the proposed system shall include security checks / controls to protect from mobile attacks, like SSL Pinning, Jailbreak, Anti-debug, Anti-hooking, and Advanced Obfuscation…		

S. No.	Description	Compliance (YES/NO/NA)	Comments
7	**Security Event Logging**		
7.1	Proposed systems shall support standard logging protocols such as CIFS/Syslog/CSV logs files		
7.2	The system shall generate and support audit logs that contain the following fields (as a minimum): a) Username b) Timestamp (Date & Time). c) Client IP Address d) Transaction ID & session information		
7.3	The proposed solution shall support the integration with Etisalat NTP for time synchronization and accurate logging.		
8	**Public Cloud Security**		
8.1	Etisalat customers' and staff personal data (PII: name, contacts, address, Emirates ID, Passport number, Nationality …) is encrypted at rest and in transit using a strong industry-standard encryption protocol		
8.2	The Public Cloud setup that stores PII information shall be hosted in the Afghanistan		
8.3	The Public Cloud setup is hosted in a dedicated tenant for Etisalat (i.e. not shared)		

8.4	The Public Cloud data Center shall not be moved to another country or location without prior coordination and approval from Etisalat		
8.5	All Etisalat data will be permanently erased from the Public Cloud on termination of the service or support agreement		
8.6	The proposed Cloud system supports Etisalat Cloud Access Security Broker (such as Microsoft MCAS, Netskope CASB)		
9	**Virtualization and Container Security**		
9.1	If applicable, Bidder shall ensure the proposed virtualized infrastructure, service based and micro services architecture to support multi tenancy, zoning & micro-segmentation, security visibility, secure virtualization (sVirt), trusted image signing, virtual Firewalls, DoS protection, Trusted platform module (TPM), Hypervisor & Host OS security to secure data and resources.		
9.2	The proposed solution shall support integration with Etisalat/Leading Container Security Solution, where applicable, to scan the container images and ensure malware protection of CI/CD pipeline.		
9.3	Suppliers must inform EA Cybersecurity of any non-conformity with defined EA policies and processes that are agreed upon in advance to acquire a written approval from		

	EA Cybersecurity Department or senior management as required otherwise Supplier will be responsible for all the potential losses		

RFP General Terms Compliance to be filled by Bidder

S/N	Clause No. and General Terms	Comply (Yes/No)	Remarks
1	**4. VALIDITY OF OFFERS:**		
2	**6. ACCEPTANCE OF OFFERS:**		
3	**7. REGISTRATION/LEGAL DOCUMENTS OF THE BIDDER**		
4	**8. PAYMENTS**		
5	**9. PENALTY:**		
6	**10. CONSTRUCTION OF CONTRACT:**		
7	**11. TERMINATION OF THE CONTRACT BY THE PURCHASER**		
8	**12. LOCAL TAXES, DUES AND LEVIES:**		

The following Information must be submitted with offer.

Bidder Contact Details	
Bidder Name	
Bidder Address	
Bidder Email Address	
Bidder Phone Number	
Bidder Contact Person Name	
Bidder Contact Person Phone No	
Bidder Contact Person Email Address	
Bidder Registration License Number	
License Validity	
TIN Number /Tax Number	

**********End of Doc**********